UNIVERSIDADE NOVE DE JULHO – UNINOVE
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA E GESTÃO DO CONHECIMENTO

JOÃO RAFAEL GONÇALVES EVANGELISTA

DETECÇÃO DE EVIDÊNCIAS DE PORNOGRAFIA INFANTOJUVENIL EM IMAGENS DIGITAIS COM ESTRATÉGIAS FORMADAS POR TÉCNICAS COMPUTACIONAIS INTEGRADAS

São Paulo
2024

UNIVERSIDADE NOVE DE JULHO – UNINOVE
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA E GESTÃO DO CONHECIMENTO

JOÃO RAFAEL GONÇALVES EVANGELISTA

DETECÇÃO DE EVIDÊNCIAS DE PORNOGRAFIA INFANTOJUVENIL EM IMAGENS DIGITAIS COM ESTRATÉGIAS FORMADAS POR TÉCNICAS COMPUTACIONAIS INTEGRADAS

Texto de Defesa apresentado ao Programa de Pós-Graduação em Informática e Gestão do Conhecimento da Universidade Nove de Julho – UNINOVE, como requisito parcial para a obtenção do título de Doutor em Informática e Gestão do Conhecimento.

Prof. Orientador: Dr. Renato José Sassi
Linha de Pesquisa 3: Gestão da Informação e do Conhecimento

São Paulo
2024

Evangelista, João Rafael Gonçalves.

Detecção de evidências de pornografia infantojuvenil em imagens digitais com estratégias formadas por técnicas computacionais integradas. / João Rafael Gonçalves Evangelista. 2024.

188 f.

Tese (Doutorado)- Universidade Nove de Julho - UNINOVE, São Paulo, 2024.

Orientador (a): Prof. Dr. Renato José Sassi.

1. Pornografia infantojuvenil. 2. Conteúdo sensível. 3. Imagens digitais. 4. Técnicas computacionais. 5. Exame pericial.

I. Sassi, Renato José. II. Título

CDU 004

UNINOVE
Universidade Nove de Julho

PARECER – EXAME DE DEFESA

Parecer da Comissão Examinadora designada para o exame de defesa do Programa de Pós-Graduação em Informática e Gestão do Conhecimento a qual se submeteu o aluno João Rafael Gonçalves Evangelista.

Tendo examinado o trabalho apresentado para obtenção do título de "Doutor em Informática e Gestão do Conhecimento", com Tese intitulada "Detecção de Evidências de Pornografia Infantojuvenil em Imagens Digitais com Estratégias Formadas por Técnicas Computacionais Integradas", a Comissão Examinadora considerou o trabalho:

(X) Aprovado **( ) Aprovado condicionalmente**

( ) Reprovado com direito a novo exame **( ) Reprovado**

EXAMINADORES

Prof. Dr. Renato José Sassi - Uninove (Orientador)

Prof. Dr. Jesus Pascual Mena Chalco – UFABC (Membro Externo)

gov.br Documento assinado digitalmente
JESUS PASCUAL MENA CHALCO
Data: 13/08/2024 14:12:32-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Edson Melo de Souza – UNINOVE (Membro Externo)

gov.br Documento assinado digitalmente
EDSON MELO DE SOUZA
Data: 13/08/2024 12:36:47-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Cleber Gustavo Dias – UNINOVE (Membro Interno)

gov.br Documento assinado digitalmente
CLEBER GUSTAVO DIAS
Data: 14/08/2024 08:54:19-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Sidnei Alves de Araújo – UNINOVE (Membro Interno)

gov.br Documento assinado digitalmente
SIDNEI ALVES DE ARAUJO
Data: 13/08/2024 17:19:56-0300
Verifique em https://validar.iti.gov.br

São Paulo, 08 de agosto de 2024

Dedico este trabalho à minha companheira Mayara Thábata, meus pais Edinalva Gonçalves e José Elizeu, e ao Prof. Dr. Renato José Sassi, meu orientador. Vocês representaram a motivação central para o desenvolvimento e conclusão deste trabalho.

AGRADECIMENTOS

Agradeço, em primeiro lugar, a Deus, que sempre esteve ao meu lado, orientando os meus passos, e colocando pessoas maravilhosas em meu caminho.

À Universidade Nove de Julho (UNINOVE) pelo apoio e pela oportunidade de crescimento e aprimoramento acadêmico, pessoal e profissional, assim como pela bolsa de estudos.

À minha companheira, Mayara Thábata Sá de Lima, que sempre me apoiou e incentivou a jamais desistir dos meus objetivos.

Aos meus pais, Edinalva Gonçalves e José Elizeu Evangelista, que sempre me incentivaram a estudar e me mostraram como a educação transforma as pessoas.

Ao Centro Paula Souza, a Claro S.A. e a Embratel, incluindo todos os meus colegas de trabalho, em especial, Alexandre Aura, Érika Pavarin e Messias de Fátima, pessoas que sempre me motivaram a alcançar meus objetivos.

Aos meus colegas da Polícia Federal do Brasil, Mateus Polastro, José Helano Matos Nogueira, Luis Nassif e Thiago Sandoval, expresso minha gratidão pelas contribuições e discussões que apoiaram o desenvolvimento deste trabalho.

Aos professores e colegas de universidade que me auxiliaram de maneira direta ou indireta. Em especial, ao Prof. Dr. Dacyr Dante de Oliveira Gatto e aos meus colegas de pesquisa do PPGI pelas dicas, pelo apoio e pelos conselhos ao longo desta jornada que é a vida acadêmica.

Ao Prof. Dr. André Felipe Henriques Librantz que, juntamente com meu orientador, Prof. Dr. Renato José Sassi, acreditaram no meu potencial e me proporcionaram momentos de crescimento e aprendizado.

Ao meu orientador, Prof. Dr. Renato José Sassi, pelo apoio, suporte e conhecimento, e pela confiança, paciência, coordenação e disponibilidade.

Enfim, os meus sinceros agradecimentos a todos que de alguma forma contribuíram para a minha jornada acadêmica.

"As coisas que já imaginei que seriam minhas maiores conquistas foram só os primeiros passos rumo a um futuro que começo, meramente, a vislumbrar."

Jace Beleren

RESUMO

Criminosos utilizam da internet para realizar crimes cibernéticos, como compartilhar arquivos com pornografia infantojuvenil. Detectar evidências deste tipo de crime é uma tarefa realizada por autoridades policiais em um exame pericial. Uma dificuldade encontrada na detecção de evidências é a variedade e quantidade de arquivos presentes em um dispositivo a ser examinado. Uma forma de aumentar as chances de sucesso do exame pericial é utilizar Estratégias formadas por técnicas computacionais integradas oriundas das áreas: Computação Forense, Inteligência Artificial e Visão Computacional. Assim, o objetivo deste trabalho foi desenvolver e aplicar Estratégias formadas por técnicas computacionais integradas das áreas da Computação Forense, Inteligência Artificial e Visão Computacional aplicadas na detecção de evidências pornografia infantojuvenil em imagens digitais, para apoiar a execução de exames periciais. Ao conjunto destas Estratégias foi dado o nome Fenrir. Foram desenvolvidas quatro Estratégias: Detecção e recuperação de valores Hash Perceptivos (A), Detecção de pessoas (B), Detecção de conteúdo textual relacionado com pornografia infantojuvenil (C) e Detecção de objetos relacionados com pornografia infantojuvenil (D). Os resultados obtidos com o desenvolvimento e aplicação das Estratégias foram considerados promissores porque atingiram o objetivo proposto para cada Estratégia e, consequentemente o objetivo geral. A Estratégia A formada pelo Algoritmo de Hash Perceptivo e as Redes Neurais de Hopfield obteve a taxa de acerto de 89,36%, sendo possível calcular e recuperar valores Hash Perceptivo para detectar imagens semelhantes ou alteradas. A Estratégia B formada pelas técnicas da Detecção de Cor de Pele e Floresta Aleatória obteve uma acurácia de 99,98%, sendo possível identificar cores de pele nos pixels de imagens e assim, detectar pessoas. A Estratégia C formada pelas técnicas de Extração de Metadados, OCR, LSTM e Processamento de Linguagem Natural obteve valores das Taxas de Erro CER e WER variando entre 0.1 e 10.0, sendo possível detectar conteúdo textual relacionado com Pornografia Infantojuvenil em imagens e, finalmente a Estratégia D formada pelas técnicas da Detecção de Objetos, Redes Neurais Artificiais Convolucionais e as Redes Adversárias Generativas obteve a taxa de acerto de 60% na identificação e classificação de objetos, sendo possível detectar objetos relacionados com Pornografia Infantojuvenil em imagens. Concluiu-se que o desenvolvimento e aplicação de Fenrir apoiou a execução de exames periciais na detecção de evidências de pornografia infantojuvenil.

Palavras-chave: Pornografia Infantojuvenil, Conteúdo Sensível, Imagens Digitais, Técnicas Computacionais, Exame Pericial.

ABSTRACT

Criminals use the internet to make cybercrimes, such as sharing files with child pornography. Detecting evidence of this type of crime is a task made by police authorities in an expert examination. A difficulty in detecting evidence is the variety and quantity of files present on a device to be examined. One way to increase the chances of success in the forensic examination is to use Strategies made up of integrated computational techniques from Forensic Computing, Artificial Intelligence, and Computer Vision. Thus, the objective of this work was to develop and apply Strategies made up of integrated computational techniques from the areas of Forensic Computing, Artificial Intelligence, and Computer Vision applied to the detection of evidence of child pornography in digital images, to support the execution of expert examinations. The name Fenrir was given to all these Strategies. Four Strategies were developed: Detection and recovery of Perceptual Hash values (A), Detection of people (B), Detection of textual content related to child pornography (C), and Detection of objects related to child pornography (D). The results obtained with the development and application of the Strategies were considered promising because they achieved the objective proposed for each Strategy and, consequently, the general objective. Strategy A formed by the Perceptual Hash Algorithm and Hopfield Neural Networks obtained an accuracy rate of 89.36%, making it possible to calculate and recover Perceptual Hash values to detect similar or altered images. Strategy B, formed by Skin Color Detection and Random Forest, achieved an accuracy of 99.98%, making it possible to identify skin colors in image pixels and detect people. Strategy C formed by Metadata Extraction, OCR, LSTM, and Natural Language Processing obtained CER and WER Error Rate values ranging between 0.1 and 10.0, making it possible to detect textual content related to Child Pornography in images, finally, Strategy D formed by Object Detection, Convolutional Artificial Neural Networks, and Generative Adversarial Networks, it obtained a 60% success rate in identifying and classifying objects, making it possible to detect objects related to Child Pornography in images. It was concluded that the development and application of Fenrir supported the execution of expert examinations to detect evidence of child pornography.

Keywords: Child Pornography, Sensitive Content, Digital Images, Computational Techniques, Expert Examination.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

AM	Aprendizagem de Máquina
AODE	*Averaged One-Dependence Estimators*
BBN	*Bayesian Belief Network*
BIRCH	*Balanced Iterative Reducing and Clustering using Hierarchies*
BMP	*Bitmap*
CAM	*Child Abuse Material*
CART	*Classification and Regression Tree*
CED	Convolução Espacial Discreta
CEM	*Child Exploitation Material*
CER	*Character Error Rate*
CHAID	*Chi-squared Automatic Interaction Detection*
CIE L*a*b	*CIE 1976 (L*, a*, b*) Color Space*
CIE L*c*h	*CIE 1976 (L*, C*, h) Color Space*
CIE L*u*v	*CIE 1976 (L*, u*, v*) Color Space*
CMY	*Cyan, Magenta, Yellow*
CMYK	*Cyan, Magenta, Yellow and Black*
CSA	*Child Sexual Abuse*
CSAI	*Child Sexual Abuse Images*
CSAM	*Child Sexual Abuse Material*
CSE	*Child Sexual Exploitation*
CSEA	*Child Sexual Exploitation and Abuse*
CSEM	*Child Sexual Exploitation Material*
CSM	*Child Sexual Material*
CTC	Convolução Temporal Contínua
CTD	Convolução Temporal Discreta
DBM	*Deep Boltzmann Machine*
DBSCAN	*Density-Based Spatial Clustering of Applications with Noise*
DL	*Deep Learning*
DPI	*Dots per Inch*
ECA	Estatuto da Criança e do Adolescente
EM	*Expectation–Maximization*

EXIF	*Exchangeable Image File Format*
FN	Falso Negativo
FP	Falso Positivo
GAN	*Generative Adversarial Network*
GBM	*Gradient Boosting Machine*
GIF	*Graphics Interchange Format*
HD	*Hard Disk*
HP	*Hewlett-Packard*
HSV	*Hue, Saturation and Value*
HSL	*Hue, Saturation and Lightness*
IA	Inteligência Artificial
ID3	*Iterative Dichotomiser 3*
IIOC	*Indecent Images of Child*
IOU	*Intersection Over Union*
JPEG	*Joint Photographic Experts Group*
KNN	*K-Nearest Neighbors*
LARS	*Least Angle Regression*
LASSO	*Least Absolute Shrinkage and Selection Operator*
LDA	*Linear Discriminate Analysis*
LOESS	*Locally Weighted Smoothing*
LSTM	*Long Short-Term Memory*
LVQ	*Learning Vectorization*
LWL	*Local Weighted Learning*
MARS	*Multivariate adaptive regression spline*
MLP	*Multi-layer Perceptron*
NER	*Named Entity Recognition*
OCR	*Optical Character Recognition*
OCSA	*Online Child Sexual Abuse*
OCSAM	*Online Child Sexual Abuse Material*
OCSE	*Online Child Sexual Exploitation*
OCSEA	*Online Child Sexual Exploitation and Abuse*
ONG	Organização Não Governamental
OSEC	*Online Sexual Exploitation of Children*
P2P	*Peer-to-Peer*

PDF	*Portable Document Format*
PID	Processamento de Imagens Digitais
PLN	Processamento de Linguagem Natural
PNG	*Portable Network Graphics*
RBF	*Radial Basis Function*
RELU	*Rectified Linear Unit*
RGB	*Red, Green and Blue*
R-CNN	*Region-based - Convolutional Neural Networks*
ROC	*Receiver Operating Characteristics*
RNN	*Recurrent Neural Networks*
RNC	*Redes Neurais Convolucionais*
RSL	Revisão Sistemática da Literatura
SEM-C	*Sexual Exploitation Material - Children*
SOM	*Self-Organizing Maps*
SSP-SP	Secretaria de Segurança Pública do Estado de São Paulo
SVM	*Support Vector Machine*
URL	*Uniform Resource Locator*
VC	Visão Computacional
VN	Verdadeiro Negativo
VP	Verdadeiro Positivo
WER	*Word Error Rate*
Xyz	*CIE 1931 Color Space*
YCbCr	*Luminance, Chrominance Blue, Chrominance Red*
YiQ	*Composite Video Color Space*
YOLO	*You Only Look Once*
YxY	*CIE 1931 Chromaticity Diagram*

SUMÁRIO

1. INTRODUÇÃO

O avanço tecnológico promove novas oportunidades para as organizações. Este avanço é sustentado por um conjunto de tecnologias, sendo a internet e suas formas de compartilhar arquivos a principal entre elas. Como resultado, uma quantidade considerável de arquivos de diversos tipos como imagens e vídeos trafegam na internet (DEORA; CHUDASAMA, 2021).

Entretanto, mesmo que compartilhar arquivos na internet traga uma série de vantagens, tal ação também traz desvantagens, uma vez que facilita a realização de crimes cibernéticos. O crime cibernético é um tipo de atividade criminosa realizada com dispositivos eletrônicos, como computadores e dispositivos móveis, ou que tenham os referidos dispositivos como alvo (SEBYAN BLACK; FENNELLY, 2021).

Pode-se citar diversos tipos de crimes cibernéticos, como o envio de *Phishing*, invasões a sistemas e computadores, vazamento de dados, roubo de identidade e espionagem industrial. Há também os crimes cibernéticos relacionados diretamente a crianças e adolescentes, como a corrupção de menores, chamada de *Grooming*, *Cyberbullying*, e a produção, compartilhamento e armazenamento de arquivos com pornografia infantojuvenil (QUAYLE, 2020).

A pornografia infantojuvenil é um crime cibernético previsto na lei nº 11.829, de 25 de novembro de 2008, no artigo 240º, descrita como: “Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente”. Esta lei é uma atualização do Estatuto da Criança e do Adolescente (ECA), descrito na lei nº 8.069, de 13 de julho de 1990 (BRASIL, 2008).

A materialidade da pornografia infantojuvenil é encontrada em arquivos multimídia, como imagens e vídeos. Além do ato sexual ou a nudez do público infantojuvenil, estes arquivos podem conter palavras, textos, objetos e símbolos relacionados a pornografia infantojuvenil (LARANJEIRA DA SILVA et al., 2022).

A detecção da materialidade de pornografia infantojuvenil requer a utilização de métodos, técnicas, estratégias e outros recursos da Computação Forense. Esta área multidisciplinar visa elucidar aspectos relacionados a autoria, materialidade e a dinâmica dos crimes cibernéticos, ao transformar vestígios em evidências, e posteriormente em provas (CHEN et al., 2020).

Os autores Elgohary, Darwish e Elkaffas (2022) abordam, em seus estudos, duas tarefas essenciais que devem ser utilizadas ao investigar um crime cibernético: a cadeia de custódia e

o exame pericial. A cadeia de custódia engloba todo o conjunto de procedimentos destinados a manter e documentar a cronologia da coleta dos vestígios em um possível local de crime. Já o exame pericial é a tarefa utilizada para transformar os vestígios coletados na cadeia de custódia em evidência, associando-os a um determinado crime específico (DÍAZ-PÉREZ et al., 2022).

Uma dificuldade encontrada pelas autoridades policiais durante a realização de um exame pericial reside na detecção de evidências do crime cibernético. A busca manual por evidências pode se tornar uma tarefa complexa e exaustiva devido à quantidade e diversidade de arquivos que podem existir em um dispositivo eletrônico a ser periciado (AL-NABKI et al., 2020).

Para apoiar a execução do exame pericial, são utilizadas técnicas de Computação Forense. Em investigações relacionadas a pornografia infantojuvenil, são utilizadas técnicas específicas para arquivos multimídia (ELEUTÉRIO; MACHADO, 2019; PADILHA et al., 2021).

Os autores Anda, Le-Khac e Scanlon (2020) e Appati, Lodonu e Chris-Koka (2021) listam em seus estudos algumas técnicas de Computação Forense que podem ser utilizadas para apoiar a execução de um exame pericial. São elas: o Hash Perceptivo, o Reconhecimento Óptico de Caracteres ou OCR (*Optical Character Recognition*), a Extração de Metadados e a análise gráfica. Esta última, abrange outras técnicas, como a detecção de pessoas e objetos.

Sobre a utilização das técnicas listadas pelos autores Anda, Le-Khac e Scanlon (2020) e Appati, Lodonu e Chris-Koka (2021) em um exame pericial, o Hash perceptivo é utilizado para detectar arquivos identificados anteriormente como evidência (Breidenbach; Steinebach e Liu, 2020). O OCR é utilizado para detectar evidências no conteúdo textual de imagens (Avyodri; Lukas; Tjahyadi, 2022). A extração de metadados é utilizada para detectar evidências nos dados intrínsecos dos arquivos (Blanchy et al., 2023). Quanto as técnicas que fazem parte da Análise Gráfica, a detecção de cor de pele é utilizada para detectar pessoas em arquivos multimídia (Ganesan et al., 2023) e a detecção de objetos é utilizada para detectar objetos em arquivos multimídia (DIWAN; ANIRUDH; TEMBHURNE, 2023).

Apesar das técnicas listadas pelos autores Anda, Le-Khac e Scanlon (2020) e Appati, Lodonu e Chris-Koka (2021) serem utilizadas em um exame pericial, estas técnicas possuem limitações que podem impactar no resultado final, que é a detecção de evidências. O Hash Perceptivo não é capaz recuperar valores Hash perceptivo para detectar imagens similares ou que tenham sofrido alguma alteração (Sabahi; Omair Ahmad; Swamy, 2018). No caso do OCR,

as limitações estão relacionadas à detecção de idioma, texturas, tamanho da fonte, distorções, estilo, resolução, luminosidade e caracteres manuscritos (GUPTA; KUMAR, 2020).

As limitações da Extração de Metadados residem na estruturação do conteúdo extraído, já que os metadados podem ser de diversos tipos e formatos (Du; Scanlon, 2019). Já para as técnicas de detecção de cor de pele e de detecção de objetos, suas limitações são semelhantes às do OCR (MANI et al., 2022; ZHU; SANG; HE, 2022; ZOU et al., 2023).

Uma forma de superar as limitações destas técnicas de Computação Forense e aplicá-las na detecção de evidências de pornografia infantojuvenil para apoiar a execução de exames periciais é integrá-las com técnicas de outras áreas computacionais. A integração de técnicas de diferentes áreas é denominada Estratégia (CIFUENTES; SANDOVAL OROZCO; GARCÍA VILLALBA, 2022; POVEDANO ÁLVAREZ et al., 2023).

Os autores Hayes e Kyobe (2020) apresentam em seu estudo um ganho de desempenho considerável ao integrar técnicas de Computação Forense com técnicas das áreas da Inteligência Artificial (IA) e da Visão Computacional (VC). Este ganho de desempenho pode significar uma redução na quantidade de falsos positivos detectados em tarefas de classificação e previsão, redução de tarefas manuais e menor tempo de processamento.

Adicionalmente, a integração de técnicas de Computação Forense com técnicas oriundas das áreas da IA e VC possibilita executar tarefas que isoladamente não seriam possíveis, como por exemplo analisar de forma automática volumes consideráveis de dados e imagens, detectar anomalias e reconhecer padrões (SANCHEZ et al., 2019).

São exemplos de técnicas de IA que podem ser utilizadas de forma integrada com técnicas de Computação Forense: as Redes Neurais Artificiais (RNAs) e suas variações, bem como a Floresta Aleatória, ambas usadas para tarefas de previsão e classificação. No contexto da VC, são exemplos de técnicas que podem ser integradas com técnicas de Computação Forense: a Detecção de cor de pele e a Detecção de objetos (CIFUENTES; SANDOVAL OROZCO; GARCÍA VILLALBA, 2022; WAELEN, 2023).

Compreendendo a relevância do ganho de desempenho ao utilizar Estratégias e a urgência que a detecção de evidências de pornografia infantojuvenil requer, os autores Povedano Álvarez et al. (2023) e Cifuentes; Sandoval Orozco e García Villalba (2022) reforçam em seus estudos a necessidade de se desenvolver novas Estratégias e aprimorar as já existentes.

Outro item destacado pelos autores Povedano Álvarez et al. (2023) e Cifuentes; Sandoval Orozco e García Villalba (2022) é que, dado o avanço contínuo das tecnologias utilizadas para propagar pornografia infantojuvenil na internet, é imperativo que as Estratégias desenvolvidas para detectar evidências deste crime cibernético acompanhem essa evolução.

As Estratégias sugeridas para serem desenvolvidas e aplicadas na detecção de evidências de Pornografia Infantojuvenil incluem a detecção de imagens similares as já identificadas como pornografia infantojuvenil, bem como a detecção de conteúdo textual e de objetos relacionados a este tipo de crime cibernético. Já as Estratégias sugeridas para serem aprimoradas, pode-se citar por exemplo, a detecção de pessoas por meio da detecção de cor de pele (CIFUENTES; SANDOVAL OROZCO; GARCÍA VILLALBA, 2022; POVEDANO ÁLVAREZ et al., 2023).

Diante deste cenário, considera-se relevante desenvolver Estratégias formadas por técnicas computacionais integradas das áreas da Computação Forense, IA e VC e aplicá-las na detecção de evidências de Pornografia Infantojuvenil em imagens digitais para apoiar a execução de exames periciais.

1.1. JUSTIFICATIVA E MOTIVAÇÃO DA PESQUISA

O panorama sobre a ocorrência de crimes cibernéticos evoluiu em razão da crescente interconectividade entre as pessoas por meio de seus dispositivos eletrônicos conectados na internet. Conforme mais pessoas compartilham informações na internet, maior o interesse dos criminosos em usufruir destas informações. Isso faz com que criminosos se sintam atraídos para desenvolver e praticar crimes cibernéticos.

Com os crimes cibernéticos cada vez mais sofisticados, as leis e normas ficam aquém da tecnologia utilizada pelos criminosos que exploram a diversidade de plataformas encriptadas e anônimas, como a *Dark Web*, para disseminar e comercializar conteúdos ilícitos, tornando o rastreamento difícil (Al-Khater et al., 2020; Setiawan et al., 2018). No contexto da Pornografia Infantojuvenil, detectar evidências é de suma importância, dado o caráter universal e impactante da violência contra a população infantojuvenil. A violência sexual representa uma forma grave de agressão, abuso e exploração do público infantojuvenil, acarretando traumas lesivos ao corpo e a mente da vítima (MACEDO; COSTA; DOS SANTOS, 2018).

A não detecção de evidências de pornografia infantojuvenil pode resultar na proliferação desse tipo de conteúdo, e consequentemente, amedrontar as vítimas após a exploração, podendo

levar a sentimento de culpa e vergonha, afetando sua autoestima e sua vida social. Além disso, a permanência deste tipo de material na internet significa que as vítimas enfrentam uma ameaça constante do ressurgimento desta exploração (AL-NABKI et al., 2020).

Ressalta-se que os impactos gerados pela propagação de pornografia infantojuvenil não estão limitadas às vítimas. Estes impactos estendem-se às suas famílias e a sociedade em geral. Isso reforça a necessidade do desenvolvimento de Estratégias capazes de prevenir, identificar e apoiar o combate desta forma de abuso e exploração (POVEDANO ÁLVAREZ et al., 2023).

Sobre o combate a pornografia infantojuvenil feito por autoridades policiais, as restrições de recursos, incluindo de financiamento e mão-de-obra, dificultam os esforços de investigação. Adicionalmente, estas restrições representam um obstáculo significativo, pois sobrecarregam as autoridades policiais com um volume considerável de trabalho. Portanto, é fundamental o desenvolvimento de Estratégias que possam apoiar o trabalho feito pelas autoridades policiais (AL-KHATER et al., 2020; NGOX et al., 2022).

No que se refere a detecção de evidências de Pornografia Infantojuvenil, é uma atividade realizada por autoridades policiais em um exame pericial. O principal desafio enfrentado neste contexto reside na detecção manual de evidências. Uma busca manual pode-se tornar uma tarefa exaustiva e complexa devido à quantidade e diversidade de arquivos presentes nos dispositivos a serem periciados (AL-NABKI et al., 2020).

Para analisar volumes consideráveis de arquivos dos mais variados tipos e tamanhos, são usados softwares e outras ferramentas computacionais. Essas ferramentas possibilitam extrair, analisar e interpretar as informações contidas nestes arquivos de maneira sistemática. Neste contexto, usar técnicas da Computação Forense para detectar pornografia infantojuvenil torna possível mapear toda a atividade criminosa, de forma a detectar evidências do crime, evidenciar os autores e as possíveis propagações realizadas.

Haverá casos em que as técnicas de Computação Forense isoladamente não conseguirão realizar determinadas tarefas ou não trarão resultados satisfatórios, seja com a duração total de uma tarefa, a escalabilidade ou a precisão. Segundo os autores Sanchez et al. (2019) e Hayes e Kyobe (2020), uma forma de viabilizar a realização destas tarefas é integrá-las com técnicas da Inteligência Artificial (IA) e da Visão Computacional (VC).

A integração de técnicas oriundas de diferentes áreas, como a Computação Forense, IA e VC é denominada Estratégia (Cifuentes; Sandoval Orozco; García Villalba, 2022; Povedano Álvarez et al., 2023). No contexto do combate à Pornografia Infantojuvenil, o desenvolvimento, aplicação e aprimoramento de Estratégias estão diretamente ligados à inovação científica. O autor, como pesquisador da área da Segurança da Informação, entende que desenvolver formas de detectar e prevenir a propagação de pornografia infantojuvenil não só contribui para o avanço da ciência, mas também gera um impacto real e positivo na vida do público infantojuvenil e de seus familiares ao combater este tipo de crime cibernético.

Detectar e combater a pornografia infantojuvenil não é apenas uma questão legal, mas também uma missão moral. Garantir a proteção do público infantojuvenil de abusos, bem como a identificação e punição dos criminosos é uma extensão natural do trabalho de um profissional de Segurança da Informação. Em adição, desenvolver novas formas para detectar pornografia infantojuvenil significa colaborar com outros pesquisadores, autoridades policiais, instituições e órgãos governamentais, ampliando assim o alcance das soluções, promovendo um ambiente digital mais seguro.

No contexto do Estatuto da Estatuto da Criança e do Adolescente (ECA), está a motivação para combater a pornografia infantojuvenil, a qual contraria os princípios fundamentais do bem-estar, da salvaguarda e da dignidade. O ECA ressalta que o público infantojuvenil tem direito a crescer em um ambiente seguro e acolhedor, livre de toda forma de abuso e exploração. Assim, combater a pornografia infantojuvenil é impulsionado por uma responsabilidade coletiva, ética e moral de proteger a inocência do público infantojuvenil.

Para o conjunto de Estratégias propostos nesse trabalho, definiu-se o nome de Fenrir. Este nome é uma referência direta à mitologia nórdica, onde Fenrir, um lobo gigante, é destinado a caçar Odin durante o fim dos tempos do mundo nórdico, chamado de Ragnarok. A escolha pelo nome Fenrir reflete a missão das estratégias propostas nesse trabalho. Assim como Fenrir, uma fera que caça e combate sua presa, as estratégias buscam evidências para combater o crime cibernético de pornografia infantojuvenil.

Assim, encontra-se na necessidade de superar os desafios relacionados com a detecção de evidências de pornografia infantojuvenil em um exame pericial, a motivação e oportunidade de desenvolver e aplicar Fenrir e suas Estratégias formadas por técnicas computacionais integradas das áreas da Computação Forense, IA e VC.

1.2. IDENTIFICAÇÃO DAS LACUNAS DE PESQUISA

O desenvolvimento e de Estratégias formadas por técnicas computacionais integradas das áreas da Computação Forense, IA e VC aplicadas na detecção de evidências de Pornografia Infantojuvenil é um tema de pesquisa em evolução, conforme demonstra a Revisão Sistemática da Literatura (RSL) disponível na seção 2.6 deste trabalho.

Na RSL sobre Pornografia Infantojuvenil realizada neste trabalho, identificou-se um total de cinco obras que tratam de Revisões da Literatura sobre o tema da Pornografia Infantojuvenil feitas pelos autores Povedano Álvarez et al. (2023), Cifuentes; Sandoval Orozco e García Villalba (2022), Gangwar et al. (2017), Ngox et al. (2022) e Lee et al. (2020) respectivamente. Estas revisões descrevem as Estratégias existentes na literatura, bem como as principais dificuldades encontradas para detectar evidências deste tipo de crime.

As principais dificuldades para detectar evidências de pornografia infantojuvenil são: a quantidade e variedade de arquivos que pode existir em um dispositivo, lesões corporais que ao alterar o corpo da vítima, pode afetar a detecção de pessoas e a ambiguidade de contexto que pode incluir imagens naturistas e práticas de nudismo.

Já as Estratégias identificadas na literatura para detectar Pornografia Infantojuvenil são: Detecção de faces (Anda; Le-Khac; Scanlon, 2020), estimativa de idade, gênero e detecção de pornografia em geral (Macedo; Costa; Dos Santos, 2018), detecção de formas de biquini (Moreira; Fechine, 2018), detecção de cores de pele (Polastro; Da Silva Eleuterio, 2010; Salah; Othmani; Kherallah, 2022), detecção de valores hash já identificados (Sanchez et al., 2019) e a detecção de órgãos sexuais (Tabone et al., 2021). Todas estas estratégias são aplicadas em arquivos multimídia, ou seja, imagens e vídeos.

Há também as Estratégias para detectar pornografia infantojuvenil em conteúdo textual. São elas: a detecção do nome e caminho do diretório do arquivo (Al-Nabki et al., 2023) e a detecção de palavras-chave em chats de mídias sociais (NGEJANE et al., 2021).

Outro estudo que apoia o desenvolvimento deste trabalho é o desenvolvido por Al-Khater et al. (2020), que realizaram uma RSL sobre a aplicação de técnicas da Computação Forense para detectar evidências de crimes cibernéticos. Neste estudo, recomenda-se o desenvolvimento de Estratégias integrando as técnicas da Computação Forense com técnicas de outras áreas para ampliar a variedade de recursos que possam ser usados em exames periciais.

Apesar das Revisões e Estratégias citadas anteriormente, nenhum destes estudos fez o que é proposto neste trabalho, que são Estratégias formadas por técnicas integradas das áreas de Computação Forense, IA e VC para:

- Detectar imagens alteradas ou similares;
- Detectar pessoas por meio da detecção de cor de pele;
- Detectar conteúdo textual relacionado com pornografia infantojuvenil;
- Detectar objetos relacionados com pornografia infantojuvenil.

Evidencia-se então como lacuna de pesquisa na literatura acadêmica o desenvolvimento de Fenrir e suas quatro Estratégias formadas por técnicas computacionais integradas das áreas da Computação Forense, Inteligência Artificial e Visão Computacional, aplicadas na detecção de evidências de pornografia infantojuvenil em imagens digitais, para apoiar a execução de exames periciais.

Quanto as contribuições deste trabalho, para a academia são:

O desenvolvimento de Fenrir e suas Estratégias aplicadas na detecção de evidências de pornografia infantojuvenil, e assim, apoiar a execução de exames periciais. As descrições sobre o desenvolvimento e aplicação podem ser utilizadas na elaboração de novas estratégias, seja com alterações pontuais em alguma das fases, ou mesmo ao adicionar novas fases ou técnicas.

O desenvolvimento da Revisão Sistemática da Literatura na seção 2.6 deste trabalho, onde foram selecionadas 129 publicações sobre Pornografia Infantojuvenil que poderá servir de base para pesquisadores interessados neste tema.

Quanto as contribuições deste trabalho, para as autoridades policiais são:

A utilização de Fenrir para detectar evidências de pornografia infantojuvenil. Entende-se que após aplicar as devidas punições aos criminosos, a confiança dos cidadãos no sistema de justiça e nas forças policiais que trabalham para proteger a sociedade será reforçada. Este cenário ajudará a transmitir a mensagem de que as forças policiais estão ativamente combatendo crimes, e consequentemente, promovendo um sentimento de segurança e justiça.

Quanto as contribuições deste trabalho, para a sociedade e o cidadão são:

A aplicação de Fenrir poderá colaborar significativamente para a segurança e bem-estar ao garantir a proteção do público infantojuvenil, promovendo um ambiente digital mais seguro e saudável ao detectar, para que posteriormente, seja retirado da internet e de outras redes de propagação, os arquivos com pornografia infantojuvenil.

A aplicação de Fenrir poderá promover a responsabilidade digital entre os usuários na internet. Ao utilizar Fenrir para detectar evidências de pornografia infantojuvenil, conscientiza-se as pessoas sobre os riscos e possíveis medidas para acessar conteúdos seguros na internet. Isso fomenta uma cultura de vigilância no ambiente digital.

1.3. QUESTÃO DE PESQUISA

A forma com que os crimes cibernéticos evoluem faz com que a demanda por soluções que detectem evidências seja cada vez maior. No contexto da pornografia infantojuvenil, detectar evidências em um dispositivo pode ser algo complexo e exaustivo devido à quantidade e diversidade de arquivos que podem estar presente nestes dispositivos (AL-NABKI et al., 2020; ELEUTÉRIO; MACHADO, 2019).

Uma forma de detectar evidências de pornografia infantojuvenil é utilizar Estratégias formadas por técnicas integradas das áreas da Computação Forense, IA e VC (CIFUENTES; SANDOVAL OROZCO; GARCÍA VILLALBA, 2022; POVEDANO ÁLVAREZ et al., 2023).

Assim, a questão de pesquisa é explicitada a partir da seguinte indagação: “Como Estratégias formadas por técnicas computacionais integradas das áreas da Computação Forense, Inteligência Artificial e Visão Computacional aplicadas na detecção de evidências de pornografia infantojuvenil em imagens digitais apoiam a execução de exames periciais?”.

1.4. OBJETIVOS

1.4.1. OBJETIVO GERAL

O objetivo geral deste trabalho é desenvolver e aplicar Estratégias formadas por técnicas computacionais integradas das áreas da Computação Forense, Inteligência Artificial e Visão Computacional aplicadas na detecção de evidências pornografia infantojuvenil em imagens digitais, para apoiar a execução de exames periciais.

1.4.2. OBJETIVOS ESPECÍFICOS

Os objetivos específicos deste trabalho são descritos a seguir:

- Desenvolver a RSL sobre Pornografia Infantojuvenil.
- Aplicar e avaliar os algoritmos de Hash Perceptivo e as Redes Neurais de Hopfield na detecção e recuperação de valores Hash Perceptivo para detectar imagens alteradas ou similares (Estratégia A);
- Aplicar e avaliar a Detecção de cor de pele e a Floresta Aleatória na detecção de pessoas (Estratégia B);
- Aplicar e avaliar a Extração de Metadados, o OCR, a LSTM e o PLN na detecção de conteúdo textual relacionado com pornografia infantojuvenil (Estratégia C);
- Aplicar e avaliar a Detecção de Objetos, as RNCs e as RAGs na detecção de objetos relacionados com pornografia infantojuvenil (Estratégia D).

1.5. DELIMITAÇÃO DO TEMA DE PESQUISA

Foi escolhido o tema da pornografia infantojuvenil pela urgência com que este conteúdo precisa ser detectado para impedir futuras propagações. Outro fator determinante é pelo fato de ter como vítima o público infantojuvenil, um dos mais vulneráveis da sociedade.

Em relação ao apoio a execução exames periciais, esta atividade foi escolhida por ser a responsável pela detecção de evidências de crimes cibernéticos, como é o caso da pornografia infantojuvenil, realizada por autoridades policiais.

Sobre os arquivos de imagens digital, foram escolhidos por serem característicos da materialidade de pornografia infantojuvenil, juntamente com os arquivos de vídeo. Reforça-se que na literatura, os vídeos são analisados por frames, ou seja, por imagens extraídas de vídeos (LARANJEIRA DA SILVA et al., 2022).

Os temas abordados neste trabalho estão inseridos nas áreas da Computação Forense, VC e IA. Foi definido pelo desenvolvimento de Estratégias inspirado pelas revisões realizadas pelos autores Povedano Álvarez et al. (2023) e Cifuentes; Sandoval Orozco e García Villalba (2022) que sugerem a integração de técnicas de diferentes áreas para detectar evidências de Pornografia Infantojuvenil.

Quanto as áreas computacionais das técnicas selecionadas nesse trabalho, escolheu-se a Computação Forense por ser a área que possui técnicas utilizadas na detecção de evidências de crimes cibernéticos. Escolheu-se a área da VC devido ao fato das evidências de pornografia infantojuvenil estarem presentes em arquivos de imagens digitais. E escolheu-se pela área da IA para realizar tarefas que somente com as técnicas de Computação Forense e VC não seriam possíveis de serem realizadas.

Neste trabalho, foram definidas quatro Estratégias aplicadas na detecção de evidências de Pornografia Infantojuvenil. Definiu-se por estas Estratégias por serem recomendações dos autores Povedano Álvarez et al. (2023) e Cifuentes; Sandoval Orozco e García Villalba (2022).

As técnicas selecionadas para formar a Estratégia A foram as seguintes:

- *Differencial Hash* por ser uma técnica de Computação Forense específica para gerar valores Hash Perceptivo;
- Redes Neurais de Hopfield por ser uma técnica específica usada para recuperar informação.

As técnicas selecionadas para formar a Estratégia B foram as seguintes:

- Detecção de Cor de Pele por ser específica para detectar pessoas em imagens;
- Floresta Aleatória por ser uma técnica capaz de obter bons resultados sem a necessidade de preparar a base de dados a ser fornecida como entrada;

As técnicas selecionadas para formar a Estratégia C foram as seguintes:

- Extração de Metadados para conseguir extrair os metadados das imagens;
- OCR para extrair o conteúdo textual das imagens;
- LSTM por ser uma técnica comumente utilizada em conjunto com OCR para aumentar a precisão da extração do conteúdo textual das imagens;
- PLN para estruturar o conteúdo gerado pela Extração de Metadados e de conteúdo textual com OCR e LSTM;

As técnicas selecionadas para formar a Estratégia D foram as seguintes:

- Detecção de objetos por ser a técnica usada na interpretação dos componentes existentes em uma imagem;

- Redes Adversárias Generativas por ser específica para Aumento de Dados;
- Redes Neurais Convolucionais por ser comumente utilizada para detectar e localizar objetos em imagens.

Por fim, destaca-se que não foram utilizadas imagens reais de pornografia infantojuvenil neste trabalho. Como o armazenamento de arquivos contendo pornografia infantojuvenil é considerado um crime cibernético, foram utilizadas bases de dados e imagens sintéticas que se assemelham com as características destes arquivos.

1.6. ORGANIZAÇÃO DO TRABALHO

Este trabalho está organizado da seguinte forma. Além do capítulo 1, no capítulo 2, são apresentadas as seguintes seções: Computação Forense, Técnicas de Computação Forense, Visão Computacional, Inteligência Artificial, Processamento de Linguagem Natural, Árvore de Decisão e Floresta Aleatória, Redes Neurais Artificiais, Métricas Aplicadas na Avaliação do Desempenho de Técnicas de Inteligência Artificial, Crimes Cibernéticos, Pornografia Infantojuvenil, Estratégias para Detectar Pornografia Infantojuvenil e a Revisão Sistemática da Literatura sobre Pornografia Infantojuvenil.

No capítulo 3, são apresentadas as seguintes seções: Materiais e Métodos, Caracterização Metodológica, Bae de Dados e Plataforma de Ensaios, Desenvolvimento das Quatro Estratégias que Formam Fenrir, Estratégia A, Estratégia B, Estratégia C e Estratégia D. No capítulo 4, são apresentadas as seguintes seções: Apresentação e Discussão dos Resultados, Estratégia A, Estratégia B, Estratégia C e Estratégia D e no capítulo 5, é apresentada a conclusão.

2. FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, apresenta-se a fundamentação teórica dos temas abordados neste trabalho. São eles: Computação Forense, Técnicas de Computação Forense, Visão Computacional, Inteligência Artificial, Processamento de Linguagem Natural, Árvore de Decisão e Floresta Aleatória, Redes Neurais Artificiais, Métricas Aplicadas na Avaliação do Desempenho de Técnicas de Inteligência Artificial, Crimes Cibernéticos, Pornografia Infantojuvenil, Estratégias para Detectar Pornografia Infantojuvenil e a Revisão Sistemática da Literatura sobre Pornografia Infantojuvenil.

2.1. COMPUTAÇÃO FORENSE

A Computação Forense é uma área multidisciplinar que se envolve principalmente com as áreas da Ciência da Computação e da Criminalística. Seu objetivo principal é a preservação e documentação de evidências, bem como auxiliar a condução de investigações relacionadas a potenciais crimes cibernéticos (KEBANDE et al., 2020).

A base da Computação Forense é a área da Criminalística. Um dos primeiros tratados que descreve a aplicação de ciência para apoiar a criminalística, com a inclusão das áreas da física, química, microscopia, antropometria e a coleta de impressões digitais foi escrito por Hans Gross em 1947 (HUSSAIN et al., 2020).

Apesar do feito de Hans Gross, conhecido por promover a ciência na criminalística foi Edmond Locard, responsável por estabelecer o princípio de que todo contato deixa um rastro. Em síntese, todo crime deixa evidências depositadas no local de crime pelo infrator, enquanto o infrator leva consigo elementos do local do crime. Estes e outros aspectos são incorporados na área da Computação Forense (HUSSAIN et al., 2020).

No contexto dos profissionais responsáveis pela condução da investigação de crimes cibernéticos, a Lei Nº 13.964 do Código de Processo Penal define-os como perito. O perito é o responsável por conduzir a investigação, cujo objetivo é identificar materialidade de crimes cibernéticos por meio de análise de arquivos digitais, como arquivos multimídia, páginas web, códigos-fonte e contratos de propriedade intelectual (BRASIL, 2019).

O perito deve possuir conhecimento sobre Computação Forense e informática para ser capaz de conduzir uma investigação, sendo frequentemente referenciado na literatura como testemunha técnica (*Expert Witness)* (KEBANDE et al., 2020).

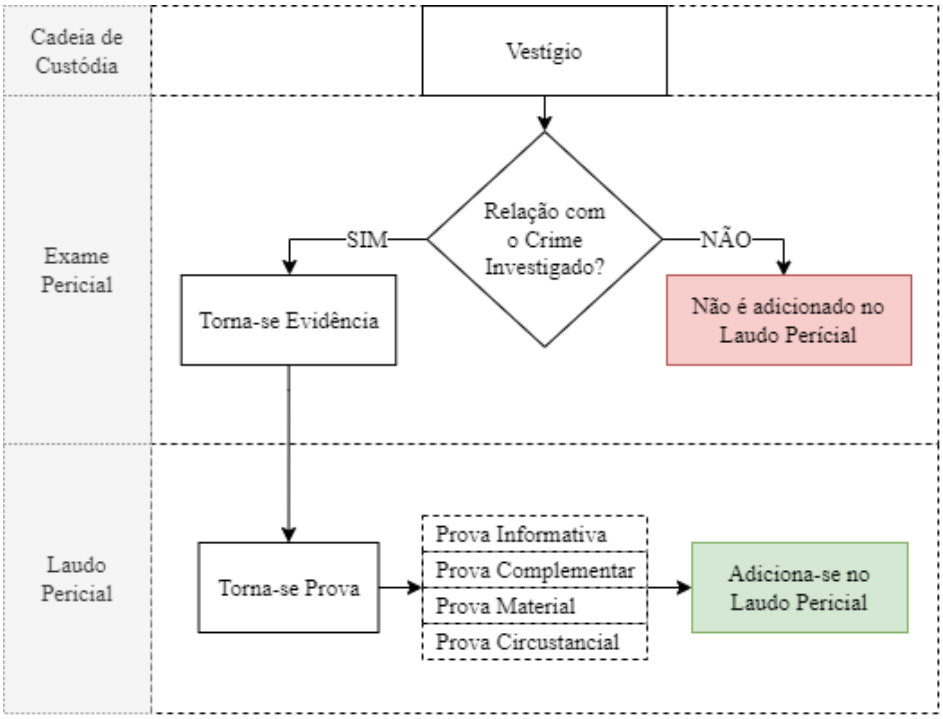
Quando uma determinada força policial é notificada sobre uma denúncia de pornografia infantojuvenil ou identifica tal ocorrência, efetua-se a apreensão dos dispositivos eletrônicos envolvidos. O ato da apreensão é descrito no capítulo 4 do Código de Processo Penal, na lei nº 3.689 de 1941, nos itens d) e e), como: “apreender armas e munições, instrumentos utilizados na prática de crime ou destinados a fim delituoso;” e “descobrir objetos necessários à prova de infração ou à defesa do réu” respectivamente (BRASIL, 1941).

A partir do momento que o perito recebe um equipamento eletrônico apreendido, cabe a ele a responsabilidade de documentar todo procedimento realizado durante a apreensão. Essa tarefa é denominada Cadeia de Custódia, definida no artigo 158º do Decreto Lei nº 3.689 do Código de Processo Penal de 03 de outubro de 1941, e incluída na Lei nº 13.964, de 2019 como “conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte” (BRASIL, 2019).

Após a conclusão da cadeia de custódia, o perito dá início ao exame pericial para dar continuidade à investigação em busca de evidências de crimes cibernéticos. É nesta fase que o vestígio coletado pode-se transformar em evidência, quando o perito consegue estabelecer uma associação com um determinado crime cibernético por meio de técnicas de Computação Forense (COSTA; NETO; JESUS, 2018; PEREIRA et al., 2019).

A indispensabilidade da realização dos exames periciais está prevista no artigo 158º do Código do Processo Penal, que diz: “Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado” (Brasil, 2019). O fluxo da análise dos vestígios, desde a cadeia de custódia, até a construção do laudo pericial é ilustrado na figura 1.

Figura 1 – Fluxo da Análise dos Vestígios



Fonte**:** Adaptado de Brasil (2019) e Elgohary, Darwish e Elkaffas (2022).

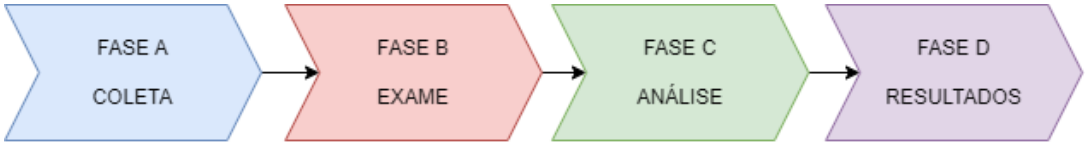
Ao analisar a figura 1, na fase inicial do fluxo da Análise dos vestígios chamada Cadeia de Custódia, os vestígios no local de crime são coletados. Em seguida, inicia-se o exame pericial para avaliar a existência de relações entre os vestígios coletados e o crime que está sob investigação. Caso positivo, o vestígio torna-se evidência, e posteriormente, prova ao ser adicionado no laudo pericial. Caso contrário, o vestígio não é adicionado no laudo pericial (ELGOHARY; DARWISH; ELKAFFAS, 2022).

Antes da inclusão das provas no laudo pericial, estas são classificadas em quatro tipos: Informativa, Complementar, Material e Circunstancial. A prova informativa refere-se a ações que ajudam no exame pericial, mas não estão documentadas, como os depoimentos de vítimas e testemunhas em interrogatórios. As provas complementares são elementos que reforçam outras provas, como por exemplo uma folha de antecedentes criminais (BRASIL, 2019).

A prova Material refere-se a vestígios produzidos ou decorrentes de conduta específica, como a produção de vídeos de pornografia infantojuvenil. Por fim, a prova circunstancial diz respeito a vestígios próximos ao possível responsável, quando, existindo a relação com o fato, pode-se inferir a existência de uma prova por indução, por exemplo encontrar alguém junto à um computador que está compartilhando pornografia infantojuvenil na internet (ELGOHARY; DARWISH; ELKAFFAS, 2022).

O exame pericial compreende quatro fases: Coleta, Exame, Análise e Resultados, conforme as normas estabelecidas pela ABNT (Associação Brasileira de Normas Técnicas) (ABNT, 2013; Mccluskey et al., 2022). É ilustrado na figura 2 as fases de um exame pericial.

Figura 2 – Principais Fases de um Exame Pericial



Fonte: Adaptado de ABNT (2013) e Mccluskey et al. (2022).

A seguir são descritas as fases do Exame Pericial ilustrado na figura 2.

– Coleta (Fase A): são identificados e isolados os equipamentos físicos e seus dados lógicos que podem possuir alguma relação com crimes cibernéticos. Em seguida, extrai-se uma cópia digital dos dados. Esta cópia digital contém todos os arquivos presentes no dispositivo eletrônico, desde arquivos multimídia até arquivos do sistema operacional.

– Exame (Fase B): são identificados e extraídos os arquivos considerados relevantes a partir da cópia digital da evidência feita na fase de coleta (A). O objetivo desta fase é extrair os arquivos que possam estar relacionados com crimes cibernéticos para serem analisados na fase posterior de análise (C). São exemplos destes arquivos: imagens, vídeos e áudios.

– Análise (Fase C): os arquivos extraídos e isolados na fase de exame (B) são analisados com o objetivo de evidenciar alguma relação com crimes cibernéticos. Para isto, o perito utiliza técnicas de diversas áreas. A extração de metadados é um exemplo desta técnica.

– Resultados (Fase D): todas informações identificadas como possíveis provas de um crime cibernético são documentadas e posteriormente, complementada com outras informações em um documento final, culminando na elaboração do Laudo Pericial.

O Exame pericial pode ser categorizado em duas abordagens: *Live-Analysis* (Ao vivo) e *Post-mortem*. Na abordagem *Live-Analysis*, o exame pericial é conduzido com o dispositivo eletrônico em funcionamento, enquanto na abordagem *Post-Mortem*, o exame é realizado com o dispositivo eletrônico desligado. A principal diferença entre as abordagens é que na Live-Analysis é possível coletar dados em transmissão e presentes na memória do dispositivo eletrônico (DÍAZ-PÉREZ et al., 2022).

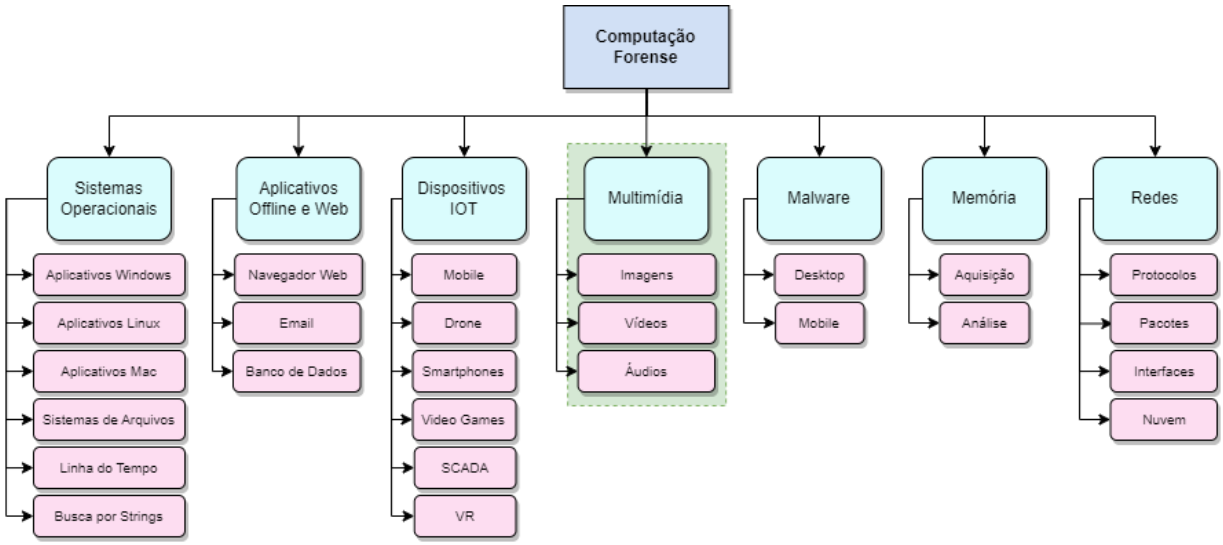
Em relação às dificuldades encontradas na execução de um exame pericial, destaca-se a quantidade e variedade de arquivos em um dispositivo eletrônico a ser periciado. O elevado número de arquivos digitais pode dificultar a detecção de evidências. Para superar este desafio e assim, reduzir o escopo de busca de arquivos a serem analisados, pode-se utilizar técnicas da área da Computação Forense para detecção de evidências de crimes cibernéticos (AL-NABKI et al., 2020; ELEUTÉRIO; MACHADO, 2019; PADILHA et al., 2021).

A seguir, são apresentados os conceitos sobre as técnicas da Computação Forense.

2.1.1. TÉCNICAS DE COMPUTAÇÃO FORENSE

A área da Computação Forense engloba diversas técnicas que fazem uso de hardware, software e bases de dados para apoiar a condução de exames periciais (Javed et al., 2022; Wu; Breitinger; O'shaughnessy, 2020). Estas técnicas podem ser aplicadas em diversos domínios da Ciência da Computação, conforme é apresentado na figura 3.

Figura 3 – Domínios da Ciência da Computação.

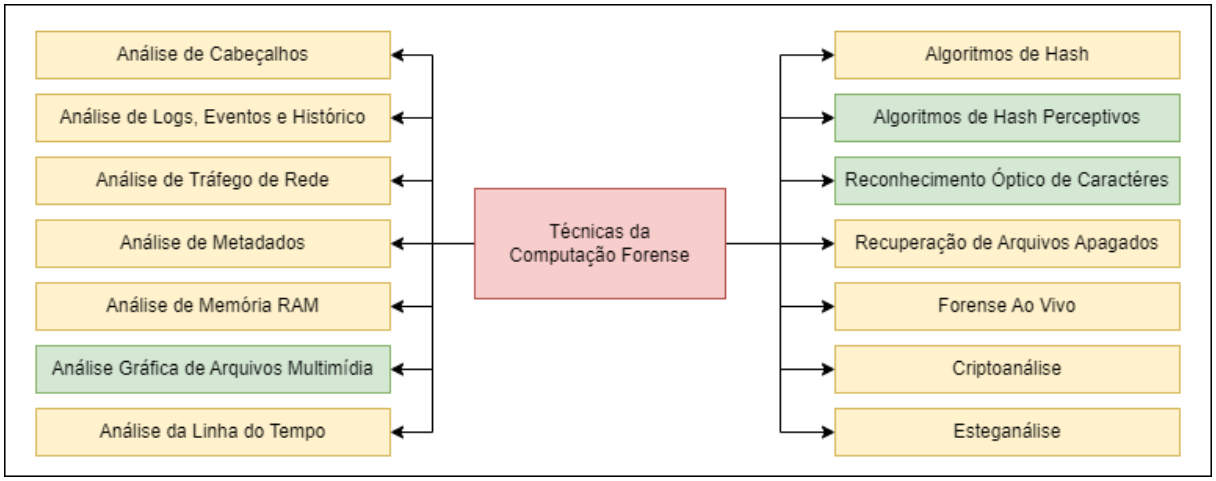


Fonte: Adaptado de Javed et al. (2022) e Wu, Breitinger e O'Shaughnessy (2020).

Na figura 3, os elementos destacados em azul representam os domínios da computação onde as técnicas de Computação Forense podem ser aplicadas. Já os itens destacados em rosa são exemplos de recursos e tarefas que possuem alguma relação com seu respectivo domínio (JAVED et al., 2022; WU; BREITINGER; O'SHAUGHNESSY, 2020).

Sobre as técnicas de Computação Forense empregadas em exames periciais, os autores Javed et al. (2022) e Wu, Breitinger e O'Shaughnessy (2020) descrevem algumas técnicas em seus estudos, todas ilustradas na figura 4.

Figura 4 – Técnicas de Computação Forense



Fonte: Adaptado de Javed et al. (2022), Mani et al. (2022) e Wu, Breitinger e O'Shaughnessy (2020).

Na figura 4, as técnicas de Computação Forense estão divididas em duas cores: Amarelo e Verde. Enquanto as técnicas destacadas na cor amarela podem ser aplicadas em diversos tipos de arquivos, as técnicas de Computação Forense destacadas na cor verde são específicas para arquivos multimídia. Destaca-se que a análise gráfica de arquivos multimídia abrange outras técnicas, como a detecção de pessoas, faces, objetos, gênero, idade, cor de pele e informações sobre o dispositivo eletrônico que gerou os arquivos multimídia (MCCLUSKEY et al., 2022).

A partir das próximas seções, são abordadas as seguintes técnicas empregadas na área da Computação Forense: Algoritmos de Hash e Algoritmos de Hash Perceptivo, Detecção de Cor de Pele, Reconhecimento Óptico de Caracteres, Extração de Metadados e Detecção de Objetos.

2.1.1.1. ALGORITMO DE HASH

O Hash é uma função matemática utilizada para resumo de dados. O algoritmo de Hash gera uma *string* denominada valor Hash, que resume o conteúdo de um determinado arquivo fornecido como entrada. A criptografia unilateral é aplicada no conteúdo do arquivo ao gerar o valor Hash. Isso significa que não é possível acessar o conteúdo original somente utilizando o valor Hash (OMRANPOUR; MOHAMMADI LEDARI; TAHERI, 2022).

O algoritmo de Hash pode ser representado por uma função H, que produz uma saída h, a partir de um valor de entrada x. A expressão matemática é definida pela equação (1):

$$h = H(x) \quad (1)$$

Cada valor Hash h é único e identifica o arquivo (x) fornecido de entrada. Se um único bit do arquivo de entrada for alterado, a saída será completamente diferente. Há exceções onde arquivos distintos possuem o mesmo valor Hash, caracterizando uma colisão de Hash. A colisão de Hash pode ser um problema, é deve ser minimizado para garantir a integridade dos arquivos (ELGOHARY; DARWISH; ELKAFFAS, 2022).

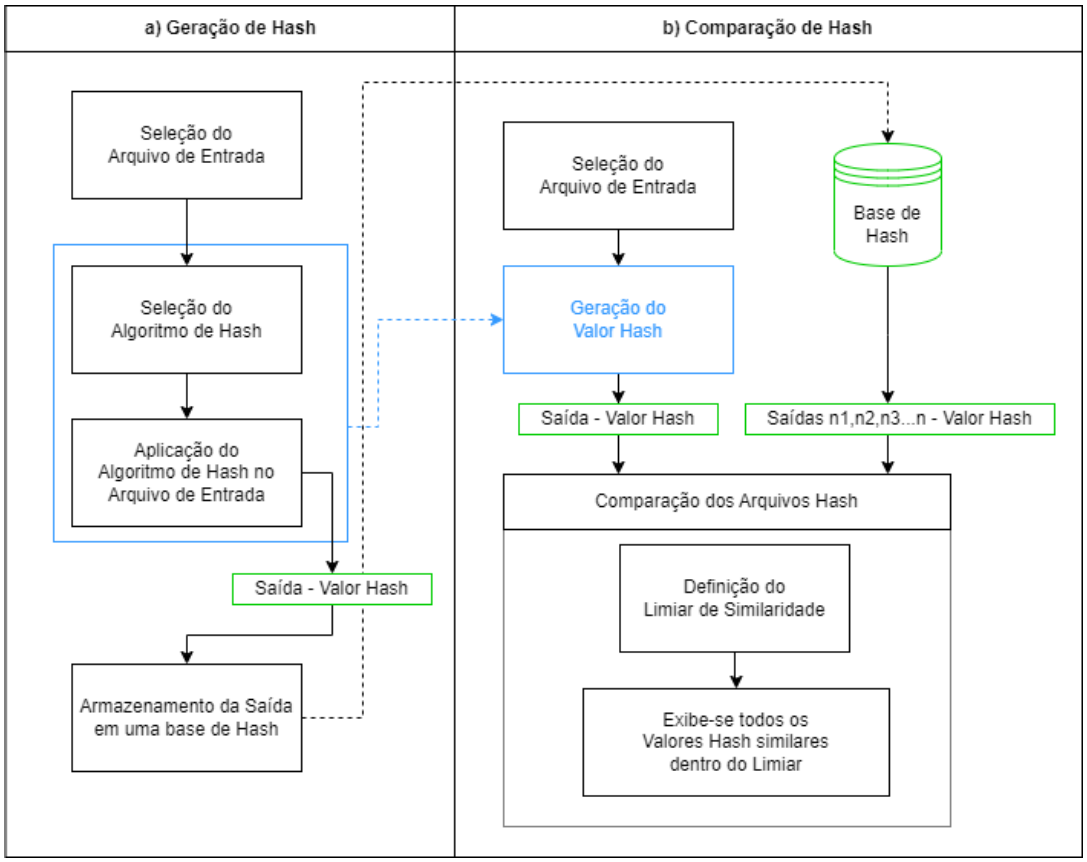
Sobre o comprimento do valor Hash, esta informação independe do tamanho do arquivo fornecido de entrada. O comprimento varia para cada algoritmo de Hash, por exemplo, os algoritmos de Hash convencionais MD5 (*Message Digest 5*) e SHA (*Secure Hash Algorithm*) nas versões SHA1, SHA256 e SHA512 produzem uma saída de 32, 40, 64 e 128 caracteres respectivamente (OMRANPOUR; MOHAMMADI LEDARI; TAHERI, 2022).

O objetivo do algoritmo de Hash é garantir a integridade de arquivos. Para isso, duas tarefas fundamentais devem ser executadas: a Geração de Hash e a Comparação de Hash. A Geração de Hash (A) tem como objetivo gerar e armazenar os valores Hash. Para isso, são selecionados os arquivos de entrada e o algoritmo de Hash que será utilizado. Em seguida, aplica-se o algoritmo de Hash no arquivo de entrada, armazenando a saída resultante em uma base de Hash (KHAIRUNNISAK; WIDODO, 2023).

A Comparação de Hash (B) visa comparar o valor Hash gerado pelo arquivo de entrada, com os valores Hash armazenados na base de Hash, a fim de encontrar valores Hash similares ou iguais. Para realizar tal comparação, seleciona-se um arquivo de entrada e gera-se o seu valor Hash. Em seguida, efetua-se a comparação deste valor Hash, com os valores Hash armazenados na base. Para direcionar a comparação, estabelece-se um Limiar de Similaridade, métrica responsável por definir a proximidade dos valores Hash comparados. Por fim, exibe-se os valores Hash dentro do limiar (KHAIRUNNISAK; WIDODO, 2023).

Ambas as tarefas: Geração de Hash (A) e Comparação de Hash (B) são apresentadas a seguir na figura 5.

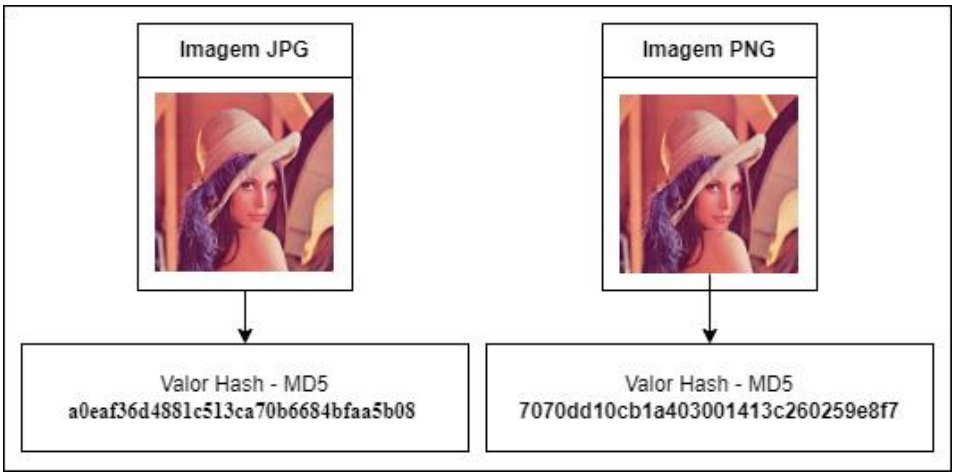
Figura 5 – Geração de Hash e Comparação de Hash



Fonte: Adaptado de Khairunnisak e Widodo (2023).

Apesar dos algoritmos de Hash serem comumente usados para assegurar a integridade de arquivos, são ineficientes para detectar arquivos semelhantes. É apresentado na figura 6 um exemplo dessa ineficiência, com dois valores Hash gerados de imagens semelhantes, diferindo apenas em sua extensão. Enquanto a primeira imagem é do tipo JPG, a segunda imagem é do tipo PNG (OMRANPOUR; MOHAMMADI LEDARI; TAHERI, 2022).

Figura 6 – Aplicação do algoritmo de Hash MD5 em Imagens Similares



Fonte: Adaptado de Omranpour; Mohammadi Ledari e Taheri (2022).

Ao analisar a figura 6, observa-se que a mesma imagem com extensões diferentes gerou valores Hash totalmente distintos. Enquanto a imagem JPG sofreu compressão com perda de dados no momento de sua geração, a imagem PNG não sofreu perda de dados em sua geração. Desta forma, não é possível relacionar o valor Hash MD5 da primeira imagem em JPG: **a0eaf36d4881c513ca70b6684bfaa5b08** com o valor Hash MD5 da segunda imagem em PNG: **7070dd10cb1a403001413c260259e8f7**.

Certas alterações em arquivos de imagens digitais causam uma mudança significativa na saída de valores Hash, mas não altera a percepção de um indivíduo ao observar a imagem. Estas alterações podem incluir ruídos, compressão, erros de transmissão, conversão de cores, recorte, alterações de escala, resolução, rotações, nos espaços de cores, nos componentes da imagem, em saturação, gama, contraste, iluminação, matiz e brilho (DU; HO; CONG, 2020).

Uma forma de identificar imagens digitais similares ou que sofreram alterações é utilizar um tipo específico de algoritmo de Hash que ao invés de calcular o valor Hash com o conteúdo de um arquivo, utiliza o conteúdo multimídia. Este tipo de Algoritmo de Hash é chamado de Hash Perceptivo, também conhecido como *"Multimídia Fingerprint*" (FARID, 2021).

2.1.1.2. ALGORITMO DE HASH PERCEPTIVO

O Hash Perceptivo é um tipo de algoritmo de Hash que baseia-se no conteúdo multimídia de arquivos, como o valor das cores dos pixels em imagens digitais. Isso garante que alterações não significativas feitas no conteúdo multimídia das imagens digitais não alterem totalmente o seu valor Hash (DU; HO; CONG, 2020; FARID, 2021).

Os estudos de Du, Ho e Cong (2020) e Hamadouche et al. (2021) listam os principais algoritmos de Hash perceptivo, incluindo o *Average Hash*, *Perceptual Hash*, *Differential Hash*, *Wavelet Hashing* e *Crop-resistance Hash*. Os tipos de algoritmos de Hash perceptivos são descritos na tabela 1.

Tabela 1 – Tipos de Algoritmos de Hash Perceptivo

Tipo	**Descrição**
Average Hash (aHash)	Baseado em estatística. inicialmente, converte-se a imagem para a escala de cinza, e a reduz para um tamanho fixo. Feito isso, gera-se um valor binário baseando-se no valor médio dos pixels. Em seguida, seleciona-se e mantém as frequências abaixo da média dos pixels, interpretando-as como estrutura da Imagem e descarta-se as frequências acima da média dos pixels.

Tipo	Descrição
Perceptual Hash (pHash)	Baseado em relações, trata-se de uma extensão do aHash. Utiliza a Transformada Discreta de Cosseno (DCT) antes do descarte das frequências acima da média dos pixels com o objetivo de obter informações mais sensíveis, que outrora seria descartada na execução do aHash.
Differential Hash (dHash)	Baseado em estatística, possui uma lógica similar ao aHash e pHash. As fases de conversão da imagem para a escala de cinza e cálculo do binário permanecem, com a exceção de que os valores selecionados para o cálculo não são mais extraídos da média dos pixels, e sim pela diferença entre os pixels adjacentes.
Wavelet Hash (wHash)	Baseado em relações, seu funcionamento é similar ao dHash. Mantem as fases de conversão da imagem para a escala de cinza e cálculo do binário. Mas neste algoritmo de Hash, extrai-se as informações com a Transformada Discreta de Wavelet (DWT). Outra diferença, é que o wHash descarta as frequências mais baixas, e mantém somente as informações de contraste.
Crop-resistant Hash (cpHash)	Baseando em Relações, o algoritmo cpHash segmenta a imagem original em outras sub-imagens, sempre recortando 5% das bordas a cada nova imagem gerada. Essa tarefa é realizada até a última sub-imagem estiver próxima do 50% da imagem original. Em cada uma das sub-imagens, é feita a conversão para a escala de cinza, e a Transformada de Watershed (STEINEBACH; LIU; YANNIKOS, 2014).

Fonte**:** Adaptado de Du, Ho e Cong (2020) e Hamadouche et al. (2021).

Quanto a sua aplicação, o Hash perceptivo pode ser utilizado para detectar alterações em imagens (Alkhowaiter; Almubarak; Zou, 2022; Samanta; Jain, 2021; Wang et al., 2021), identificar imagens duplicadas (Chen; Xiang; Sun; 2021), detectar faces (Jain et al., 2023) avaliar a qualidade de imagens (Yu, et al., 2022), reconhecer arquivos na Dark Web (Biswas et al., 2021) e detectar evidências de pornografia infantojuvenil (STRUPPEK et al., 2022).

Sobre a detecção de evidências de pornografia infantojuvenil com Hash perceptivo, as companhias de destaque na área da tecnologia como: Apple, Microsoft e Facebook possuem aplicações baseadas em Hash perceptivo para proteger suas plataformas, são elas: NeuralHash, PhotoDNA e Facebook’s PDQ respectivamente (STRUPPEK et al., 2022).

Uma tarefa relevante realizada pelo Hash perceptivo é a recuperação de conteúdo visual em imagens digitais. Contudo, para recuperar um valor Hash de arquivos de imagens digitais visando a comparação e detecção de imagens similares ou imagens iguais que sofreram alterações, o algoritmo de Hash perceptivo por si só não é suficiente. Uma solução é combiná-lo com técnicas da Inteligência Artificial (IA) para recuperação de informação (AL-THANI et al., 2022; MEENALOCHINI et al., 2018; SABAHI; OMAIR AHMAD; SWAMY, 2018).

Para avaliar os valores Hash gerados pelos algoritmos de Hash perceptivo, é utilizado o limiar de similaridade. O Limiar de similaridade é responsável por definir o quão próximo uma imagem está de outra imagem, para serem consideradas similares. As métricas que podem ser

utilizadas como Limiar de Similaridade são: Distância Euclidiana, Distância de Manhattan, Distância de Minkowski e a Distância de Hamming (Du; Ho; Cong, 2020), todas descritas na subseção 2.3.4 deste trabalho.

2.1.1.3. DETECÇÃO DE COR DE PELE

A detecção de cor de pele é uma técnica multidisciplinar inserida nas áreas da Visão Computacional (VC) e Computação Forense, utilizada para detectar a presença de pessoas em arquivos multimídia. Sua aplicação abrange diversos cenários, como a estimativa de idade, a detecção de nudez, a identificação de expressões faciais, o controle de conteúdo armazenado em plataformas na internet. Sua utilização inclui desde a detecção de suspeitos em um local de crime, até potenciais vítimas (MOREIRA; FECHINE, 2018; REJÓN PIÑA; MA, 2023).

Sobre o funcionamento da técnica de detecção de cor de pele, ao receber uma imagem como entrada, é feita uma classificação das cores dos pixels em cor de pele e não cor de pele. Para realizar essa classificação, são consideradas as informações sobre o espaço de cores da imagem de entrada, como o RGB (SALAH; OTHMANI; KHERALLAH, 2022).

No âmbito do combate ao crime cibernético, a detecção de cor de pele pode apoiar a detecção dos indivíduos envolvidos, sejam eles suspeitos, testemunhas ou vítimas. A detecção de cor de pele otimiza a busca por evidências ao torná-la automática, para assim, reduzir o campo de pesquisa a um subconjunto de arquivos que contenham cor de pele em seu conteúdo multimídia (LY et al., 2020; ZHU; SANG; HE, 2022).

Apesar de suas vantagens, a detecção de cor de pele em imagens digitais possui uma série de limitações relacionadas à iluminação e resolução da imagem, espaços de cores, ruídos, filtros e a ampla gama de cores de pele (SESHADRI SASTRY; MADHUSUDHANA RAO; PRAVEEN CHAKRAVARTHY, 2018; ZHU; SANG; HE, 2022).

Para superar essas limitações e aprimorar seu desempenho, alguns estudos recomendam a utilização de outros espaços de cores e a combinação da detecção de cor de pele com técnicas da IA. Essa combinação possibilita aprender com um conjunto de dados sobre cor de pele, e assim, adaptar-se bem a diferentes limitações que possam vir a surgir ao receber novas imagens para detectar cores de pele (GANESAN et al., 2023; NASREEN et al., 2023).

Uma abordagem complementar à detecção de cor de pele, é a segmentação por cor de pele. Enquanto a detecção de cor de pele tem como objetivo detectar os pixels com cor de pele, a segmentação de cor de pele consiste na criação de uma máscara da mesma dimensão da imagem fornecida como entrada. Esta máscara é composta por *pixels* preenchidos com as cores preta e branca. Enquanto a cor branca destaca os pixels detectados como cor de pele, a cor preta é atribuída para todos os pixels restantes (Ding; Liu; Lei, 2023; Ly et al., 2020). É ilustrado na figura 7 um exemplo de segmentação de cor de pele.

Figura 7 – Exemplo de segmentação de cor de pele

Fonte: Adaptado de Ding, Liu e Lei (2023) e Ly et al. (2020).

A segmentação de cor de pele pode ser utilizada no pré-processamento de imagens para apoiar a realização de diversas técnicas, como a detecção de faces e a estimativa de idade. Além disso, a segmentação de cor de pele é utilizada para avaliar qualitativamente a qualidade de uma tarefa de detecção de cor de pele, ao observar se as regiões com cor de pele foram separadas corretamente das regiões de plano de fundo da imagem (YOU et al., 2023).

Sobre a avaliação de desempenho da técnica de detecção de cor de pele, utiliza-se as métricas: Matriz de Confusão, Precisão, *Recall*, *F-Score* e Curva ROC (*Receiver Operating Characteristics*) (Nasreen et al., 2023), todas descritas na subseção 2.3.4 deste trabalho.

2.1.1.4. RECONHECIMENTO ÓPTICO DE CARACTERES

O Reconhecimento Óptico de Caracteres ou OCR (*Optical Character Recognition*) é uma técnica usada para extrair o conteúdo textual de uma imagem, por meio da identificação de caracteres. Outra definição é que OCR pode ser entendido como uma técnica que converte texto impresso ou manuscrito em texto legível por máquina (GUPTA; KUMAR, 2020).

OCR é uma técnica multidisciplinar que faz parte das áreas da Computação Forense e VC. As primeiras aplicações desenvolvidas para OCR utilizavam métodos baseados em regras e em reconhecimento de padrões para extrair o conteúdo textual de imagens, seja ele impresso ou manuscrito. Estudos mais recentes mostram as técnicas de OCR combinadas com técnicas da IA (ALGHYALINE, 2023; PATEL, 2021).

O funcionamento do OCR é composto por três fases: Entrada, Extração e Saída (Akhtar et al., 2023). O funcionamento do OCR é ilustrado na figura 8.

Figura 8 – Funcionamento do OCR

Adaptado de Akthar et al. (2023)

A figura 8 apresenta a execução do OCR composta pelas fases de entrada, extração e saída. Na fase de entrada, ao receber uma imagem, identifica-se frases, palavras e caracteres por meio de um conjunto de regras e algoritmos de reconhecimento de padrões. Na fase de extração, identifica-se o conteúdo textual por meio de uma combinação e comparação de formas e caracteres, além de bases de dados com textos dos mais variados idiomas e símbolos. Finalmente, na fase de saída, o texto reconhecido é extraído e convertido em formato digital editável (AKHTAR et al., 2023; AVYODRI; LUKAS; TJAHYADI, 2022).

São exemplos de aplicação de OCR, a leitura de cheques bancários, o desenvolvimento de sistemas de leitura para pessoas com deficiência visual, o reconhecimento de impressões e assinaturas digitais, a detecção de placas de veículos e o reconhecimento de marcas d'água (ALGHYALINE, 2023; PATEL, 2021; SULTAN et al., 2023).

Sobre à aplicação de OCR no combate à crimes cibernéticos, sua utilização é essencial em tarefas como exames periciais para encontrar evidências em arquivos multimídia devido a sua capacidade de extrair conteúdo textual de forma automática (Memon et al., 2020; Pant et al., 2023; Vezeteu et al., 2019). Sobre suas limitações, pode-se citar o tamanho da fonte, idioma, estilo, luminosidade, além de caracteres distorcidos e manuscritos (AKHTAR et al., 2023).

Uma forma de superar as limitações do OCR é utilizá-lo em conjunto com Processamento de Linguagem Natural (PLN) e técnicas da IA. Esta combinação permite que, além de detectar e extrair o conteúdo textual de arquivos multimídia, também sejam feitas outras tarefas, como interpretação, sumarização, análise de sentimentos e semânticas, modelagem de tópicos e agrupamento de palavras por similaridade (KHAN; NAZIR; KHAN, 2023).

Para avaliar a técnica de OCR é utilizada a medida da acurácia. Esta acurácia pode ser quantificada ao comparar o texto reconhecido com OCR com o texto original. As métricas que podem ser utilizadas como acurácia são: Taxa de Erro de Palavras (WER) e a Taxa de Erro de Caracteres (CER) (Mulyanto; Hartati; Wardoyo, 2022), todas descritas na subseção 2.3.4 deste trabalho.

2.1.1.5. EXTRAÇÃO DE METADADOS

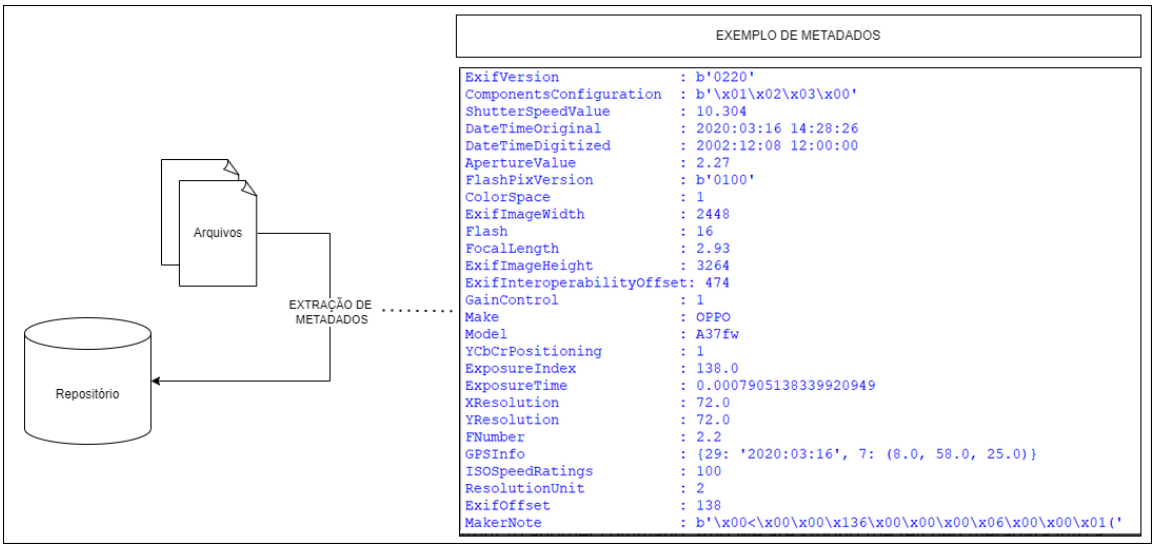
A extração de metadados é uma técnica da Computação Forense utilizada para extrair informações de arquivos em um dispositivo eletrônico. Estas informações abrangem desde sua origem, como data e hora de criação, até o histórico de suas alterações. Extrair metadados permite esclarecer quais usuários interagiram com um determinado arquivo, além de quando, como e onde foram feitas estas interações (DU; SCANLON, 2019).

Os metadados, também chamados de “dados ocultos” ou “dados sobre dados”, são os dados intrínsecos dos arquivos, que podem conter informações sobre: data de criação, tipo, extensão, tamanho, autor, alterações, se houve compressão, anotações e geolocalização. Obter estas informações é essencial para entender o contexto de um arquivo armazenado em um dispositivo eletrônico (CHAVAN; JADHAV; BORKAR, 2020).

A extração de metadados depende dos softwares utilizados. Geralmente, a extração é feita por softwares específicos de recuperação de dados ou automações customizadas. Para extrair os metadados, estes softwares analisam a estrutura e o formato do arquivo, para em seguida, coletar todos os metadados e armazená-los em um repositório (BLANCHY et al., 2023).

Em relação aos arquivos que podem ter metadados extraídos, não há nenhuma exceção. Todo arquivo armazenado em um dispositivo eletrônico em uma plataforma na internet possui metadados, e estes podem ser extraídos (Mani et al., 2022). O funcionamento da Extração de Metadados é ilustrada na figura 9.

Figura 9 – Funcionamento da Extração de Metadados



Adaptado de Mani et al. (2022)

São exemplos de aplicações da extração de metadados: investigar crimes cibernéticos, analisar arquivos multimídia, classificar artigos científicos, testar valores de coordenadas e geolocalização (BOUKHERS; BOUABDALLAH, 2022; LAPARRA et al., 2023).

Extrair metadados é uma das principais técnicas usadas em uma investigação de crime cibernético. Isso porque as informações extraídas dos metadados permitem estabelecer uma relação entre o arquivo digital e o crime cibernético. Essa relação abrange as motivações, os métodos usados, a extensão e o alcance do crime, além das possíveis vítimas (GRIGALIUNAS; BRUZGIENE; VENCKAUSKAS, 2023).

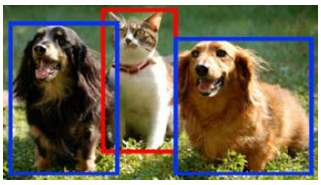
Quanto às limitações da extração de metadados, os principais desafios encontram-se na estruturação do resultado da extração. Os metadados extraídos podem ser de diversos tipos, formatos e tamanhos. Uma forma de estruturar estes metadados é utilizar as técnicas de PLN e IA (BLANCHY et al., 2023; LAPARRA et al., 2023).

Para avaliar a técnica de Extração de metadados, pode-se utilizar as mesmas métricas citadas para a técnica de OCR. São elas a Taxa de Erro de Palavras (WER) e a Taxa de Erro de Caracteres (CER) (Mulyanto; Hartati; Wardoyo, 2022), todas descritas na subseção 2.3.4 deste trabalho.

2.1.1.6. DETECÇÃO DE OBJETOS

A detecção de objetos é a técnica responsável por detectar e localizar objetos em arquivos multimídia, como vídeos e imagens digitais. Seu objetivo é ajudar na interpretação dos objetos de um determinado cenário ao detectá-los e classificá-los (Diwan; Anirudh; Tembhurne, 2023; Jain et al., 2020). Importante destacar as principais diferenças entre a classificação, localização, detecção e segmentação de objetos. Um exemplo de cada é ilustrado na figura 10.

Figura 10 – Classificação, localização, detecção e segmentação de objetos

Único Objeto		**Múltiplos Objetos**	
Classificação	Classificação + Localização	Detecção	Segmentação
			
GATO	**GATO**	**CÃO, GATO**	**CÃO, GATO**

Adaptado de Diwan; Anirudh; Tembhurne (2023) e Sharma e Mir (2020).

Ao analisar a figura 10, percebe-se que na classificação, busca-se identificar a existência de um objeto em uma imagem. Neste caso, não importa onde o objeto está posicionado. Na classificação e localização, utiliza-se uma região retangular para identificar um objeto em uma imagem. Na detecção de objetos, utiliza-se a região retangular para identificar a existência e a posição de múltiplos objetos de diferentes classes. Por fim, na Segmentação de objetos, busca-se identificar a existência, a forma e a posição de múltiplos objetos (SHARMA; MIR, 2020).

Sobre seu funcionamento, a técnica de detecção de objetos pode ser classificada em dois tipos: Modelo de Estágio Único e Modelo de Dois Estágios (Almeida, 2020). É descrito na tabela 2 os Modelos de Estágio Único e Modelo de Dois Estágios.

Tabela 2 – Modelos de estágio único e Modelo dois estágios

Modelo	**Descrição**
Modelo de Estágio Único	Neste modelo não é necessário um estágio inicial de extração. Trata-se de modelos mais poderosos que permitem dividir a imagem em sub-imagens, sendo que cada uma destas sub-imagens possui um único objeto. Apesar de mais simples, o modelo de Estágio Único apresenta melhores resultados na detecção de objetos do que em modelos em de Dois Estágios. Um exemplo de modelo de estágio único é o YOLO (*You Only Look Once*).

Modelo	Descrição
Modelo de Dois Estágios	Neste modelo, existe um estágio inicial, chamada de extração de regiões de interesse (*Region Proposal*) antes de detectar os objetos de uma imagem. Neste primeiro estágio, as técnicas: Janela Deslizante (*Sliding Window*) e Busca Seletiva (*Selective Search*) podem ser usadas. Sua principal vantagem é sua capacidade de identificar objetos em diferentes escalas com elevada acurácia. Já sua principal desvantagem é a aplicação em tempo real, devido as suas limitações sobre o tempo de processamento. São exemplos deste modelo as técnicas de R-CNN (*Region-based - Convolutional Neural Networks*), *Fast R-CNN* e *Faster R-CNN*.

Fonte**:** Adaptado de Almeida (2020).

A detecção de objetos está presente em diversas aplicações. Pode-se citar como exemplo os sistemas de vigilância, veículos autônomos, visão robótica, a inspeção de alimentos e a interpretação de imagens médicas, como ressonâncias (KINRA; WALIA; SHARANYA, 2023).

Além das possíveis aplicações para a técnica de detecção de objetos já mencionadas, ressalta-se a importância desta técnica para a área da Computação Forense. Detectar objetos pode servir de base para o desenvolvimento de outras técnicas que necessitem interpretar informações visuais e assim, identificar informações relevantes e transformá-las em evidências. São exemplos de aplicações de detecção de objetos para a área da Computação Forense a análise de cenas de crime e a detecção de armas de fogo (JAIN et al., 2020; ZOU et al., 2023).

Quanto a aplicação da técnica de detecção de objetos para combater o crime cibernético de pornografia infantojuvenil, os estudos publicados na literatura concentram-se na detecção de faces, na estimativa de idade e na detecção de conteúdo pornográfico em geral. Autores como Anda, Le-Khac e Scanlon (2020), Wiratama et al. (2017) e Tahir et al. (2023) apontam em seus estudos a necessidade do desenvolvimento de novas Estratégias com a detecção de objetos para combater a pornografia infantojuvenil. Como sugestão, os autores mencionam a detecção de objetos e símbolos que possam ter alguma relação com este crime cibernético.

Sobre as limitações da técnica de detecção de objetos, uma parte considerável reside na identificação dos objetos e na interpretação dos cenários de fundo. Os cenários podem ser os mais diversos e complexos possíveis. Além disso, o cenário e os objetos podem conter filtros, ruídos, além de possuírem diferentes escalas, cores, posições e iluminações (ZOU et al., 2023).

Estas limitações mantém a técnica de detecção de objetos no estado da arte. Os estudos sobre detecção de objetos propõem a sua combinação com técnicas da IA para superar essas limitações. Dentre as principais técnicas da IA que podem ser utilizadas, destacam-se as Redes Neurais Artificiais (RNAs) (KINRA; WALIA; SHARANYA, 2023; SHARMA; MIR, 2020).

Outra técnica que pode ser usada para melhorar o desempenho da técnica de detecção de objetos é o Aumento de Dados (*Data Augmentation*). O aumento de dados irá gerar novos objetos sintéticos realistas, variados de um objeto original. Estes novos objetos possibilitam superar limitações impostas pela falta de imagens para treinamento. Estes objetos gerados por aumento de dados podem contemplar rotações aleatórias, inversões, aplicações de filtros e alterações de escalonamento (NIE et al., 2022; WANG et al., 2020).

Para avaliar a técnica de detecção de objetos, podem ser utilizadas as seguintes métricas: Matriz de Confusão, Precisão, *Recall*, *F-Score*, Curva ROC, Intersecção sobre União ou IoU (*Intersection Over Union*) e a distância de Hausdorff (Chau et al., 2023; Jain et al., 2020), todas descritas na subseção 2.3.4 deste trabalho.

A próxima seção fundamentará a área da Visão Computacional (VC), Processamento de Imagens Digitais (PID) e Imagens Digitais.

2.2. VISÃO COMPUTACIONAL

A Visão Computacional (VC) é a subárea da Ciência da Computação responsável por analisar, interpretar e extrair informações de imagens digitais. A área da VC tem por objetivo desenvolver sistemas de Processamento de Imagens Digitais (PID) capazes de simular a visão humana e manipular imagens digitais (GONZALEZ; WOODS, 2009; WAELEN, 2023).

Segundo os autores Luo, Wang e Zhang (2021) e Matsuzaka e Yashiro (2023) a área da VC possui componentes fundamentais que são utilizados para o desenvolvimento de sistemas de PID. Estes componentes, juntamente com suas descrições, são apresentados na Tabela 3.

Tabela 3 – Principais componentes da área da VC

Componentes	**Descrição**
Cor	A cor pode ser definida como uma percepção visual resultante da interação de um objeto com a luz.
Resolução Temporal	Trata-se de capacidade de capturar e representar mudanças ou eventos em um determinado tempo.
Resolução Espacial	Trata-se do nível de granularidade no domínio espacial de uma imagem ou sinal. Quanto maior a granularidade, maior a qualidade da imagem. Em geral, a métrica usada para medir a resolução espacial é a Pontos por Polegada ou DPI (*Dots per Inch*).
Captura ou Aquisição de Imagens	Processo de aquisição de imagens realizada por algum mecanismo, como: Scanners, Digitalizadores de Sinal de Vídeo e Câmeras.

Componentes	Descrição
Análise Gráfica	Trata-se da utilização de técnicas para explorar, visualizar e interpretar dados por meio de representações gráficas, como gráficos, histogramas, diagramas, entre outros. A análise gráfica possibilita identificar tendências, correlações, distribuições, reconhecer padrões e outras características essenciais de imagens de modo a facilitar a interpretação de imagens e seus componentes.
Pré-processamento de Imagens	Trata-se do tratamento prévio realizado em uma imagem com o objetivo de aumentar a probabilidade de sucesso nas tarefas posteriores.
Processamento de Imagens Digitais (PID)	Processo responsável pela manipulação de imagens digitais por meio de algoritmos e técnicas computacionais para atingir um determinado objetivo.

Fonte: Adaptado de Luo, Wang e Zhang (2021), Matsuzaka e Yashiro (2023).

Todos os principais componentes de relacionados com a área da VC descritos na tabela 3 estão relacionados com Imagens Digitais, sendo este, o principal objeto de estudo da área (LUO; WANG; ZHANG, 2021; MATSUZAKA; YASHIRO, 2023).

A imagem digital pode ser definida como uma função bidimensional, representada por $f(x, y)$, onde x e y são coordenadas espaciais discretas em uma grade retangular. O valor de f caracteriza a amplitude para qualquer coordenada. Também chamada de nível ou intensidade de cinza, a função $f(x, y)$, tem tamanho finito e é responsável por definir a intensidade da coordenada (LIN et al., 2018; VOULODIMOS et al., 2018).

Uma imagem digital, juntamente com suas coordenadas espaciais e um exemplo de coordenada com valores aleatórios representada por $f(x, y)$ é ilustrada na figura 11.

Figura 11 – Exemplo de uma Imagem digital

Fonte: Adaptado de Lin et al. (2018) e Voulodimos et al. (2018).

A imagem ilustrada na figura 11 pode ser interpretada como uma matriz (x, y), e cada uma de suas coordenadas é chamada pixel (*Picture Element*). O valor de cada pixel pode variar entre 0 e 255, sendo 0 a representação da cor mais escura (preta) e 255 a representação da cor mais clara (branca). Assim, pode-se entender a topologia de um pixel como quadrados alinhados, um ao lado do outro, formando a matriz (x, y), também encontrada na literatura de grade (*grid*) (FAN et al., 2021; STÖHR, 2023).

Três exemplos da mesma imagem com cores diferentes são ilustrados na figura 12. A imagem binária (a) é classificada como monocromática, pois seus pixels possuem uma única cor com diversas intensidades. Já as imagens em níveis de cinza (b) e colorida (c) são classificadas como policromáticas por possuírem mais de uma cor.

Figura 12 – Exemplos de imagens binária (a), em níveis de cinza (b) e colorida (c)

(a) Binária (b) Níveis de Cinza (c) Colorida

Fonte: Adaptado de Fan et al. (2021) e Stöhr (2023).

Na figura 12, há três imagens com colorações diferentes: binária (a), em níveis de cinza (b) e colorida (c). Na imagem binária (a) os valores dos pixels assumem os valores 0 ou 255 somente. Já na imagem em níveis de cinza (b), os pixels podem assumir qualquer valor em um intervalo de 0 a 255 (GONZALEZ; WOODS, 2009; SABER; KHAN; MEJBEL, 2020).

No caso da imagem colorida (c), trata-se de três ou quatro matrizes $f(x, y)$ sobrepostas, a depender do sistema de cores. Cada matriz possui os seus respectivos pixels que podem assumir um valor dentro do intervalo de 0 a 255. Isto significa que o pixel na posição $f(x, y)$ será representado por n valores, sendo n o total de matrizes sobrepostas. Estas matrizes são chamadas de bandas. São exemplos de espaços de cores: o RGB, CMY, CMYK, Xyz, Yxy, Yiq, HSV, HSL, YCbCr, CIE L*a*b, CIE L*c*h e CIE L*u*v, sendo o RGB o mais utilizado por dispositivos eletrônicos para produzir imagens digitais (KOREN IVANČEVIĆ et al., 2023).

Sobre a produção e armazenamento de imagens digitais, seus arquivos são gerados por meio de softwares configurados em dispositivos eletrônicos como scanners e câmeras. Em relação ao armazenamento dos arquivos, as imagens podem estar armazenadas com diversas extensões, como: JPEG (*Joint Photographic Experts Group*), BMP (*Bitmap*), PNG (*Portable Network Graphics*), TIFF (*Tagged Image File Format*), GIF (*Graphics Interchange Format*) e PDF (*Portable Document Format*) (FAN et al., 2021; MULLAN; RIESS; FREILING, 2019).

É essencial compreender sobre a extensão e o espaço de cores de imagens digitais para usar e desenvolver técnicas, métodos e algoritmos de PID corretamente. Estas informações estão diretamente relacionadas com a estrutura do arquivo da imagem digital (WAELEN, 2023). São descritas na tabela 4 exemplos de técnicas utilizadas para PID.

Tabela 4 – Exemplos de Técnicas utilizadas para PID

ID	**Técnica**	**Descrição**
01	Aprimoramento	Utilização de Algoritmos para melhorar a qualidade visual da imagem.
02	Restauração	Remoção ou redução das degradações presentes em uma imagem.
03	Compressão	Redução dos dados para redução de tamanho
04	Segmentação	Divisão da imagem em regiões de interesse pré-determinadas.
05	Detecção de Objetos	Identificação e Classificação de objetos em uma imagem.
06	Morfologia	Manipulação de formas e estruturas presentes em uma imagem
07	Autenticação	Identificação de manipulações intencionais ou não em imagens.
08	Processamento de Cores	Manipulação das cores dos pixels nas imagens.
09	Fusão	Combinação de múltiplas imagens para formar uma única imagem.
10	Granulometria	Medição da distribuição dos objetos com uma determinada textura
11	Extração de Características	Extração de recursos e padrões considerados relevantes em uma imagem.
12	Análise de Componentes	Determinação e Análise de bordas, objetos e regiões de uma imagem por meio da análise das cores dos pixels e seus vizinhos.
13	Limiarização	Separação das cores dos pixels em duas classes distintas (1 e 0). Dentre as principais técnicas para limiarização, destaca-se o método proposto por Otsu (OTSU, 1979).

Fonte**:** Adaptado de Waelen (2023).

A próxima seção fundamentará a área da Inteligência Artificial (IA) e sua subárea, o Processamento de Linguagem Natural (PLN).

2.3. INTELIGÊNCIA ARTIFICIAL

A Inteligência Artificial (IA) é uma subárea da Ciência da Computação responsável por desenvolver sistemas inteligentes capazes de resolver problemas complexos e, assim, auxiliar na tomada de decisão (ANEJA; CHANG; OMURO, 2019; MCKINNEL et al., 2019).

A área da IA possui inúmeras técnicas que podem ser utilizadas para apoiar na tomada de decisão e na realização de tarefas complexas. Estas tarefas podem incluir: regularização, regressão, agrupamento, classificação e associação. Na literatura, é comum encontrar as técnicas de IA referenciadas como algoritmos de Aprendizagem de Máquina (AM) (DUNSIN et al., 2023; KOOSHA; MAHYAR, 2023; MIJWIL; SALEM; ISMAEEL, 2023).

São exemplos de aplicações onde a IA pode ser usada na detecção e análise de evidências de crimes cibernéticos: a descoberta de padrões de comportamento, a extração de informações ocultas em arquivos, a descoberta de atividades ilícitas em tráfegos de rede, a reconstrução de cenas de crime e a detecção de vítimas e criminosos em arquivos multimídia (MOHAMMAD; ALQAHTANI, 2019; OLADIPO et al., 2020).

Sobre a utilização de técnicas da IA em conjunto com técnicas de Computação Forense e VC para combater a pornografia infantojuvenil, os autores Kloess, Woodhams e Hamilton-Giachritsis (2021) e Ngejane et al. (2021) reforçam a necessidade do desenvolvimento de novos estudos envolvendo técnicas e Estratégias que viabilizem uma maior precisão para detectar evidências.

2.3.1. PROCESSAMENTO DE LINGUAGEM NATURAL

O Processamento de Linguagem Natural (PLN) é uma subárea da IA responsável pela análise, processamento, produção e reconhecimento de textos e falas em linguagem humana, considerando diferentes aspectos de gramática, semântica, pragmática e morfologia. Para isso, relaciona-se com outras áreas além da IA, como a Linguística, Estatística, Psicologia e a Matemática (MONTASARI, 2023).

As primeiras publicações sobre PLN datam da década de 1950, inicialmente como um sistema de tradução automática. A partir deste momento, a evolução da área fez com que PLN fosse aplicado para diversos setores, como negócios, saúde, finanças, recrutamento, comércio, esportes, energia, meio ambiente, computação forense e segurança da informação (PRAVEEN GUJJAR; PRASANNA KUMAR; GURU PRASAD, 2023).

A aplicação de PLN na área da Computação Forense permite um ganho de desempenho significativo na detecção de evidências de crimes cibernéticos. Sua aplicação engloba dispositivos eletrônicos, mídias sociais, nuvem e dispositivos de armazenamento removíveis, como HDs e Pen Drives (MONTASARI, 2023).

Dentre os principais objetivos que podem ser alcançados por meio da combinação de PLN e Computação Forense na identificação evidências de crimes cibernéticos, pode-se citar a análise semântica de conteúdo textual, a classificação e agrupamento de palavras e textos, a recuperação e estruturação de palavras, e a detecção de URLs maliciosas, mensagens de Spam e *Phishings* (Ukwen; Karabatak, 2021). As principais técnicas e tarefas de PLN que podem ser aplicadas na área da Computação Forense são apresentadas na tabela 5.

Tabela 5 – Principais técnicas e tarefas de PLN utilizadas na área da Computação Forense

Item	**Tipo**	**Descrição**
Stemização	Técnica	Consolidação de diferentes variações de palavras que usam o mesmo radical em uma forma raiz comum. Por exemplo, as palavras “Gosto” e “Gostei” serão simplificadas para "Gost".
Sumarização	Tarefa	Produção de um resumo contendo os tópicos e as informações mais relevantes a partir de um texto fornecido como entrada.
Produção de Corpus	Tarefa	Conjunto de todas as palavras presentes em um conteúdo textual. É a base para a maioria das tarefas de PLN
Tokenização	Técnica	Também chamada de “Segmentação de Palavras”, é responsável por quebrar uma determinada sequência de caracteres de um texto para determinar onde uma palavra inicia e termina. Feito essa segmentação, cada palavra é interpretada como um token.
Lematização	Técnica	Redução de palavras à sua forma canônica chamada de lema responsável por relacionar diferentes palavras com o mesmo significado, como “Melhor” e “Bom”.
Marcação Gramatical	Técnica	Trata-se da atribuição de características morfossintáticas a cada palavra em uma frase de acordo com o seu contexto.
Remoção de Stopwords	Técnica	Tem o objetivo de manter um corpus mais conciso e limpo. Para isso, remove as palavras com menos relevância em uma sentença, como conjunções e numerais.
Concordância	Tarefa	Busca em um corpus todas as ocorrências de cada palavra selecionada e exibe seu contexto imediato. Além disso, as concordâncias podem ser produzidas em vários formatos, mas a forma mais comum é a concordância para produzir palavras-chave.
Frequência	Tarefa	Produz conjuntos de palavras e sua frequência em um determinado corpus. Trata-se da principal técnica utilizada para a formação de nuvem de palavras.
Colocação Estatística	Técnica	Busca por informações estatísticas relacionadas a composição de um corpus. Estes valores podem estar relacionados a associação de palavras, frequência e semântica.

Item	Tipo	Descrição
Produção de texto sintético	Técnica	Trata-se da produção de um texto em linguagem humana ou natural feita por um sistema inteligente
Análise de Sentimentos	Tarefa	Busca entender o sentimento por trás de um conteúdo textual, para posteriormente, classificá-lo em positivo, negativo ou neutro.
Modelagem de Tópicos	Tarefa	Identificação dos principais tópicos presentes em um conjunto de conteúdo textual.
Identificação de Entidades Nominais	Tarefa	Identificação e classificação de entidades pré-definidas, como: nomes, data, localizações, códigos médicos, hora, valores financeiros, dentre outros.

Fonte**:** Adaptado de Montasari (2023), Ukwen e Karabatak (2021).

Segundo Montasari (2023), Ukwen e Karabatak (2021), a aplicação das técnicas de PLN descritas na Tabela 5 tem se mostrado relevante em tarefas que envolvam a análise de volumes de conteúdo textual. Utilizar estas técnicas permite interpretar, extrair e estruturar informações a partir de arquivos, e-mails, mensagens de texto, documentações e até transcrições de áudio.

A próxima seção fundamentará as técnicas da Árvore de Decisão e Floresta Aleatória.

2.3.2. ÁRVORE DE DECISÃO E FLORESTA ALEATÓRIA

A Árvore de Decisão é uma técnica de IA de aprendizado supervisionado composta por diversos nós estruturados de forma hierárquica. Comumente usada em tarefas de classificação e regressão, a Árvore de Decisão é considerada uma técnica versátil devido a sua capacidade de lidar com dados categóricos e numéricos (COSTA; PEDREIRA, 2023).

Em relação a sua arquitetura, a Árvore de Decisão é formada por Raiz, Ramos, Nós e Folhas (Costa; Pedreira, 2023; Saisundar; Devi, 2023). Os componentes da Árvore de Decisão são descritos na tabela 6, juntamente com sua descrição.

Tabela 6 – Componentes de uma Árvore de Decisão

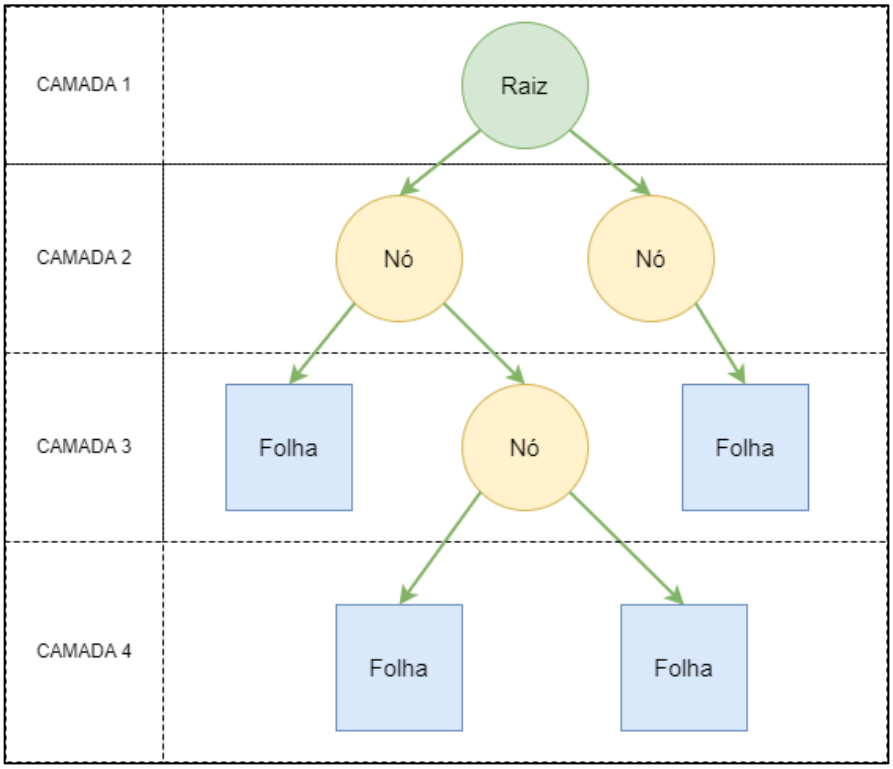
Componente	Descrição
Raiz	Trata-se do primeiro nó da árvore de decisão. Este nó armazena todos os exemplos do conjunto de treinamento fornecidos como entrada.
Ramos	Representação do relacionamento entre os Nós da Árvore de Decisão.

Componente	Descrição
Nós	Representação dos possíveis resultados das decisões descobertas na Raiz na Árvore de Decisão. Estas decisões também são chamadas de testes ou regras *if else*. Destaca-se que quanto mais decisões a Árvore de Decisão possuir, maior será a sua profundidade.
Folhas	Também chamadas de Nós Terminais, as folhas representam as possíveis saídas previstas na Árvore de Decisão. Em uma tarefa de classificação, por exemplo, as folhas representam as possíveis classes de saída.

Fonte**:** Adaptado de Costa e Pedreira (2023) e Saisundar e Devi (2023)

Todos os componentes que formam a Árvore de Decisão são apresentados na figura 13.

Figura 13 – Arquitetura de uma Árvore de Decisão



Fonte: Adaptado de Sarang (2023).

Para construir a arquitetura que melhor represente o conjunto de exemplos fornecidos como entrada, a Árvore de Decisão procura o atributo que melhor faz a divisão dos exemplos. Para isto, a Árvore de Decisão testa todos os atributos por meio de uma métrica para obter um valor denominado pureza. A pureza é o valor que representa a homogeneidade do conjunto de exemplos. São exemplos de métricas usadas para medir a pureza de uma Árvore de Decisão: o Índice Gini e a Entropia da Informação (Sarang, 2023). As métricas utilizadas pela Árvore de Decisão para medir a pureza de sua arquitetura são descritas na tabela 7, juntamente com sua descrição e equação.

Tabela 7 – Métricas utilizadas para medição de Pureza em uma Árvore de Decisão

Métrica	Descrição
Índice Gini	Métrica responsável por medir a desigualdade entre os exemplos fornecidos como entrada. Para isso, testa e seleciona os indivíduos extremos entre os exemplos, um puro com o valor igual a 0, e um impuro com o valor igual ou próximo a 1. $$G(X) = 1 - \sum_{i=1}^{n} (p(x_i))^2 \quad (2)$$
Entropia da Informação	Métrica responsável por medir o balanceamento do conjunto de exemplos fornecidos como entrada. Seu objetivo é garantir a homogeneidade entre os exemplos, onde $P(x_i)$ indica a probabilidade de um exemplo ser classificado em uma classe. Quanto mais puro os exemplos, mais próximo de 0 será o valor da Entropia. Desta forma, o valor começa a se afastar do zero à medida que os exemplos forem se tornando mais heterogêneo. $$H(X) = -\sum_{i=1}^{n} P(x_i) log P(x_i) \quad (3)$$

Fonte**:** Adaptado de Sarang (2023).

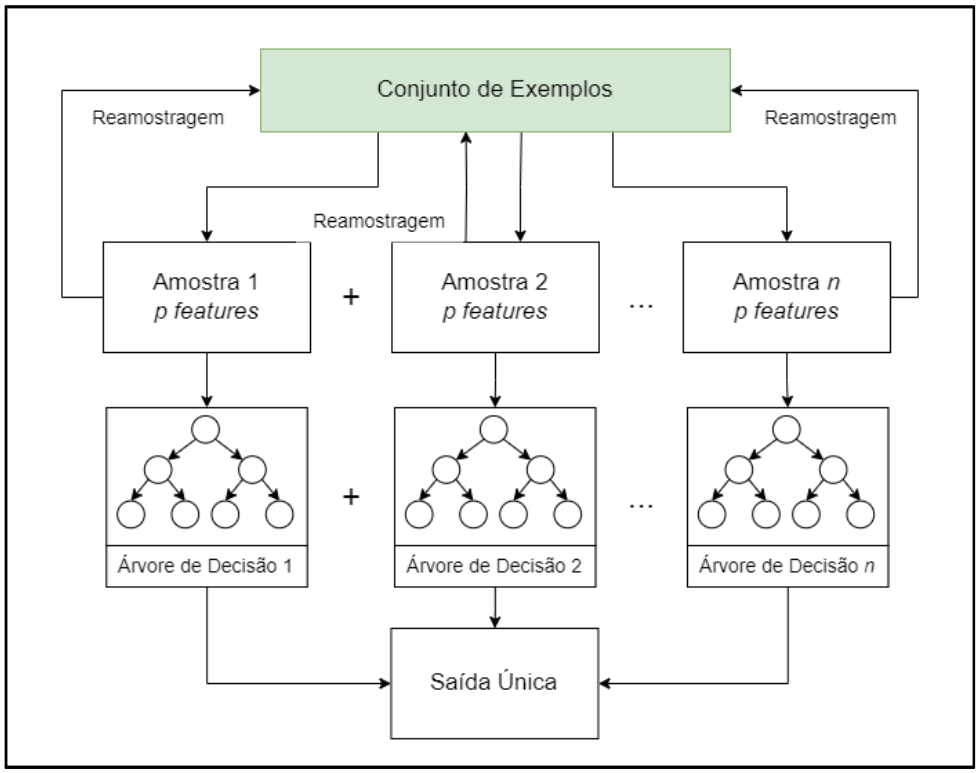
Uma evolução da técnica da Árvore de Decisão é a técnica da Floresta Aleatória. Criada por Leo Breiman. A Floresta Aleatória é uma técnica de IA de aprendizagem supervisionada desenvolvida por Breiman (2001). A Floresta Aleatória pode ser descrita como um classificador formado por um conjunto de Árvores de Decisão $\{h(X, v_k), k, 1, \dots\}$, onde v_k são amostras aleatórias distribuídas de maneira uniforme entre todas as Árvores (BREIMAN, 2001).

O resultado da Floresta Aleatória é obtido por meio da agregação das previsões de todas as árvores individuais, geralmente através de votação majoritária no caso de classificação ou pela média das previsões no caso de regressão (ARABAMERI et al., 2022).

Dentre as principais vantagens da Floresta Aleatória, destaca-se a sua versatilidade, pois é possível obter bons resultados sem que seja necessário preparar o conjunto de exemplos a ser fornecido como entrada. Isso porque a Floresta Aleatória escolhe os atributos para cada amostra de exemplos aleatoriamente, forçando suas árvores a considerarem diferentes atributos para obter sua pureza (COSTA; PEDREIRA, 2023; CZAJKOWSKI; KRETOWSKI, 2019).

Sobre sua arquitetura, a Floresta Aleatória é formada por um conjunto de Árvores de Decisão. Esta arquitetura é ilustrada na figura 14.

Figura 14 – Arquitetura da Floresta Aleatória



Fonte: Adaptado de Costa e Pedreira (2023) e Czajkowski e Kretowski (2019).

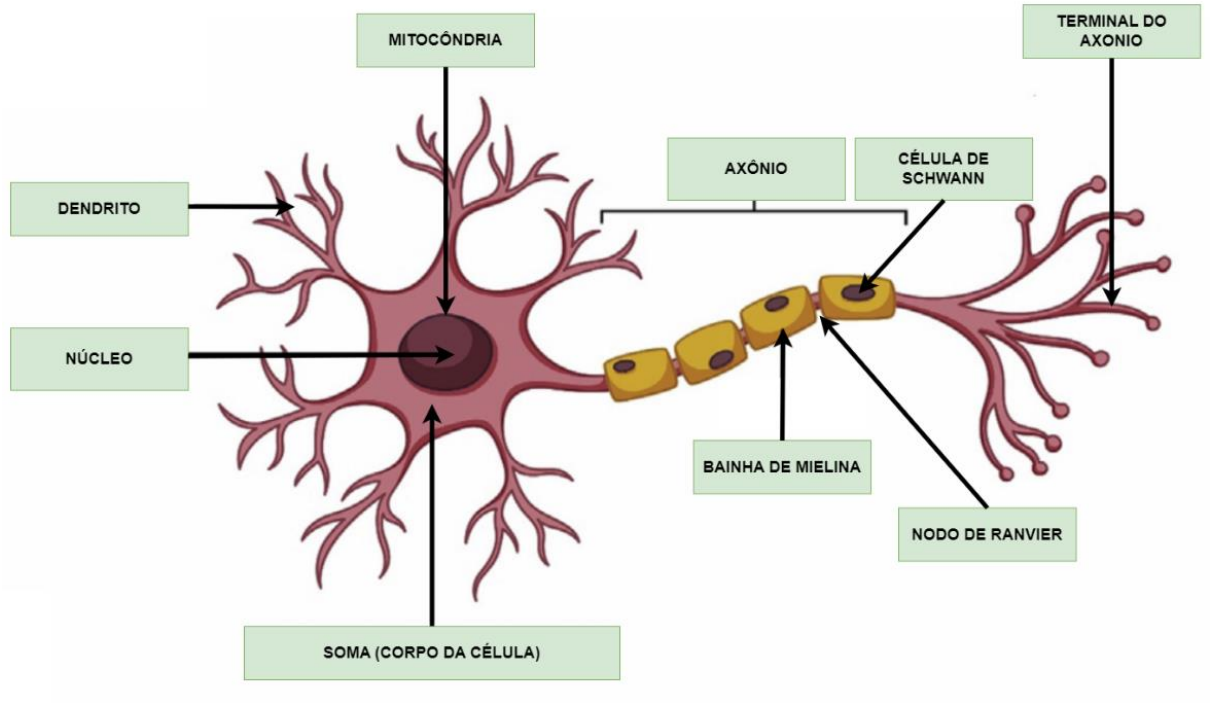
Quanto a sua aplicação, por se tratar de uma técnica versátil, a Floresta Aleatória pode ser empregada nas mais diversas áreas, como economia e segurança da informação. Sobre o combate ao crime cibernético, a Floresta Aleatória é comumente usada para lidar com tarefas que envolvam a interpretação e manipulação de conjuntos de dados complexos. A capacidade de mitigar *Overfitting* e *Underfitting* faz da Floresta Aleatória uma técnica adequada para tarefas de classificação, regressão e descoberta de padrões (KAYODE-AJALA, 2022).

2.3.3. REDES NEURAIS ARTIFICIAIS

As Redes Neurais Artificiais (RNA), modelos matemáticos de IA inspirados na estrutura do cérebro com o objetivo de simular o comportamento humano em processos como: aprendizado, adaptação, associação, generalização e abstração (HAYKIN, 2001).

A principal inspiração das RNAs, o neurônio biológico pode ser entendido como célula do sistema nervoso de organismos vivos responsável por receber, processar e transmitir sinais eletroquímicos. Também chamado de unidade básica da neuroanatomia, o neurônio biológico reage a diferentes estímulos para propagar sinais para os outros neurônios (Le et al., 2020). A estrutura do neurônio biológico é ilustrado na figura 15.

Figura 15 – Estrutura do Neurônio Biológico

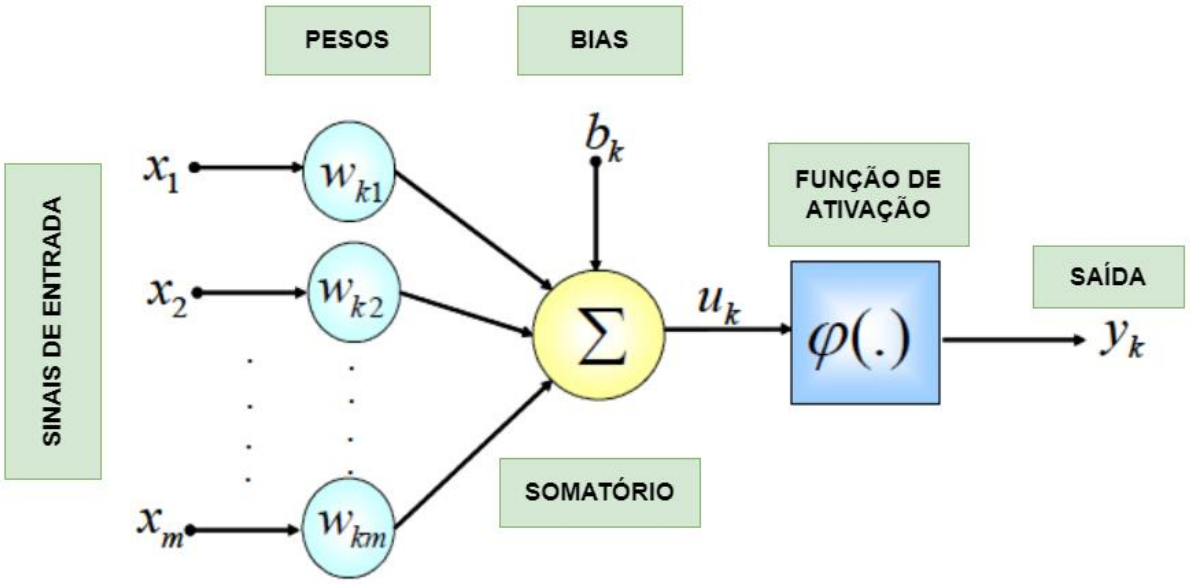


Fonte: Adaptado de Le et al. (2020).

A estrutura do neurônio biológico e seus principais componentes é apresentada na figura 15. Em relação ao funcionamento do neurônio biológico, os dendritos recebem os sinais eletroquímicos de outros neurônios e os conduzem até o Soma. Em seguida, os sinais são processados e enviados pelos axônios para os próximos neurônios. Esta transmissão de sinais é chamada de Sinapse (MUTHUKRISHNAN et al., 2020).

No caso do neurônio artificial, o primeiro modelo matemático consolidado e aceito pela comunidade acadêmica foi proposto por McCulloch e Pitts (1943). Este modelo tem como objetivo implementar de forma simplificada os componentes e o funcionamento de um neurônio biológico (Haykin, 2001). A estrutura do neurônio artificial é ilustrada na figura 16.

Figura 16 – Estrutura do Neurônio Artificial



Fonte: Adaptado de Haykin (2001)

A figura 16 apresenta a estrutura do neurônio artificial e seus principais componentes. Também chamado de unidade simples de processamento, o neurônio artificial é composto por um vetor de entrada $X[x_1, x_2, x_3, \dots\ x_m]$, um vetor de pesos $W[k_1, k_2, k_3, \dots\ k_m]$, o somatório $\sum$, a função de ativação $\varphi(\cdot)$ e a saída y_k.

Em um neurônio artificial, os dados dos vetores de entrada e pesos são enviados para o somatório. Enquanto os dados do vetor de entrada são fornecidos externamente, os dados do vetor de pesos são iniciados aleatoriamente. Em seguida, a função de ativação transmite ou bloqueia os dados processados no somatório, similar ao neurônio biológico. Assim, o vetor de pesos tem seus dados atualizados baseando-se em seu antigo valor, conforme é demonstrado na equação (4):

$$\boldsymbol{w_i^{t+1} = w_i^t + \Delta w_i^t} \tag{4}$$

A atualização dos dados do vetor de pesos depende da RNA utilizada, mas costuma se basear na minimização do erro entre os valores previstos pela RNA e as saídas y_k desejadas. A atualização dos pesos é apresentada na equação (5):

$$\boldsymbol{\varepsilon_i = \sum w_i x_i - y_i} \tag{5}$$

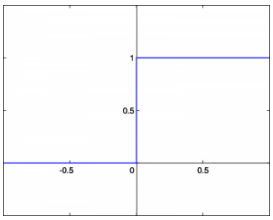
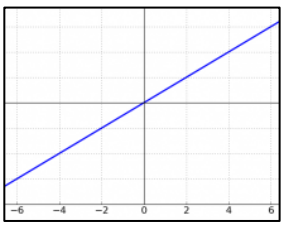
A atualização dos dados do vetor de pesos possibilita que a RNA aprenda com os dados fornecidos como entrada, também chamados de conjunto de exemplos de treinamento. Ao longo deste processo, os dados do vetor de pesos são atualizados até que a taxa de erro tenha alcançado níveis baixos. A taxa de erro é utilizada como métrica para avaliar o desempenho da RNA. Todo este procedimento faz parte da Aprendizagem da RNA (HAYKIN, 2001).

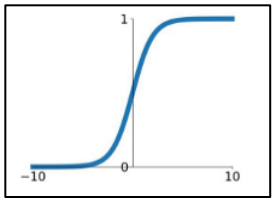
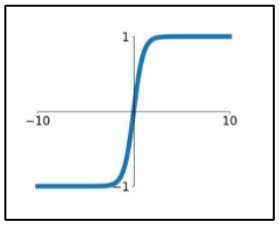
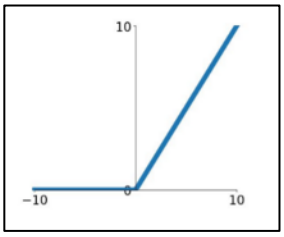
O aprendizado das RNAs pode ser classificado em dois tipos principais: supervisionado e não-supervisionado. Na aprendizagem supervisionada, são fornecidos os dados de entrada e suas respectivas saídas. As saídas representam diferentes classes e servem de "professor" para possibilitar a RNA generalizar e modelar novos dados. No aprendizado supervisionado, as tarefas mais comuns são a de classificação e a de regressão (BAO; LIANJU; YUE, 2019).

Na aprendizagem não-supervisionada, a RNA infere propriedades nos dados fornecidos como entrada e assim, exime a necessidade de um "professor". Neste tipo de aprendizado, a RNA deve encontrar padrões ou relacionamentos nos dados sem nenhuma orientação explícita sobre a saída. No aprendizado não-supervisionado, as tarefas mais comuns são a de reconhecimento de padrões e a de agrupamentos (BAO; LIANJU; YUE, 2019).

Concluído o processamento dos dados de entrada e dos pesos no somatório, o resultado é enviado para a função de ativação da RNA. A função de ativação é responsável por definir a amplitude do sinal de saída y_k do neurônio artificial. Este valor costuma estar nos intervalos entre 0 e 1, ou entre -1 e 1 (Szandala, 2021). Entre os diversos tipos de funções de ativação, as mais utilizadas são apresentadas na tabela 8, juntamente com sua função e equação.

Tabela 8 – Principais funções de ativação das RNA

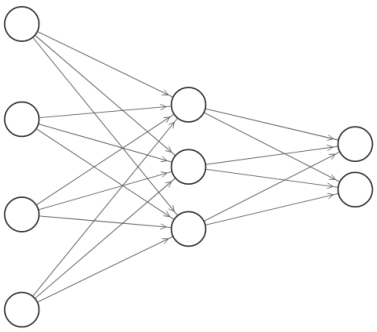
ID	Nome	Função	Equação	
01	Binária		$f(x) = \begin{cases} 0 \; if \; 0 > x \\ 1 \; if \; x \geq 0 \end{cases}$	(6)
02	Linear		$f(x) = x$	(7)

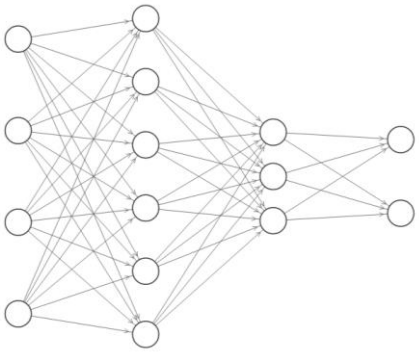
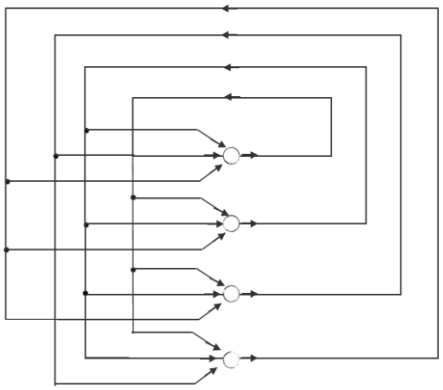
ID	Nome	Função	Equação	
03	Sigmóide		$\sigma(x) = \frac{1}{1 + e^{-x}}$	(8)
04	Tanh		$f(\sum) = \frac{e^{\Sigma} - e^{-\Sigma}1}{e^{\Sigma} + e^{-\Sigma}}$	(9)
05	ReLU		$f(x) = max(0,x) = \begin{cases} 0 \; se \; x \leq 0 \\ x \; se \; x > 0 \end{cases}$	(10)

Fonte**:** Adaptado de Szandala (2021).

Os neurônios artificiais podem ser estruturados em diferentes tipos de arquiteturas de RNA. As principais arquiteturas de RNA são as *Feedforward* de 1 camada, as *Feedforward* Multicamadas e as Recorrentes (Ghorpade; Bhad; Khairnar, 2023). As principais arquiteturas de RNA são descritas na tabela 9.

Tabela 9 – Principais tipos de arquiteturas de RNA

ID	Nome	Tipos de Arquitetura da RNA	Descrição
01	*Feedforward* de 1 Camada		O termo *Feedforward* significa que o sinal processado na camada oculta é enviado para os neurônios de saída unilateralmente. Isso significa que os dados não são processados na camada de saída e nem podem retornar para a camada oculta. É uma arquitetura utilizada na resolução de problemas simples de classificação.

ID	Nome	Tipos de Arquitetura da RNA	Descrição
02	*Feedforward* Multicamadas		Este tipo de arquitetura se distingue da arquitetura *Feedforward* de 1 camada por possuir mais camadas ocultas. As camadas ocultas ficam posicionadas entre os neurônios de entrada e os neurônios de saída. Adicionar mais camadas ocultas pode fazer com que essa arquitetura de RNA possa lidar com problemas complexos de maneira eficiente.
03	Recorrente		Este tipo de arquitetura de RNA se distingue da *Feedforward* por permitir uma realimentação da camada de neurônios com a sua própria saída. Este tipo de arquitetura é usado para tarefas em que os dados precisam ser recuperados ou reconstruídos, como reconhecer fala e reconstruir informações.

Fonte**:** Adaptado de Ghorpade, Bhad e Khairnar (2023).

Em relação a aplicação das RNAs na Computação Forense, os autores Ghorpade, Bhad e Khairnar (2023), Mohammad (2018) e Worden et al. (2023) descrevem em seus estudos um aumento de desempenho considerável em diversas tarefas executadas em um exame pericial, como identificar, preservar, coletar, analisar e estruturar as evidências de crimes cibernéticos.

Sobre o combate à pornografia infantojuvenil, os autores Apruzzese et al. (2023) e Kloess, Woodhams e Hamilton-Giachritsis (2021) descrevem que o uso das RNAs pode desempenhar um papel crucial na detecção de evidências. Os autores reforçam a necessidade de desenvolver novas pesquisas com RNA para aumentar a variedade de recursos à disposição do combate ao crime cibernético de pornografia infantojuvenil.

Os principais conceitos das seguintes RNAs são apresentados a seguir.

2.3.3.1. REDES NEURAIS DE HOPFIELD

Hopfield propôs em (1982) um modelo de rede neural capaz de armazenar informação em uma configuração de neurônios artificiais dinamicamente estáveis, para posteriormente poder recuperá-la ao receber informações similares (DE MARZO; IANNELLI, 2023).

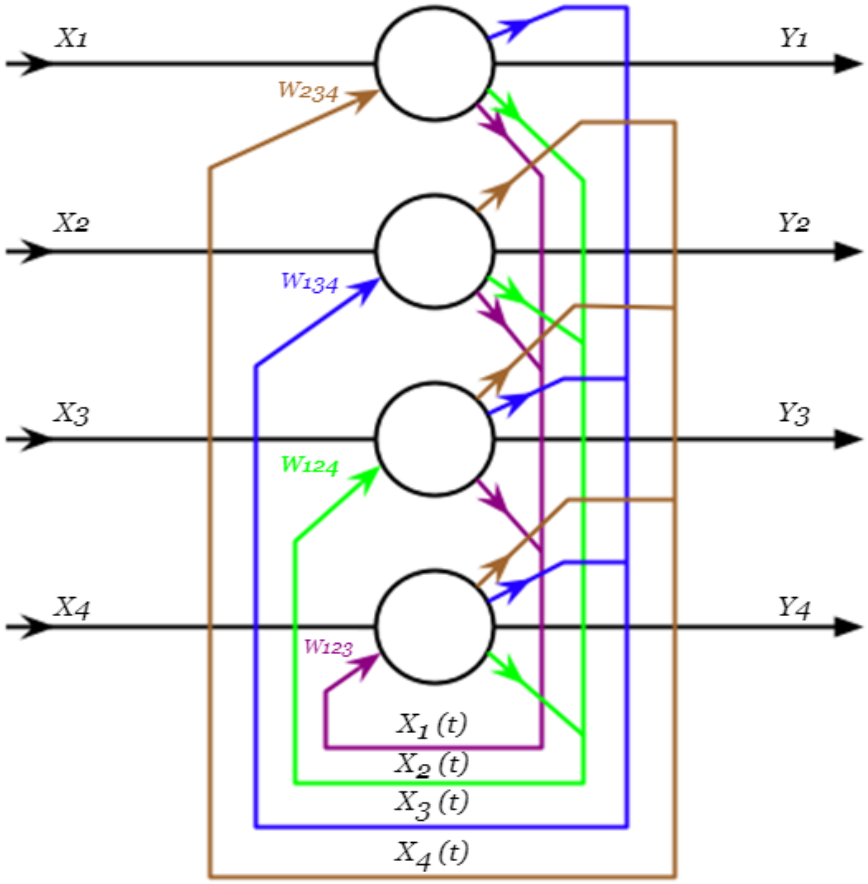
A Rede Neural de Hopfield (RNH) é um tipo de RNA inspirada no funcionamento da memória humana que utiliza auto associação – auto associativa que significa promover uma saída com apenas fragmentos de informação submetidos na entrada (De Marzo; Iannelli, 2023; Xu; Chen, 2022). Sobre o funcionamento da RNH, ao receber um conjunto de dados de entrada em um vetor X, diferentemente das demais redes, o vetor de entrada recebe uma adição de estado contínuo representado por $X(t)$, conforme demonstra a equação (11):

$$X(t) = [x_1(t), x_2(t), \dots, x_N(t),]^T \tag{11}$$

Os dados do vetor de entrada $X(t)$ são propagados para todos os outros neurônios. Cada neurônio processa então estes dados juntamente com o vetor de pesos $W[k_1, k_2, \ \dots \ k_m]$ para gerar uma saída única y_k. Concluído a geração da saída y_k, verifica-se a existência de novos dados sendo fornecidos como entrada para o vetor $X(t)$. Em caso positivo, repete-se todo o procedimento e assim, os neurônios são atualizados ao remover os valores atuais e adicionar os novos valores (SABAHI; OMAIR AHMAD; SWAMY, 2018).

Esta atualização dos valores dos neurônios é executada de forma contínua até que não haja mais novos dados sendo fornecidos como entrada n o vetor $X(t)$. Todo este processo caracteriza o aprendizado da RNH (Alemanno et al., 2023; Sabahi; Omair Ahmad; Swamy, 2018). Uma RNH formada por quatro neurônios é ilustrada na figura 17.

Figura 17 – RNH composta por quatro neurônios



Fonte: Adaptado de Sabahi, Omair Ahmad e Swamy (2018).

Em uma RNH, cada neurônio é representado por um valor binário, também referenciado na literatura como binário ou bipolar (12),

$$y_k = \begin{cases} +1 \; if \; \sum_j w_{ij} x_i \geq 0_i \\ -1 \; if \; \sum_j w_{ij} x_i < 0_i \end{cases} \tag{12}$$

Na qual, o único valor possível de ser assumido em cada neurônio da RNH é 1 (neurônio ativo) ou -1 (neurônio não-ativo) (ALEMANNO et al., 2023).

Todo este procedimento de atualização e armazenamento dos valores nos neurônios via conexões recorrentes caracteriza a aprendizagem da RNH. Este tipo de aprendizagem onde os neurônios enviam os sinais e são ativados de forma simultânea é denominada aprendizagem Hebbiana. Na aprendizagem Hebbiana, quanto maior o valor de um peso $W[k_m]$, maior será a probabilidade de serem ativados simultaneamente, conforme está demonstrado na equação (13):

$$w_{km} = \frac{1}{N} \sum_{n=1}^{N} x_{ki} x_{kj} \quad (13)$$

Sendo que x_k é uma representação binária do valor do peso, enquanto o valor de x_{ki} representa cada valor de k (CENTORRINO; BULLO; RUSSO, 2022).

Ao analisar a execução da RNH em um contexto de sistemas dinâmicos não-lineares, pode-se utilizar a função de Lyapunov para validar sua estabilidade. A função de Lyapunov é um conceito da teoria de controle usado na análise da estabilidade de sistemas dinâmicos. Seu objetivo é determinar se um sistema permanecerá em um estado desejado ou convergirá para um estado estável ao longo do tempo (ALEMANNO et al., 2023; WU et al., 2022).

Em uma RNH, para que o neurônio receba e armazene o valor de saída y_k, é necessário que a saída y_k esteja em estado estável. Isso significa que o neurônio só irá armazenar o valor de 1 ou -1 quando este valor não estiver mais sofrendo alteração. Assim, utiliza-se a função de Lyapunov para determinar que a RNH atingiu estado estável, uma vez que os valores dos neurônios não irão mais sofrer alterações (WU et al., 2022).

Quando um vetor de entrada $X(t)$ for enviado a RNH, será feita a aprendizagem da RNH e o armazenamento da saída y_k. Ao receber um novo vetor $X(t)$ como entrada, mesmo que possua ruído ou valores faltantes em relação ao valor armazenado, será possível recuperá-lo. Isso porque se os valores armazenados e o novo valor de entrada foram próximos, o estado estável do neurônio se tornará igual ao estado estável armazenado (CHEN et al., 2023).

Quanto às suas aplicações, a RNH é utilizada com frequência na resolução de problemas de recuperação de informação, por exemplo: a restauração de imagens incompletas (Li; Guan; Xu, 2018), a manipulação de criptografia em imagens (Xu; Chen, 2022), e a detecção de esteganografia em arquivos multimídia (ÇAVUŞOĞLU, 2022).

Para validar a qualidade da RNH, uma métrica que pode ser utilizada é a distância de Hamming. A distância de Hamming calcula a diferença entre número de bits do padrão de saída e o número de bits do valor original fornecido como entrada (Antipova; Rashkovskiy, 2021), A distância de Hamming é descrita na subseção 2.3.4 deste trabalho.

2.3.3.2. LONG SHORT-TERM MEMORY (LSTM)

A Rede de Memória de Longo e Curto Prazo ou LSTM (*Long Short-Term Memory*) é um tipo de RNA recorrente utilizada para armazenar informação em diferentes períodos de tempo de forma simplificada. Foi desenvolvida em 1997 com o objetivo de processar, classificar e prever séries temporais com maior facilidade do que os outros tipos de RNAs (HOCHREITER; SCHMIDHUBER, 1997).

A arquitetura da LSTM é formada por laços capazes de tornar persistentes as informações consideradas relevantes. Estas informações são armazenadas em memórias de longo e curto prazo (Hochreiter; Schmidhuber, 1997). Ambas as memórias são descritas na tabela 10.

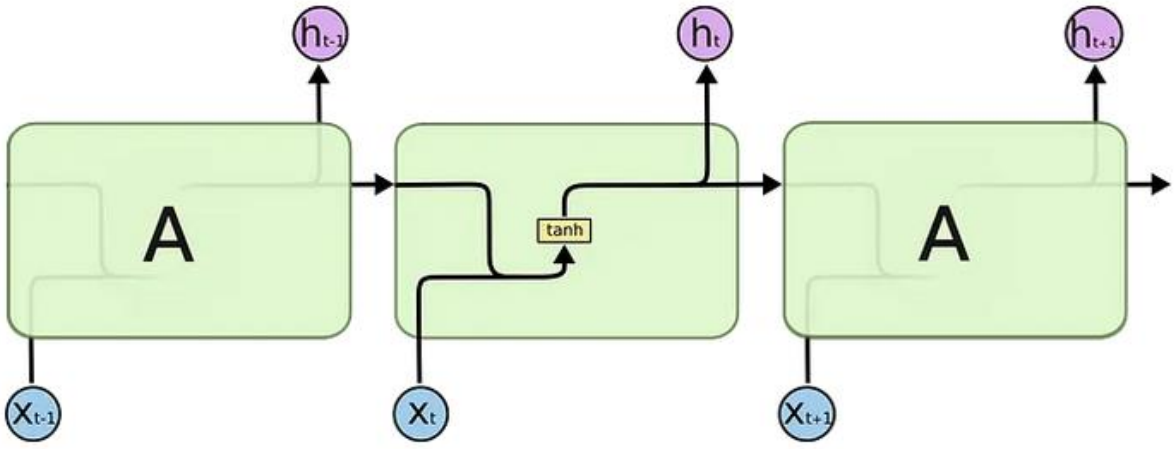
Tabela 10 – Memórias de Longo e Curto Prazo em uma LSTM

Memória	**Descrição**
Memória de Curto Prazo	No momento da aquisição da informação, é feito o armazenamento desta informação por alguns segundos até que outra informação seja fornecida como entrada. Neste momento, a informação pode ser descartada ou destinada para as unidades de armazenamento de longo prazo.
Memória de Longo Prazo	Recebe a informação armazenada na memória de curto prazo. Esta informação fica armazenada, possibilitando sua recuperação ou chamada posteriormente. É na memória de longo prazo que a informação considerada relevante fica armazenada.

Fonte**:** Adaptado de Hochreiter e Schmidhuber (1997).

Sobre a arquitetura da LSTM, trata-se de uma cadeia de células interconectadas, conforme é ilustrado na figura 18.

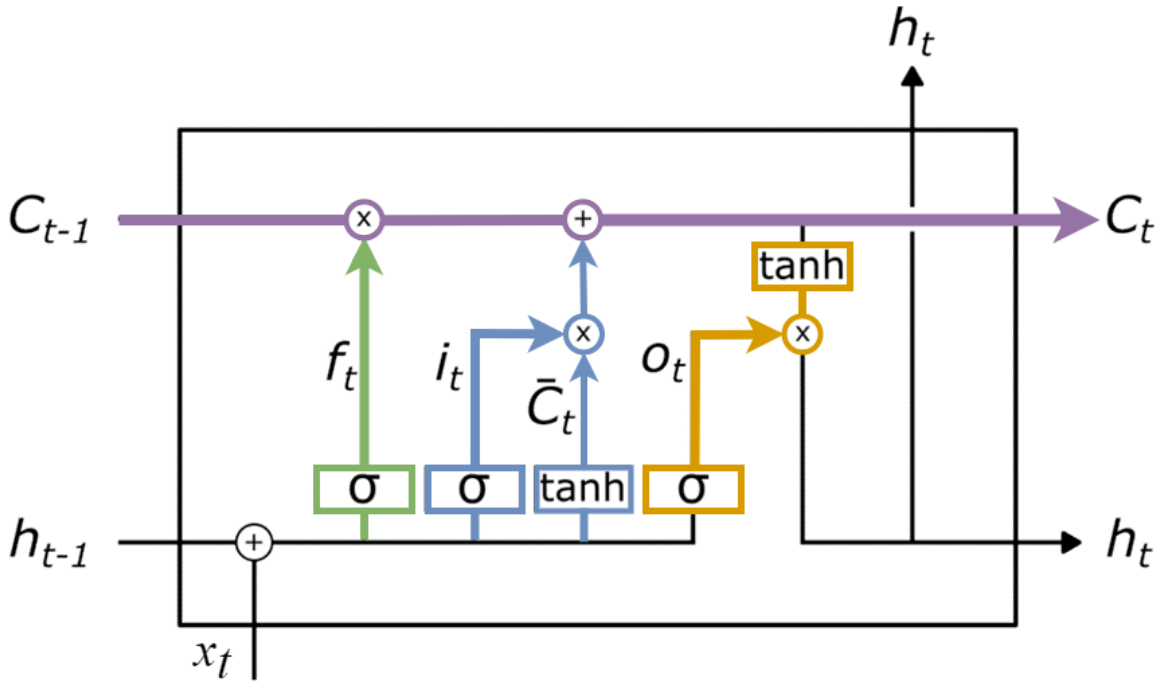
Figura 18 – Arquitetura da LSTM



Fonte**:** Adaptado de Hochreiter e Schmidhuber (1997).

A manipulação da informação dentro da rede LSTM acontece por meio de três portões denominados: Esquecimento, Entrada e Saída (Shewalkar; Nyavanandi; Ludwig, 2019). A arquitetura de uma célula LSTM é ilustrada na figura 19.

Figura 19 – Arquitetura da Célula LSTM



Fonte: Adaptado de Shewalkar, Nyavanandi e Ludwig (2019).

O portão do esquecimento (f_t), destacado na cor verde, é responsável por descartar as informações consideradas irrelevantes. Neste portão, multiplica-se os dados de entrada (x_t) e a memória curta (h_{t-1}), pelos pesos $(W_f\ U_f)$ e adicionado um valor de Bias (B_f). O resultado é enviado para uma função sigmoide σ de saída 0 ou 1. A função da porta de esquecimento é definida na equação (14) da seguinte forma:

$$f_t = \sigma\,(x_t * U_f + h_{t-1} * W_f + B_f) \qquad (14)$$

O portão denominado entrada i_t, destacado na cor azul, é responsável por definir quais informações devem ser atualizadas dentro da célula. Para isso, multiplica-se o valor de entrada x_t e o estado oculto h_t pelos seus respectivos pesos $U_i\ W_i$. Em seguida, adiciona-se um viés b_i caso exista, e encaminha-se o resultado para uma função sigmoide σ que irá gerar um valor entre 0 e 1. Ao mesmo tempo que este resultado é enviado para a função sigmoide σ, os valores de entrada x_t e do estado oculto h_t também são enviados para a função $tanh$ para gerar candidatos $\bar{C}_t$ para o estado da célula LSTM.

Por fim, acontece uma comparação para decidir qual informação será considerada relevante, e assim, enviada para o estado da célula LSTM. Isso é feito através da multiplicação entre i_t e $\bar{C}_t$ (Shewalkar; Nyavanandi; Ludwig, 2019). Ambas as funções são definidas nas equações (15) e (16), respectivamente:

$$i_t = \sigma\,(x_t * U_i + h_{t-1} * W_i + B_i) \tag{15}$$

$$\bar{C}_t = tanh\,(x_t * U_c + h_{t-1} * W_c + B_c) \tag{16}$$

Após comparar os valores entre i_t e $\bar{C}_t$, a célula LSTM está pronta para atualizar o estado da $\bar{C}_t$. Ou seja, a informação considerada relevante está pronta para ser armazenada. Isso é feito por meio da multiplicação do estado anterior da célula C_{t-1} e a saída da porta de esquecimento f_t. O resultado desta multiplicação é adicionado com a multiplicação dos resultados da porta de entrada i_t e os candidatos $\bar{C}_t$. Isso irá criar um novo estado na célula LSTM e enviará as informações para a próxima célula LSTM (Sherstinsky, 2020), conforme a equação (17).

$$C_t = C_{t-1} * f_t + i_t * \bar{C}_t) \tag{17}$$

O último portão é denominado saída o_t. Neste portão, destacado na cor laranja, calcula-se o novo estado oculto. Para isto, encaminha-se para uma função sigmoide σ os dados de entrada x_t e do estado oculto anterior h_{t-1}. Este resultado é enviado para uma função $tanh$. Após isto, multiplica-se estes resultados para gerar um novo estado oculto h_t (Sherstinsky, 2020). O cálculo da porta de saída o_t e a geração do novo estado oculto h_t são definidos nas equações (18) e (19), respectivamente:

$$o_t = \sigma\,(x_t * U_o + h_{t-1} * W_o + B_o) \tag{18}$$

$$h_t = o_t * \tanh\,(C_t) \tag{19}$$

Aplicações baseadas em LSTM necessitam de uma quantidade de dados consideráveis para treinamento. Dentre as principais, destacam-se o reconhecimento de falas e de conteúdo textual de diversas línguas. A popularização da LSTM dentro da ciência ganhou força com o surgimento do Tesseract, um software de código aberto desenvolvido pela HP entre 1984 e 1994 para realizar OCR (IDREES; HASSANI, 2021; SHERSTINSKY, 2020).

Sobre o combate a crimes cibernéticos, as redes LSTM podem ser utilizadas em tarefas de classificação e extração de textos, para assim, determinar se possuem alguma relação com atividades ilícitas. Devido a capacidade da LSTM de armazenar as informações consideradas

relevantes, estas redes são indicadas para tarefas que envolvam a análise de um volume de texto considerável (AL-KHATER et al., 2020).

Para avaliar o desempenho da LSTM na extração e análise de textos, utiliza-se a medida da acurácia. Esta acurácia pode ser quantificada ao comparar o valor recuperado pela LSTM com o valor desejado fornecido como entrada. As métricas que podem ser utilizadas para a acurácia da LSTM são as mesmas mencionadas neste trabalho para extração de metadados e OCR. São a Taxa de Erro de Palavras (WER) e a Taxa de Erro de Caracteres (CER) (Kundaikar; Pawar, 2020), todas descritas na subseção 2.3.4 deste trabalho.

2.3.3.3. REDES NEURAIS CONVOLUCIONAIS

A Rede Neural Convolucional (RNC) é um tipo de RNA de aprendizado profundo inspirada no processo biológico da percepção visual dos seres vivos. A RNC foi proposta por LeCun et al. (1998) como uma solução para problemas de classificação, principalmente de arquivos multimídia como imagens digitais.

A inspiração para o desenvolvimento da primeira RNC foi a resolução do problema de reconhecimento de caracteres manuscritos em imagens digitais. Posteriormente, outras RNCs foram desenvolvidas, como a AlexNet, VGG-19 e a LeNet-5 (SANGHVI et al., 2021).

Sobre a convolução, do ponto de vista matemático, pode ser definido como um operador que ao receber duas funções como entrada, retorna uma terceira função como saída. Dentre os principais tipos de convolução, pode-se citar a Convolução Temporal Contínua, a Convolução Temporal Discreta e a Convolução Espacial Discreta, sendo a última a mais utilizada no PID (Alzubaidi et al., 2021). Os principais tipos de convolução são descritos na tabela 11.

Tabela 11 – Principais tipos de convolução

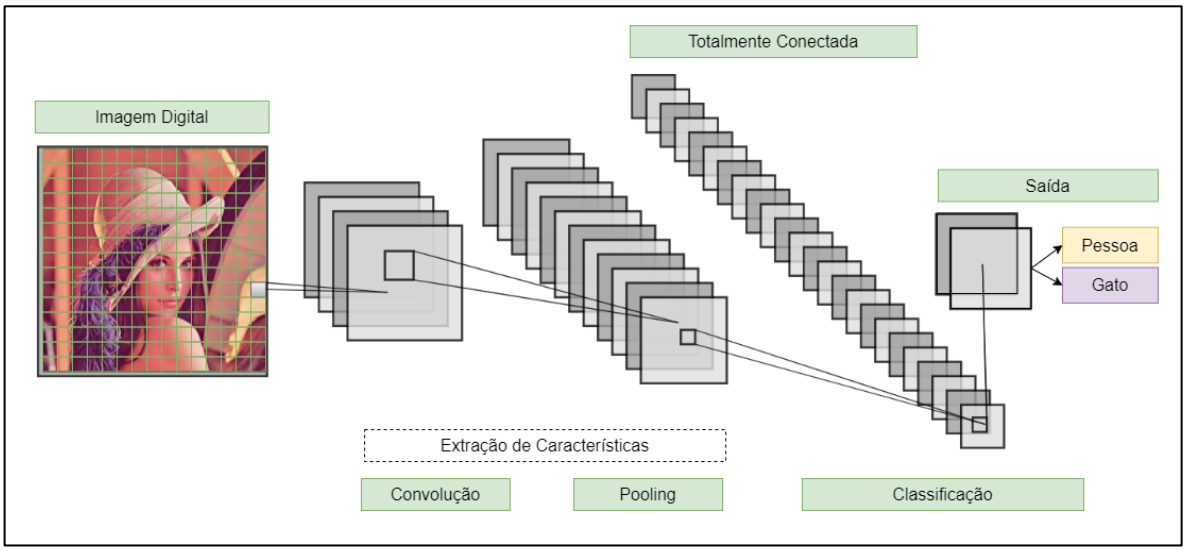
Convolução	**Descrição**
Convolução Temporal Contínua (CTC)	Trata-se de uma operação para identificar sinais sobrepostos (funções contínuas) em diferentes posições de tempo e unificá-los para gerar um terceiro sinal. A equação para calcular a convolução temporal contínua entre sinais é: $$f(t) * g(t) = \int_{-\infty}^{\infty} f(T) * g(t-T) * dT \quad (20)$$

Convolução	Descrição
Convolução Temporal Discreta (CTD)	Similar a Convolução Temporal Contínua, busca identificar sinais sobrepostos (funções contínuas) mas invariantes ao tempo, ou seja, sistemas lineares no mesmo tempo. A equação para calcular a convolução temporal discreta entre sinais é: $$(f * g)(n) = \sum_{k=-\infty}^{\infty} f(k) * g(n-k) \quad (21)$$
Convolução Espacial Discreta (CED)	Trata-se da operação para identificar matrizes sobrepostas. No caso de imagens digitais, são operações onde as imagens se sobrepõem por meio da multiplicação dos valores dos pixels.

Fonte**:** Adaptado de (ALZUBAIDI et al., 2021)

Sobre a arquitetura de uma RNC, é ilustrado na figura 20 uma RNC e suas camadas de convolução, *pooling* e totalmente conectadas.

Figura 20 – Arquitetura de uma RNC



Fonte: Adaptado de Yao, Lei e Zhong (2019).

Ao analisar a figura 20, percebe-se que a RNC é composta por diferentes camadas, cada uma com sua função. As camadas que formam a RNC são: Convolucional, *pooling* e a camada totalmente conectada (Yao; Lei; Zhong, 2019). A descrição sobre o funcionamento de cada camada é descrita na Tabela 12.

Tabela 12 – As Camadas da RNC

Camada	Descrição
Convolucional	Camada responsável pela extração das características das imagens por meio de filtros convolucionais de redução. Estes filtros percorrem os pixels da imagem fornecida como entrada, coleta as informações de largura, altura e profundidade. A cada processamento, os filtros são ajustados para extrair as características das imagens, como arestas, cores, dentre outras.
Pooling	Camada responsável pela redução da dimensionalidade da imagem fornecida como entrada. Seu objeto é alcançar um certo nível de invariância ao deslocamento da imagem fornecida como entrada e assim, gerar sub-imagens. Os tipos mais comuns de pooling são o *Max Pooling* e o Average Pooling. No *Max pooling*, seleciona-se o maior valor do pixel na região selecionada, enquanto no Average Pooling calcula-se a média dos valores da região selecionada.
Totalmente Conectada	Esta camada está posicionada após a última camada de Pooling. É a responsável por utilizar todas as características extraídas nas camadas anteriores para gerar uma saída.

Fonte**:** Adaptado de Yao, Lei e Zhong (2019).

Sobre o treinamento de uma RNC, utiliza-se o método de atualização dos parâmetros de bias e pesos. Este método é chamado de função custo ou função objetivo. Em uma RNC, uma função custo comumente utilizada é o gradiente descendente. Seu objetivo é reduzir os erros que afetam o desempenho da RNC. Seu resultado é denominado parâmetro ótimo (22):

$$\theta_{opt} = min_{\theta \in A^{\{L(\theta)\}}} \tag{22}$$

sendo A o espaço de parâmetros. Para suavizar a descida do gradiente descendente para alcançar o parâmetro ótimo θ_{opt}, pode incrementar a função *momentum*. Esta função utiliza o movimento anterior da descida do gradiente para variar os valores dos pesos em direção a um valor menor não abrupto, chamado de termo *momentum* (23):

$$w_i^{t+1} = w_t^i - \Delta w_i^t + \alpha \Delta w_i^{t-1} \tag{23}$$

onde α é o *momentum* e seu valor pondera e controla a atualização dos valores dos pesos com base nos parâmetros anteriores (ALZUBAIDI et al., 2021; YAO; LEI; ZHONG, 2019).

A RNC é comumente utilizada em aplicações que necessitam manipular imagens digitais. Pode-se citar como exemplo a classificação de imagens, o reconhecimento de faces, a detecção de objetos, a análise de imagens médicas e a classificação de vídeos. No combate a crimes cibernéticos, a RNC pode ser usada na detecção de intrusão, detecção de aplicativos maliciosos (*malwares*), e detecção de *phishings* (SONY et al., 2021).

Já para combater o crime cibernético de pornografia infantojuvenil, estudos como o de Gangwar et al. (2021) e Vitorino et al. (2018) descrevem o uso de RNC na detecção de faces, estimativa de idade e na detecção de conteúdo pornográfico generalizado.

Sobre as métricas utilizadas para medir o desempenho da RNC, pode-se utilizar as métricas: Matriz de Confusão, Precisão, *Recall*, *F-Score* e Curva ROC (Gangwar et al., 2021; Vitorino et al., 2018), todas descritas na subseção 2.3.4 deste trabalho.

2.3.3.4. REDES ADVERSÁRIAS GENERATIVAS

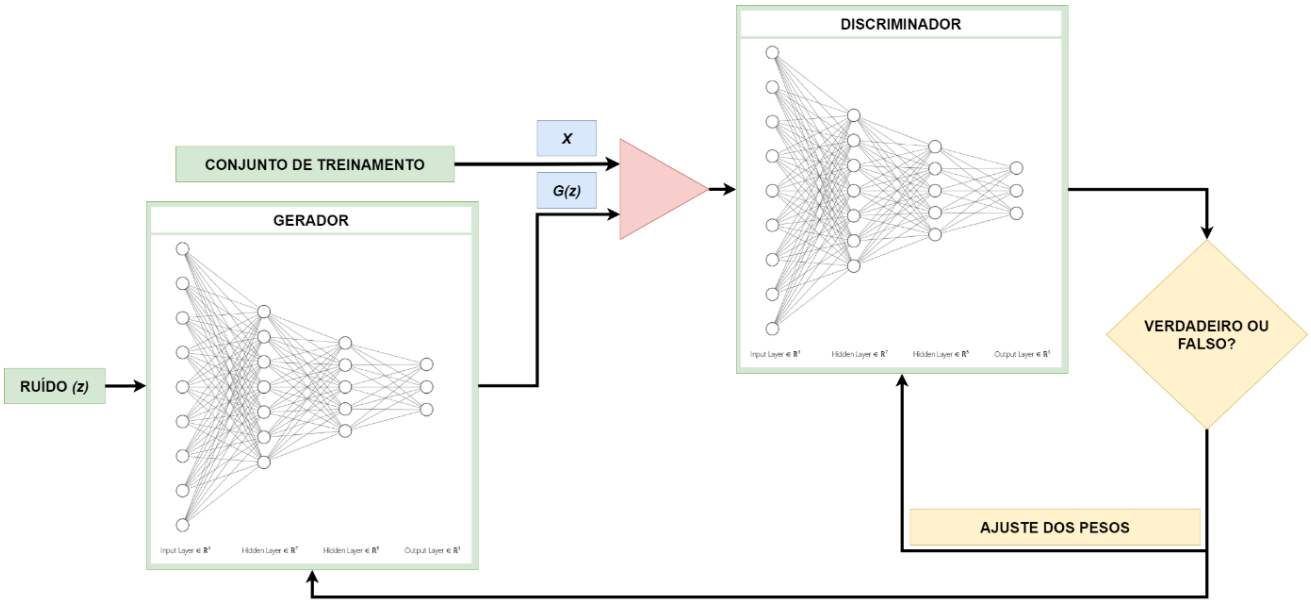
A Rede Adversária Generativa (RAG) é um tipo de RNA de aprendizagem profunda composta por duas RNAs colocadas uma contra a outra. Goodfellow et al. (2014) propôs a RAG com o objetivo de descobrir e aprender automaticamente padrões de um determinado conjunto de dados fornecidos como entrada, e a partir disso, produzir novos exemplos.

As RAGs fazem parte dá área da modelagem generativa. Trata-se de uma área voltada para o aumento de dados, baseando-se em um conjunto de dados inicial. Para isso, cria-se uma função de distribuição probabilística que ao tentar entender o grau de pertinência de um determinado exemplo, tenta gerar novos exemplos com o mesmo grau de pertinência que os dados originais (GOODFELLOW et al., 2020).

Dentre os principais usos para a modelagem generativa, pode-se citar como exemplo a simulação com baixo custo computacional e taxas de erro, e a correção de dados faltantes em um conjunto de exemplos de treinamento por meio de um aumento de novos exemplares. Esta capacidade de gerar novos exemplos, faz com que a RAG seja comumente usada em tarefas de aumento de dados (*Data Augmentation*), principalmente quando o conjunto de exemplos é composto por arquivos multimídia, como imagens digitais (TRAN et al., 2021).

As RAGs são compostas por duas RNAs *Multilayer Perceptron* (MLP) adversárias. As MLPs são RNAs do tipo *Feedforward* com múltiplas camadas ocultas. Em uma arquitetura RAG, uma MLP desempenha o papel generativo, chamada de Gerador (G) e a outra MLP desempenha o papel discriminativo (D). O gerador é responsável por criar os novos exemplos similares aos fornecidos como entrada. Já seu adversário, o Discriminador, é responsável por avaliar os exemplos criados e classificar se eles pertencem ou não ao conjunto original (XIE et al., 2023). A arquitetura da RAG é apresentada na figura 21.

Figura 21 – Arquitetura de uma RAG



Fonte: Adaptado de Xie et al. (2023)

Ao analisar a figura 21, percebe-se a rede Gerador (G) recebe um ruído, e gera a saída $G(z)$. A rede Descriminador (D) recebe o conjunto de treinamento X e a saída $G(z)$ e com essas informações, verifica se as entradas são verdadeiras ou falsas. Ou seja, se a saída $G(z)$ é similar ao conjunto de treinamento.

Assim, a competição entre o Gerador (D) e o Discriminador (D) pode ser entendida da seguinte forma: Enquanto o Descriminador (D) busca maximizar a probabilidade de acerto ao mandar dados sintéticos para o Gerador (G), o Gerador (G) quer minimizar a probabilidade de acerto do discriminador (D). A função objetivo a ser otimizada, também chamada de "*jogo de mínimo e máximo",* que introduz a perda mínima é representada na equação (24):

$$\min_G \max_D E_{x\sim q_{data}(x)}[\log D(x)] + E_{z\sim p(z)}[\log\left(1 - D\left(G(z)\right)\right)] \qquad (24)$$

O treinamento de uma RAG é realizado por meio de um constante aprimoramento do atributo chamado espaço latente. É necessário que o treinamento seja feito desta forma para evitar que uma rede avance mais rápido que a outra. A abordagem pelo espaço latente busca promover um certo equilíbrio no treinamento de ambas as redes. O Espaço latente é uma representação utilizada para agrupar dados com características similares ao posicioná-los em um espaço n-dimensional (XIE et al., 2023).

Dentre os métodos que podem ser utilizados para a geração de novas imagens, pode-se citar a rotação, inversão horizontal ou vertical, a alteração de escala, a inserção de ruído, a inserção, alteração ou substituição de espaços de cores, alterações no contraste e brilho, alteração na forma da imagem e a segmentação em recortes menores (XIE et al., 2023).

Sobre a utilização das RAG para combater crimes cibernéticos, os autores Krundyshev e Kalinin (2021) classificam em quatro grandes áreas possíveis de aplicação. A primeira é no processamento de arquivos multimídia como imagens e vídeos. A segunda é na detecção de anomalias em bases de dados. A terceira é na aplicação de Aumento de Dados. E a quarta é na detecção de *Deepfakes*, ou seja, vídeos falsos criados por IA.

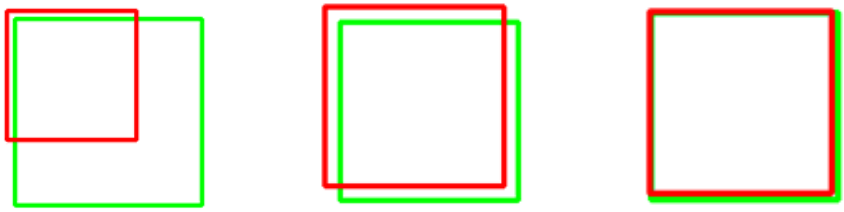
2.3.4. MÉTRICAS APLICADAS NA AVALIAÇÃO DO DESEMPENHO DE TÉCNICAS DA INTELIGÊNCIA ARTIFICIAL

A avaliação de técnicas de IA é uma tarefa essencial para garantir a confiabilidade dos resultados. Para realizar estas avaliações, são utilizadas diversas métricas. Estas métricas não apenas ajudam a avaliar o desempenho das técnicas de IA, mas também fornecem uma base para comparações entre diferentes abordagens (DALIANIS, 2018; ZHOU et al., 2021).

Na tabela 13, são descritas as principais métricas que podem ser utilizadas para avaliar o desempenho de técnicas de IA.

Tabela 13 – Métricas utilizadas na avaliação de desempenho das técnicas de IA

Métrica	**Descrição**	
Distância Euclidiana	É a distância entre dois pontos presentes em um espaço.	$Dist_E = \sqrt{((x_1 - x_2)^2 + (y_1 - y_2)^2)}$ (25)
Distância de Manhattan	Também chamada de distância de Taxi, é a distância entre dois pontos em ângulos retos.	$Dist_{Ma} = \lvert x_1 - x_2 \rvert + \lvert y_1 - y_2 \rvert$ (26)
Distância de Minkowski	É a distância generalizada entre dois ou mais pontos.	$Dist_{Mi} = (\lvert x_1 - x_2 \rvert^m + \lvert y_1 - y_2 \rvert^m)^{\frac{1}{m}}$ (27)
Distância de Hamming	É o número de bits que diferem entre duas strings com a mesma quantidade de caracteres.	$Dist_{Hamm} = \sum \lvert x_i - y_i \rvert$ (28)

Métrica	Descrição
Matriz de Confusão	Métrica usada para evidenciar o total de erros e acertos por meio de uma matriz. Para isso, utiliza-se as seguintes informações: VP, VN, FP e FN VP — Verdadeiro Positivo VN — Verdadeiro Negativo FP — Falso Positivo FN — Falso Negativo A diagonal com os valores verdadeiros (VP e VN) exibe o total de acertos, enquanto a diagonal dos valores falsos (FN e FP) exibe o total de erros. VP | FN FP | VN
Acurácia	Métrica utilizada para exibir o desempenho de um determinado modelo $A = \frac{VP + VN}{VP + VN + FP + FN}$ (29)
Precisão	Métrica utilizada para verificar se um dado pertence a uma determinada classe. $P = \frac{VP}{VP + FP}$ (30)
Recall	Métrica utilizada para evidenciar o total de acertos ao classificar o dado em uma classe $R = \frac{VP}{VP + FN}$ (31)
F-Score	Métrica utilizada para evidenciar a média entre a Precisão e o Recall $F1 = 2 * \frac{Precisão * Recall}{Precisão + Recall}$ (32)
Distância de Hausdorff	É a distância máxima de um conjunto ao ponto mais próximo do outro conjunto. Seu cálculo pode ser representado da seguinte forma: $Dist_{Hau}(A, B) = \max\{\min\{d(a, b)\}\}$ (33)
Interseção sobre União (IoU)	Métrica de avaliação responsável por comparar as regiões retangulares utilizadas na detecção de objetos para determinar sua localizaçao e tamanho. A seguir, são apresentados três exemplos de métricas por IoU (Ruim, Bom e Ótimo), sendo a região verde o valor desejado, e a região vermelha, o valor alcançado na detecção de objetos.  Valor IoU: 0,4034 Ruim — Valor IoU: 0,7330 Bom — Valor IoU: 0,9264 Ótimo IoU pode ser resumido como a área da transposição dividido pela área da união. Sua equação pode ser representada da seguinte forma: $IoU = \frac{\lvert A \cap B \rvert}{\lvert A \rvert \lvert \cup \rvert \lvert B \rvert}$ (34) Para classificação binária, utiliza-se a seguinte equação: $IoU = \frac{VP}{VP + FN + FP}$ (35)

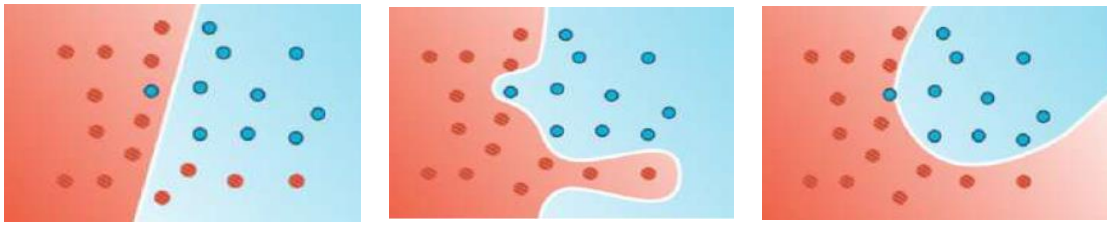
Métrica	Descrição	
Curva ROC	Gráfico que exibe as probabilidades dos resultados VP e FP. Para isto, utiliza-se as seguintes Taxas: TFN Falso Negativo TVN Verdadeiro Negativo TVP Verdadeiro Positivo Quanto maiores os valores de TVN e TVP, em um intervalo de 0 a 1, melhor é o desempenho.	$TFN = \frac{FN}{VP + FN}$ (36) $TVN = \frac{VN}{VN + FP}$ (37) $TVP = \frac{FP}{VN\ + FP} = 1 - TVN$ (38)
Taxa de Erro de Palavras (WER)	Calcula a diferença entre duas palavras. Para isso, considera todos os valores de Inserção, Exclusão e Substituição. Quanto maior o valor da taxa, maior a diferença entre as palavras.	$WER = \left[\frac{S + I + D}{n}\right]$ (39)
Taxa de Erro de Caracteres (CER)	Similar a WER, mede o total de caracteres diferentes em duas palavras, incluindo espaços. Para isso, considera todos os valores de Inserção, Exclusão e Substituição. Quanto maior o valor da taxa, maior será a diferença entre as palavras.	$CER = \left[\ \frac{S + I + D}{n}\ \right] * 100$ (40)

Fonte**:** Adaptado de Nasreen et al. (2023) e Samuelsson (2018).

Ao utilizar as métricas de avaliação das técnicas de IA corretamente, é possível evitar que ocorram problemas, como o *Underfitting* e o *Overfitting*. Ambos significam que não houve uma adequação correta da técnica de IA com os dados fornecidos como entrada (CZAJKOWSKI; KRETOWSKI, 2019).

Enquanto no *Underfitting* a técnica de IA não conseguiu aprender o suficiente sobre os exemplos, o *Overfitting* significa que a técnica aprendeu demais com os exemplos, a ponto de perder a sua capacidade de generalização (Czajkowski; Kretowski, 2019; Oliveira, 2022). Um exemplo de *Underfitting*, *Overfitting* e o "Comportamento Desejado" é ilustrado na figura 22.

Figura 22 – Underfitting, Overfitting e "Comportamento Desejado"



Underfitting *Overfitting* Comportamento Desejado

Fonte: Adaptado de Czajkowski e Kretowski (2019) e Oliveira (2022).

2.4. CRIMES CIBERNÉTICOS

O termo crime cibernético denota a prática de atividades ilícitas mediante a utilização de dispositivos eletrônicos, tais como *smartphones* e computadores. Uma parcela substancial destas atividades já era realizada sem a utilização de dispositivos eletrônicos. Entretanto, com o advento de novas tecnologias, exemplificadas pelos aplicativos de mensagens instantâneas *Telegram* e *WhatsApp*, passaram a serem executadas por meio de dispositivos eletrônicos (CHANDRA; SNOWE, 2020; HO; KO; MAZEROLLE, 2022).

Quando um dispositivo eletrônico é utilizado para cometer um crime, ou quando se torna alvo de um crime, o crime é caracterizado como crime cibernético. Caso contrário, o crime é classificado como tradicional (SEBYAN BLACK; FENNELLY, 2021).

Da perspectiva do criminoso, os crimes cibernéticos são atrativos pois oferecem várias oportunidades, impulsionadas pelo anonimato e ganhos financeiros. O anonimato proporciona ao criminoso a capacidade de ocultar a sua verdadeira identidade e localização, dificultando as atividades investigativas das autoridades policiais. Por sua vez, os ganhos financeiros podem ser altamente lucrativos. Os criminosos podem, por exemplo, apropriar-se de dados confidenciais, como dados de cartões de crédito e vendê-los posteriormente, ou até mesmo utilizá-los em práticas de extorsão (LEE; KANG; KIM, 2023).

No que diz respeito aos impactos gerados pelos crimes cibernéticos, estes podem ser tanto tangíveis, como a perda de equipamentos e dados sensíveis, quanto intangíveis, como a perda de reputação ou de desempenho de um software. Vale destacar que ambos os impactos podem resultar em prejuízo financeiro (CHANDRA; SNOWE, 2020).

Para mitigar os impactos ocasionados por crimes cibernéticos, as entidades responsáveis por estabelecer leis e padrões, em colaboração com outras instituições implementam medidas corretivas, como a promulgação de estruturas legais e a formação de equipes especializadas em respostas à crimes cibernéticos (DONALDS; OSEI-BRYSON, 2019).

Além das leis e padrões, os órgãos e agências internacionais responsáveis pelo combate ao crime cibernético estabelecem categorias para estes crimes. Os autores Ho, Ko e Mazerolle (2022) e Sebyan Black e Fennelly (2021) apresentam uma categorização para estes crimes. De acordo com os autores, a categorização de crimes cibernéticos desempenha um papel crucial na

identificação destas atividades. Uma categorização de crimes cibernéticos é apresentada no Anexo A deste trabalho.

Após identificar um crime cibernético, é importante efetuar a denúncia por meio de uma delegacia eletrônica, um serviço responsável por realizar o registro destes delitos. Iniciativas como a "Central Nacional de Denúncias de Crimes Cibernéticos" desempenham um papel essencial na disseminação de informações acerca das delegacias eletrônicas, além de contribuir para o monitoramento das denúncias (FLORENCIO, 2018).

No âmbito nacional, a lei responsável por tipificar os crimes cibernéticos é a Nº12.737 de 30 de Novembro de 2012 (Brasil, 2012), intitulada: "Lei de tipificação criminal de delitos informáticos". Neste texto, os crimes cibernéticos são descritos e classificados, englobando práticas como a invasão de dispositivos eletrônicos, a interrupção ou perturbação de serviços informáticos e falsificação de documentos.

Embora as leis, normas e denúncias sejam relevantes para combater crimes cibernéticos, muitas vezes ficam aquém da tecnologia utilizada pelos perpetradores. Assim, o combate ao crime cibernético demanda o desenvolvimento de novas estratégias, muitas vezes integrando novas tecnologias, como a Inteligência Artificial (IA) (APRUZZESE et al., 2023).

Há também os crimes cibernéticos relacionados diretamente à grupos vulneráveis, como crianças e adolescentes. Estes grupos enfrentam frequentemente um risco maior de serem alvo de crimes cibernéticos devido a diversos fatores. Estes fatores abrangem uma combinação de elementos sociais, psicológicos e tecnológicos, tornando-os suscetíveis a assédio direcionado. Um exemplo de crime direcionado a crianças e adolescentes é a produção e compartilhamento de arquivos com pornografia infantojuvenil (QUAYLE, 2020; RHOADS, 2023).

2.4.1. PORNOGRAFIA INFANTOJUVENIL

A pornografia infantojuvenil é um crime cibernético previsto na lei nº 11.829, de 25 de novembro de 2008, no artigo 240º, descrita como: "Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente". Esta lei é uma alteração no Estatuto da Criança e do Adolescente (ECA), descrito na lei nº 8.069, de 13 de Julho de 1990 (BRASIL, 2008).

Quanto à definição do público infantojuvenil, o ECA considera criança o indivíduo que possui até 12 anos incompletos, e adolescente aquele que possui de 12 a 18 anos incompletos. Ainda segundo a lei, ambos os públicos gozam de direitos fundamentais, tais como o direito à vida, saúde, liberdade, respeito e dignidade, à convivência familiar e comunitária, e do direito à guarda, à tutela e à adoção (BRASIL, 2008).

Importante destacar a confusão frequente entre os termos “pornografia infantojuvenil” e “pedofilia”, especialmente em meios de comunicação, como canais de televisão e sites. Embora ambos os crimes tenham o mesmo público-alvo como vítima, suas distinções são claras. Enquanto a pedofilia é uma psicopatia caracterizada pela atração sexual compulsiva e obsessiva pelo público infantojuvenil, a pornografia infantojuvenil engloba toda e qualquer exposição de cenas de nudez envolvendo crianças ou adolescentes, desde que apresentem conotação pornográfica (CASTRO; BULAWSKI, 2011; NIRVAN et al., 2023).

Os perpetradores do crime cibernético de pornografia infantojuvenil são classificados em dois tipos: primários e secundários. O perpetrador primário é aquele que explora a vítima, produzindo e divulgando o conteúdo de exploração. Já o perpetrador secundário é aquele que, muitas vezes mediante compensação financeira, incentiva o perpetrador primário. Em grande parte dos casos, o perpetrador primário é alguém próximo a família da vítima, ou mesmo um membro familiar, como pais ou tios (MCCORMACK; LOWE, 2022).

No que tange às vítimas, as meninas representam o dobro das ocorrências em relação aos meninos. Adicionalmente, é pertinente ressaltar que em diversos casos, a exposição a este tipo de crime configura-se como um agravante de outros crimes antecessores, como a relação sexual forçada e o tráfico sexual de menores. Mesmo após a libertação dos criminosos, as vítimas enfrentam consequências pós-traumáticas, como o uso de entorpecentes, depressão e, em casos mais extremos, tentativas de suicídio (BURSZTEIN et al., 2019).

Pelo fato de a pornografia infantojuvenil ser um crime cibernético, sua materialidade é encontrada em arquivos multimídia digitais, como vídeos e imagens. Estes arquivos têm como característica, o ato sexual e a nudez do público infantojuvenil. Adicionalmente, podem ter palavras, textos, símbolos e objetos associados à pornografia infantojuvenil (Laranjeira da Silva et al., 2022). A materialidade do crime de pornografia infantojuvenil é referenciada na literatura por diferentes termos. Os termos identificados são descritos na tabela 14, juntamente com seu acrônimo e os autores responsáveis pela publicação de cada terminologia.

Tabela 14 – Termos utilizados para referenciar a materialidade da Pornografia Infantojuvenil

Termos em Português	**Acrônimos**	**Autores**
Abuso e Exploração Sexual de Crianças	CSEA	(RAMIRO et al., 2019)
Abuso e Exploração Sexual de Crianças Online	OCSEA	(RAMIRO et al., 2019)
Abuso Sexual de Crianças Online	OCSA	(JURINIC; RAMLJAK, 2021)
Exploração Sexual Online de Crianças	OCSE / OSEC	(MCCORMACK; LOWE, 2022)
Imagens de Abuso Sexual de Crianças	CSAI	(GUERRA; WESTLAKE, 2021)
Abuso Sexual de Crianças	CSA	(GUERRA; WESTLAKE, 2021)
Material de Abuso Infantil	CAM	(AL-NABKI et al., 2020)
Material de Abuso Sexual Infantil	CSAM	(LEE et al., 2020)
Material de Abuso Sexual Infantil Online	OCSAM	(LEE et al., 2020)
Material de Exploração de Crianças	CEM	(HOLT et al., 2020)
Material de Exploração Infantil	CSM	(HOLT et al., 2020)
Exploração Sexual Infantil	CSE	(STEEL et al., 2020)
Material de Exploração Sexual Infantil	CSEM / SEM-C	(ANDA; LE-KHAC; SCANLON, 2020)
Imagens Indecentes de Crianças	IIOC	(LARANJEIRA DA SILVA et al., 2022)

Fonte**:** Adaptado de Jurinic e Ramljak (2021) e Ramiro et al. (2019).

A disseminação de pornografia infantojuvenil ocorre predominantemente pela internet, através de plataformas como as redes P2P (*Peer-to-Peer*), *DarkWeb* e mídias sociais. Essa disseminação faz com que os crimes de pornografia infantojuvenil tenham um destaque especial nas operações realizadas por autoridades policiais (KLOESS; WOODHAMS; HAMILTON-GIACHRITSIS, 2021; LEE et al., 2020).

Para detectar a materialidade de pornografia infantojuvenil em exames periciais, utilizam-se técnicas de Computação Forense. A partir do momento em que os vestígios coletados em um processo de cadeia de custódia, estas técnicas são aplicadas nos vestígios em um exame pericial para torná-los evidências (KLOESS; WOODHAMS; HAMILTON-GIACHRITSIS, 2021).

2.5. ESTRATÉGIAS PARA DETECTAR PORNOGRAFIA INFANTOJUVENIL

A detecção e prevenção do crime cibernético de pornografia infantojuvenil é uma tarefa de considerável complexidade. Uma maneira de garantir o sucesso desta tarefa é desenvolver Estratégias ou aprimorar as existentes (NGOX et al., 2022).

As Estratégias podem ser definidas como o conjunto de técnicas integradas de diferentes áreas para alcançar um determinado objetivo. No caso do combate à crimes cibernéticos, as Estratégias envolvem desde o desenvolvimento de sistemas baseados em conhecimento para apoiar a área criminalística e jurídica, até modelos computacionais capazes de traçar e prever perfis psicológicos (COSTANTINI; DE GASPERIS; OLIVIERI, 2019; WAELEN, 2023).

As Estratégias para detecção de evidências de pornografia infantojuvenil podem ser categorizadas em dois tipos principais: As que empregam evidências reais no momento de sua construção e as que fazem uso de dados sintéticos ou secundários para sua construção. Ambas as Estratégias têm mostrado sucesso em diversas aplicações, sendo que a Estratégia que utiliza evidências reais em sua construção é geralmente desenvolvida em conjunto ou sob a supervisão de entidades policiais (LARANJEIRA DA SILVA et al., 2022).

Utilizar Estratégias para detectar evidências de pornografia infantojuvenil é uma forma de solucionar as dificuldades encontradas pelas autoridades policiais (Kloess; Woodhams e Hamilton-Giachritsis, 2021). As principais dificuldades encontradas para detectar evidências de pornografia infantojuvenil são descritas na tabela 15.

Tabela 15 – Principais dificuldades encontradas para detectar evidências de pornografia infantojuvenil

Dificuldade	**Descrição**
Quantidade e Variedade de Arquivos	A quantidade de arquivos presentes em um dispositivo eletrônico torna a busca por evidências um procedimento exaustivo e complexo.
Lesões Corporais	Alteração na aparência da vítima por lesões corporais, além de variações naturais no desenvolvimento sexual de diversos grupos étnicos.
Detecção do Ato Sexual	Ambiguidade de contexto, que pode incluir imagens naturistas e práticas de nudismo.

Fonte**:** Adaptado de Kloess; Woodhams e Hamilton-Giachritsis (2021)

Os autores Povedano Álvarez et al. (2023) e Cifuentes; Sandoval Orozco e García Villalba (2022) realizaram uma revisão sobre as Estratégias existentes na literatura utilizadas na detecção de conteúdos sensíveis. Todas estas Estratégias são descritas na tabela 16.

Tabela 16 – Estratégias para detecção de conteúdo sensível

Estratégia	Descrição
Baseadas em Valores Hash perceptivo	Busca encontrar evidências ao comparar valores Hash já mapeados anteriormente. Microsoft Photo DNA, Facebook PDQ e NeuralHash são exemplos de aplicações encontradas na literatura.
Baseada em Detecção de Pessoas	Busca encontrar pessoas por meio da detecção de pixels com cores de pele. As Estratégias existentes na literatura usam os espaços de cores RGB, HSV e YCbCr de forma isolada ou com operadores lógicos.
Baseada em Nome dos Arquivos e Metadados	Busca detectar evidências pelo conteúdo textual do nome e metadados do arquivo, além do seu caminho de diretório.
Baseada na detecção de Faces, Idade e Gênero	Busca detectar pessoas por meio da identificação de pixels com cores de pele e descritores.
Baseada em Rastreadores Web e Mecanismos de Busca	Busca encontrar evidências em páginas web por meio que Querys construídas com palavras-chave selecionadas.
Baseada em Descritores ou em Fusão	Busca exibir as características de um determinado elemento em uma imagem. Na literatura, são utilizados: SIFT, SURF, HOG, TRoF, Vetores de Movimento e Descritores Binários.

Fonte**:** Adaptado de Povedano Álvarez et al. (2023) e Cifuentes; Sandoval Orozco e García Villalba (2022).

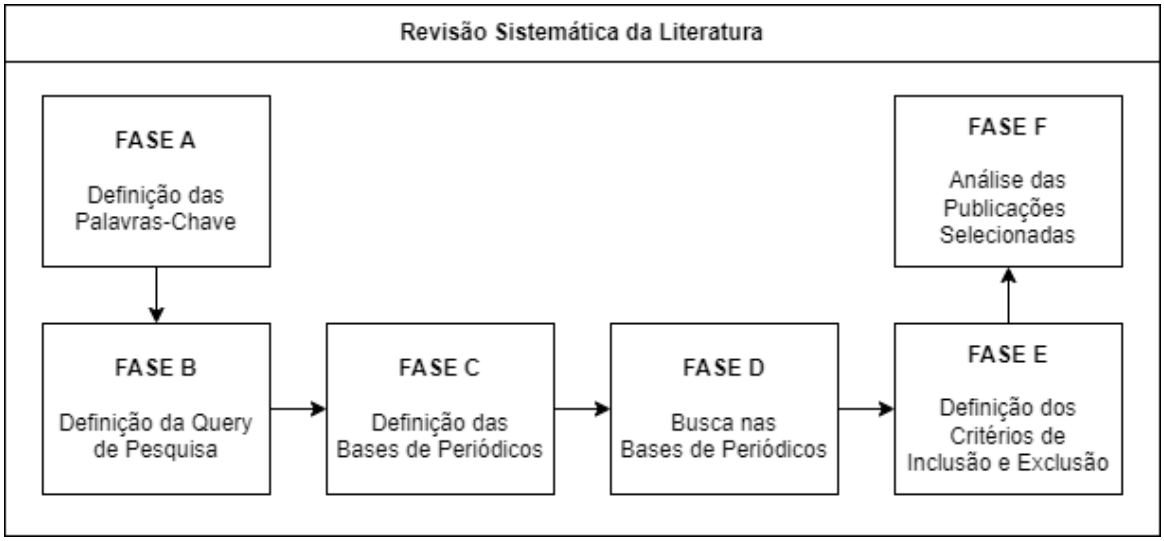
Destaca-se que todas as Estratégias descritas na tabela 16 são formadas por técnicas das áreas computacionais: Computação Forense, VC e IA. Integrar estas técnicas permite obter um ganho de desempenho considerável na detecção de evidências de Pornografia Infantojuvenil (CIFUENTES; SANDOVAL OROZCO; GARCÍA VILLALBA, 2022; POVEDANO ÁLVAREZ et al., 2023).

Adicionalmente, os autores Povedano Álvarez et al. (2023) reforçam a necessidade de aprimorar as Estratégias já existentes identificadas na literatura. Este aprimoramento requer uma abordagem proativa e deve capaz de lidar com grandes quantidades de dados.

2.6. REVISÃO SISTEMÁTICA DA LITERATURA SOBRE PORNOGRAFIA INFANTOJUVENIL

A Revisão Sistemática da Literatura (RSL) é um tipo de método científico usado para sintetizar e analisar todo o conteúdo de pesquisa existente na literatura sobre um determinado tema. Ao contrário das revisões de literatura tradicionais, que podem ser mais subjetivas e menos rigorosas em sua abordagem, a RSL é guiada por métodos bem definidos para garantir um padrão na análise e síntese do conteúdo identificado na literatura (Hiebl, 2023). A RSL realizada neste trabalho é formada por seis fases ilustradas na figura 23.

Figura 23 – Fases da Revisão Sistemática da Literatura



Fonte: Adaptado de Hiebl (2023)

A seguir são descritas as seis fases da RSL sobre o tema de pornografia infantojuvenil.

a) Fase A – Definição das Palavras-Chave: Nesta primeira fase, foram definidas as palavras-chave relacionadas com o tema pornografia infantojuvenil. Optou-se pelas palavras-chave nos idiomas inglês e português, além de seus acrônimos. A escolha do idioma Inglês decorreu da predominância das publicações sobre o tema neste idioma, enquanto o idioma português foi escolhido para identificar o contexto nacional da pesquisa sobre pornografia infantojuvenil.

As palavras-chave definidas nesta pesquisa foram divididas em dois grupos: Termos e Acrônimos. As palavras-chave definidas são apresentadas na tabela 17.

Tabela 17 – Definição das Palavras-Chave

Termos	Acrônimos
Pornografia Infantojuvenil	Não Possui
Child Pornography	CP
Child Sexual Exploitation and Abuse	CSEA
Online Child Sexual Exploitation and Abuse	OCSEA
Online Child Sexual Abuse	OCSA
Online Sexual Exploitation of Children	OSEC
Online Child Sexual Exploitation	OCSE
Child Sexual Abuse Images	CSAI
Child Sexual Abuse	CSA
Child Abuse Material	CAM
Child Sexual Abuse Material	CSAM
Online Child Sexual Abuse Material	OCSAM
Child Exploitation Material	CEM
Child Sexual Material	CSM
Child Sexual Exploitation	CSE
Child Sexual Exploitation Material	CSEM
Sexual Exploitation Material – Children	SEM-C
Indecent Images of Children	IIOC

Fonte: o Autor (2024).

b) Fase B – Definição da Query de Pesquisa: Definiu-se a *query* de pesquisa com as palavras-chave selecionadas na fase A. Por meio desta *query*, busca-se identificar as publicações relacionadas à pornografia infantojuvenil que contenha qualquer uma das palavras-chave definidas anteriormente. A *query* de pesquisa foi definida da seguinte forma:

*"*Pornografia Infantojuvenil*" OR "Child Pornography" OR "Child Sexual Exploitation and Abuse" OR "CSEA" OR "Online Child Sexual Exploitation and Abuse" OR "OCSEA" OR "Online Child Sexual Abuse" OR "OCSA" OR "Online Sexual Exploitation of Children" OR "OSEC" OR "Online Child Sexual Exploitation" OR "OCSE" OR "Child Sexual Abuse Images" OR "CSAI" OR "Child Sexual Abuse" OR "CSA" OR "Child Abuse Material" OR "CAM" OR*

"Child Sexual Abuse Material" OR "CSAM" OR "Online Child Sexual Abuse Material" OR "OCSAM" OR "Child Exploitation Material" OR "CEM" OR "Child Sexual Material" OR "CSM" OR "Child Sexual Exploitation" OR "CSE" OR "Child Sexual Exploitation Material" OR "CSEM" OR "Sexual Exploitation Material – Children" OR "SEM-C" OR "Indecent Images of Children" OR "IIOC".

c) Fase C – Definição das Bases de Periódicos: Definiu-se as seguintes bases de periódicos: *ACM Digital Library*, *Emerald Insight*, *IeeeXplore – Digital Library*, Portal Capes, Scielo e *Science Direct*. As publicações disponíveis no Portal Capes abrangem outras bases de periódicos, tais como *Scopus*, *ProQuest*, *Google Scholar* e *Web of Science*.

d) Fase D – Busca nas Bases de Periódicos: Realizou-se uma busca por publicações nas bases definidas na fase C com a query de pesquisa definida na fase B. Para isso, definiu-se o período de Janeiro de 2000 a Junho de 2024. O total de publicações encontradas é apresentada na tabela 18.

Tabela 18 – Total de Publicações

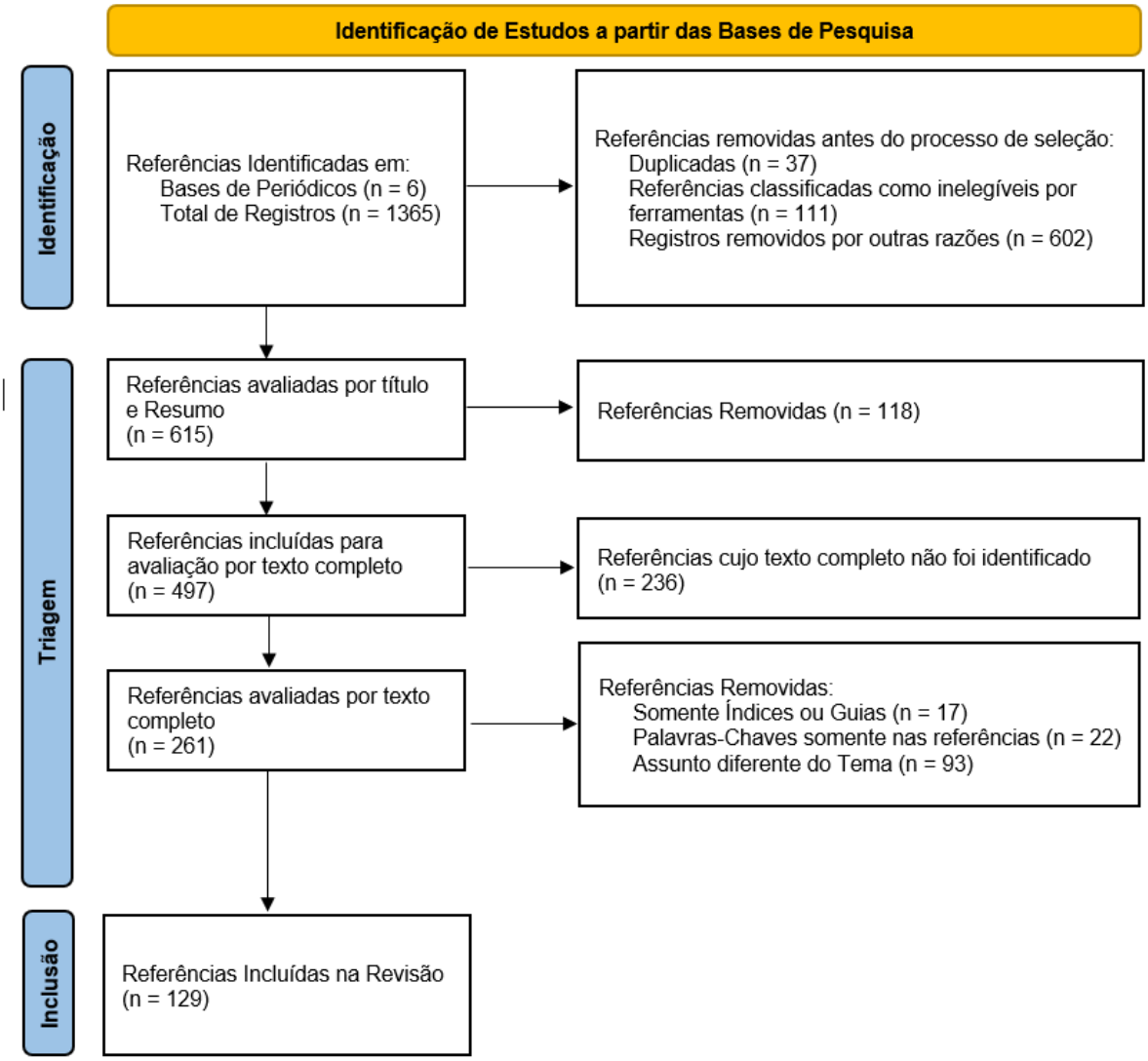
Base de Pesquisa	Total
ACM Digital Library	329
Emerald Insight	268
IeeeXplore - Digital Library	99
Portal CAPES	103
Scielo	165
ScienceDirect	401
Total	**1365**

Fonte: o Autor (2024).

e) Fase E – Definição dos Critérios de Inclusão e Exclusão: Na Fase E, foi definido quais publicações serão consideradas e desconsideradas neste trabalho. Para isso utilizou-se o fluxo de seleção de publicações da metodologia PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*).

A metodologia PRISMA fornece diretrizes para construir relatórios transparentes e conduzir revisões sistemáticas. Seu objetivo é promover a clareza, reprodutibilidade e robustez de uma revisão sistemática (Page et al., 2022). A aplicação da metodologia PRISMA para definir os critérios de Inclusão e Exclusão é ilustrada na figura 24.

Figura 24 – Metodologia PRISMA na definição dos critérios de Inclusão e Exclusão



Fonte: o Autor (2024).

Ao analisar a figura 24, percebe-se que das 1365 publicações identificadas nas bases de periódicos na fase D, somente 129 foram selecionadas nesta fase após aplicar os critérios de inclusão e exclusão por meio da metodologia PRISMA. Assim, foram desconsiderados 1236 itens. Os critérios utilizados para inclusão e exclusão incluíram: Somente índices ou guias, palavras-chave somente nas referências, assuntos diferentes do tema, publicações duplicadas em diferentes bases de periódicos, dentre outros.

f) Fase F – Análise das Publicações Selecionadas: Nesta última fase, foram analisadas todos as 129 publicações selecionadas pelos critérios de Inclusão com a Metodologia PRISMA na fase E. A tabela 19 descreve o total de publicações selecionadas em cada base de pesquisa.

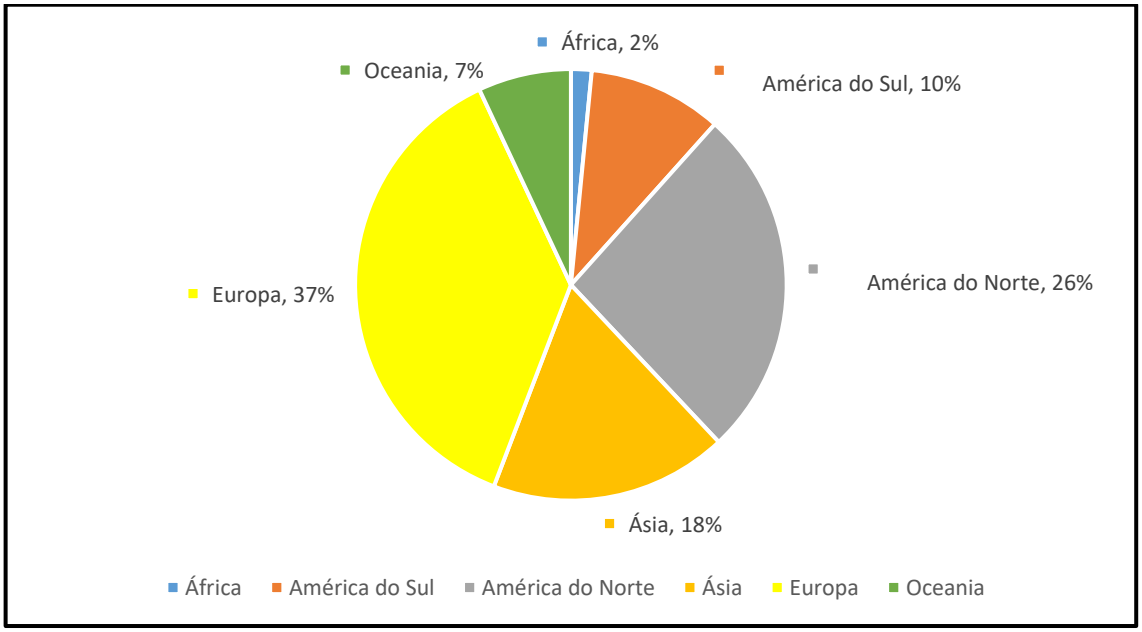
Tabela 19 – Total de Publicações selecionadas

Base de Pesquisa	Total
ACM Digital Library	24
Emerald Insight	9
IeeeXplore - Digital Library	45
Portal CAPES	10
Scielo	8
ScienceDirect	33
Total	**129**

Fonte: o Autor (2024).

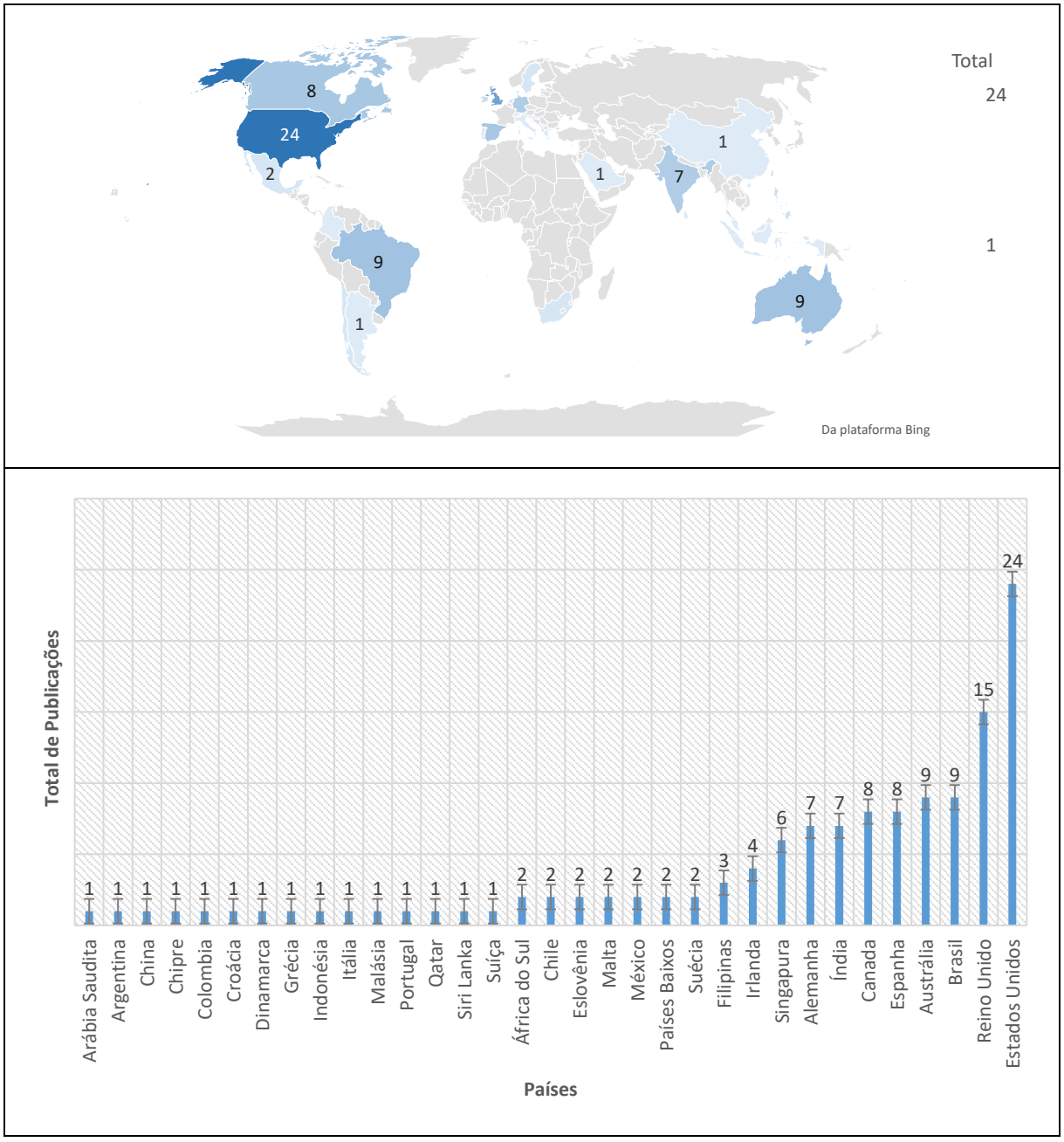
Ao analisar a tabela 19, percebe-se que a maior concentração das publicações sobre o tema de pornografia infantojuvenil estão nas bases *ACM Digital Library*, *IeeeXplore - Digital Library* e *ScienceDirect*. Em seguida, foi realizada uma análise temporal, para poder identificar em qual período está a maior concentração de publicações sobre Pornografia Infantojuvenil. O total de publicações por continentes é apresentado na figura 25 e o total de publicações por país é apresentado na figura 26.

Figura 25 – Total de publicações por continente



Fonte: o Autor (2024).

Figura 26 – Total de publicações por país



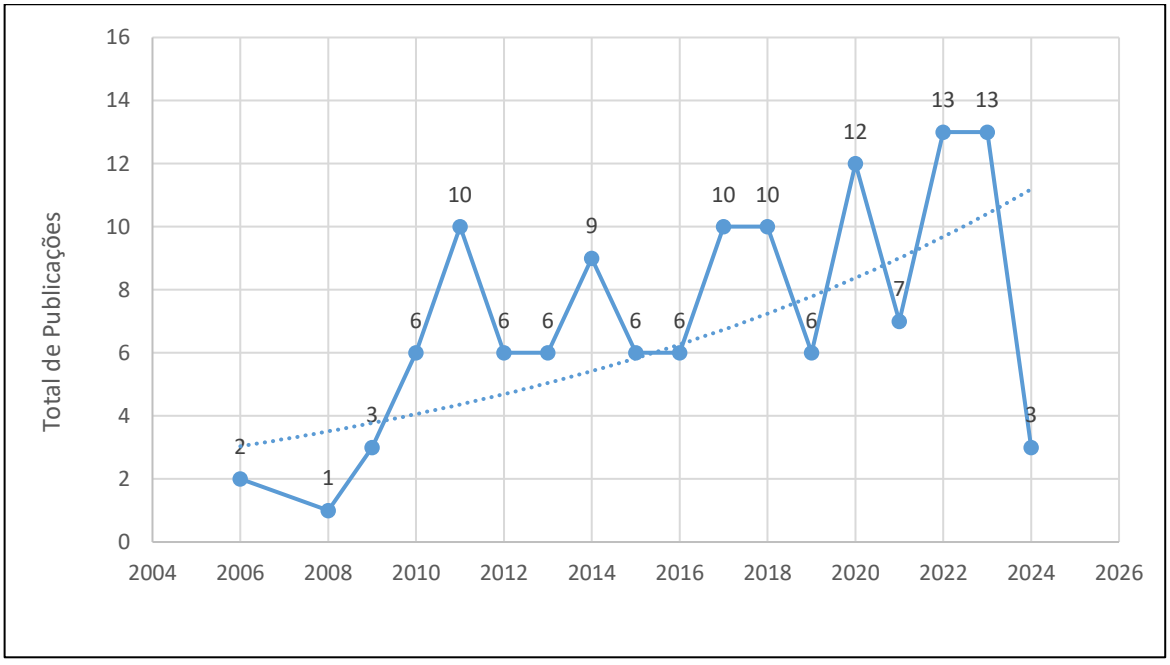
Fonte: o Autor (2024).

Ao analisar as figuras 25 e 26, observa-se que a predominância das publicações está centralizada na Europa com 48,37% das publicações e na América do Norte com 34,26% das publicações. Entre esses, os Estados Unidos lideram na América do Norte com um total de 24 publicações, enquanto o Reino Unido lidera na Europa com um total de 15 publicações. Em seguida, os outros países com a maior quantidade de publicações relacionadas a Pornografia Infantojuvenil são: Brasil e Austrália, ambos com 9 publicações cada, seguidos por Canadá e Espanha, cada um com 8 publicações, e Alemanha e Índia, ambos com 7 publicações.

Os países com a maior concentração de publicações sobre Pornografia Infantojuvenil também possuem os maiores índices de denúncias desse tipo de crime cibernético. De acordo com a *Safernet*, instituição responsável pela **Central de Denúncias de Crimes Cibernéticos**, disponível no endereço eletrônico: https://new.safernet.org.br/denuncie, nos últimos 17 anos, desde 2006, a Central processou um total de 1.973.116 denúncias anônimas de Pornografia Infantil envolvendo 524.197 páginas, sendo o Estados Unidos com a maior quantidade de páginas, um total de 46.665 páginas. Todos os indicadores podem ser acessados por meio do seguinte endereço eletrônico: https://indicadores.safernet.org.br/.

Em seguida, realizou-se uma análise temporal, para poder identificar em qual período se encontra a maior quantidade de publicações sobre Pornografia Infantojuvenil. Destaca-se que o ano de 2024 representa um resultado parcial, visto que o período de desenvolvimento da RSL foi até Junho de 2024. Descobriu-se que a maior concentração ocorreu no período entre 2022 e 2023, sendo que cada um destes anos teve um total de 13 publicações sobre o tema Pornografia Infantojuvenil. As informações sobre o total de publicações por ano são ilustradas na figura 27.

Figura 27 – Total de publicações por ano



Fonte: o Autor (2024).

Concluído a análise temporal, foi realizada uma classificação das publicações pelo tipo de pesquisa. Para isto, analisou-se o resumo, a metodologia e os resultados das publicações para classificá-las em relação a abordagem, objetivos e procedimentos técnicos. A classificação das publicações pelo tipo de pesquisa é ilustrada na tabela 20.

Tabela 20 – Classificação das publicações pelo tipo de pesquisa

Abordagem	Objetivos	Procedimentos Técnicos	Total	%
Qualitativa	Exploratória	**Bibliográfica**	**76**	**59%**
		Survey	5	4%
		Estudo de Caso	2	1,5%
Quantitativa	Descritiva	Experimental	46	35,5%

Fonte: o Autor (2024).

Concluída a classificação, evidenciou-se que as pesquisas qualitativas, destacadas na cor verde, são a maioria sobre o tema de Pornografia Infantojuvenil, com um total de 83 publicações contra 46 publicações descritivas. Todas as publicações qualitativas são categorizadas como exploratórias e apresentam uma concentração significativa em pesquisas bibliográficas. Estas publicações abordam os desafios, impactos, comportamento dos criminosos, legislação e outras características relacionadas a Pornografia Infantojuvenil.

As publicações que adotaram a abordagem quantitativa são classificadas como descritivas e experimentais. Estas publicações descrevem o uso de técnicas, estratégias, abordagens e métodos na detecção de evidências de Pornografia Infantojuvenil. Concluído a classificação, verificou-se quais são os periódicos com a maior quantidade de publicações sobre Pornografia Infantojuvenil. Esta informação é descrita na tabela 21.

Tabela 21 – Periódicos com a maior quantidade de publicações sobre Pornografia Infantojuvenil

Posição	Periódico	Total	%
1º	**Child Abuse and Neglect**	**11**	**14,19%**
2º	Forensic Science International: Digital Investigation	6	7,74%
	Computer Law and Security Review	4	5,16%
3º	Digital Investigation	4	5,16%
	Policing	4	5,16%

Fonte: o Autor (2024).

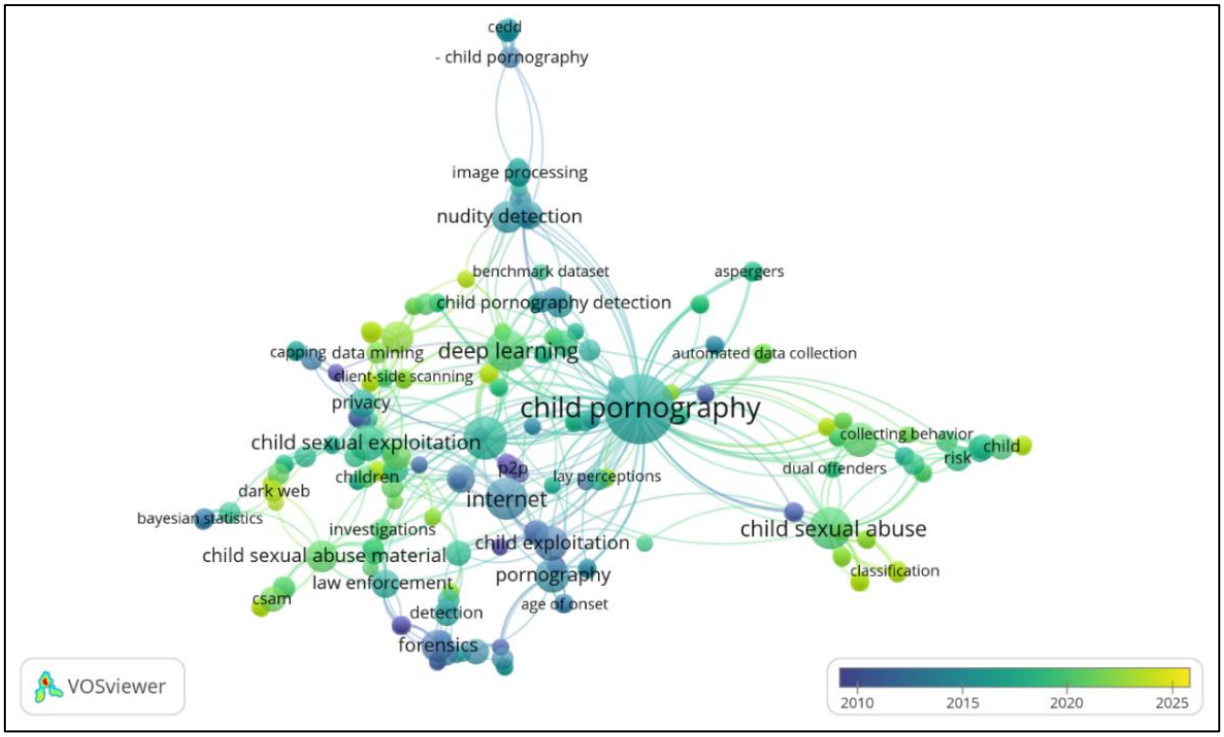
Ao analisar a tabela 21, pode-se verificar os cinco periódicos com as maiores quantidades de publicações sobre Pornografia Infantojuvenil. Estes cinco periódicos concentram 37,41% das publicações selecionadas nesta RSL, ou seja, mais de um terço das publicações. Dentre os

cinco, o periódico com a maior concentração das publicações é o "*Child Abuse and Neglect*" com um total de 11 publicações.

As publicações no periódico "*Child Abuse and Neglect*" são as mais diversas, incluindo discussões sobre propagação de Pornografia Infantojuvenil na internet, impactos globais, principais desafios no combate a este tipo de crime cibernéticos, caracterização dos perfis das vítimas e criminosos, dentre outros. Destaca-se que todas as publicações encontradas neste periódico são classificadas como qualitativa. Sobre os outros quatro periódicos destacados na tabela 21, somente o "*Forensic Science International: Digital Investigation*" possui publicações classificadas como descritivas sobre a detecção de evidências de Pornografia Infantojuvenil. Todos os demais periódicos possuem publicações qualitativas.

Concluída a análise dos periódicos, desenvolveu-se um mapa baseado nas palavras-chave das publicações para identificar aquelas que possuem a maior quantidade de ocorrências e suas inter-relações. O mapa de palavras-chave é apresentado na figura 28.

Figura 28 – Mapa de Palavras-Chave



Fonte: o Autor (2024).

As palavras-chave com a maior quantidade de ocorrências estão dispostas em círculos maiores no mapa, enquanto as palavras-chave com menor quantidade de ocorrências estão em

círculos menores. No mapa, cada palavra-chave é associada a uma cor, e cada cor denota o ano em que a palavra-chave registrou a maior quantidade de menções.

Ao analisar a figura 28, percebe-se que as palavras-chave com a maior quantidade de ocorrências são: "*Child Pornography*", "*Child Sexual Abuse*", "*Child Sexual Exploitation*" e "*Deep Learning*". O termo *Child Pornography* refere-se ao termo Pornografia Infantojuvenil em inglês. Já as palavras-chave "*Child Sexual Abuse*" e "*Child Sexual Exploitation*" referem-se à materialidade da Pornografia Infantojuvenil. Por fim, "*Deep Learning*" refere-se as RNAs multicamada usadas na resolução de problemas de classificação. Baseando-se na figura 28, desenvolveu-se uma linha do tempo para ilustrar a evolução das publicações relacionadas a Pornografia Infantojuvenil. A linha do tempo é ilustrada na figura 29.

Figura 29 – Linha do tempo sobre a evolução das publicações sobre Pornografia Infantojuvenil

Fonte: o Autor (2024).

As primeiras publicações envolvendo pornografia infantojuvenil anterior aos anos 2000 tinham como objetivo entender a motivação dos criminosos para produzir este tipo de conteúdo. A materialidade de Pornografia Infantojuvenil citada nestas publicações, englobava fotografias, vídeos, apresentações visuais e simulações teatrais contendo representações de atos sexuais envolvendo o público infantojuvenil. Adicionalmente, durante este período, as publicações buscavam entender como os efeitos derivados do consumo de pornografia de forma geral poderiam impactar e gerar interesse no consumo de pornografia infantojuvenil.

Entre os anos 2000 até 2010, as publicações abordam a disseminação de Pornografia Infantojuvenil na internet, com ênfase em mídias sociais e redes P2P. Neste período, emerge o termo "*Sexting*", utilizado principalmente por adolescentes em aplicativos e mídias sociais para a produção e compartilhamento de imagens de nudez e atividades sexuais.

Entre os anos de 2011 e 2012, as publicações abordam a detecção de evidências de pornografia infantojuvenil através de técnicas da área da Computação Forense, como os algoritmos de Hash MD5, SHA1 e SHA256, Webcrawlers e mecanismos de busca, bem como a detecção de cor de pele utilizando o espaço de cor RGB. Além disso, passou-se a investigar o *Torrent*, outra plataforma de disseminação de arquivos na internet similar as redes P2P.

Entre os anos de 2013 e 2015 intensifica-se as publicações relacionadas a detecção de pornografia infantojuvenil. São desenvolvidos e aplicados novas Estratégias e técnicas na detecção de evidências de Pornografia Infantojuvenil. Algumas das palavras-chave destas publicações são: "*Child Pornography Detection*", "*Nudity Detection*" e "*Investigations*". Adicionalmente, as áreas da Computação Forense, IA e VC passam a ser mencionadas nas publicações através das palavras-chave: "*Statistics*", "*Forensics*", e "*Image Processing*".

Ainda no período de 2013 a 2015, há publicações específicas sobre a regulamentação de mídias sociais. Este tema envolve a definição de responsabilidades de propagar pornografia infantojuvenil em mídias sociais. Nos Estados Unidos por exemplo, as revelações feitas por *Edward Snowden* em 2013 sobre práticas de vigilância em massa realizadas por plataformas de mídias sociais promoveram a discussão sobre privacidade e vigilância governamental.

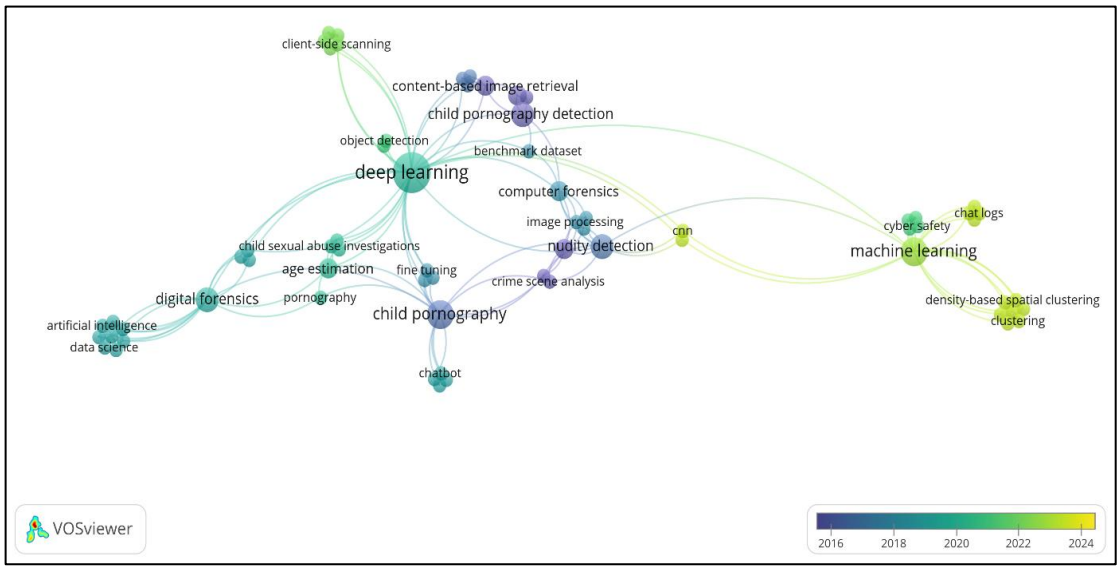
Entre 2016 e 2019, algumas publicações sobre Pornografia Infantojuvenil permanencem na discussão sobre a regulamentação de mídias sociais. As Palavras-chave "*Cyberbulling*" e "*CyberLaw*" revelam essa continuidade. Além disso, novas plataformas passam a ser usadas para disseminar Pornografia Infantojuvenil: a *Darknet* e a *Darkweb.* Importante esclarecer a diferença entre *DarkNet* e *Darkweb*. Enquanto a *Darknet* refere-se as redes privadas indexadas por ferramentas específicas como *RedOnion* e *I2P*, a *Darkweb* refere-se as redes ocultas não indexadas. Para concluir este período, percebe-se um crescimento das publicações envolvendo a utilização de técnicas da IA, principalmente com a adoção das RNAs de Aprendizagem profunda, como as RNCs.

Por fim, de 2020 a 2024, as palavras-chave destacadas no mapa estão relacionadas com as técnicas de IA, como: "*Data Mining*", "*Deep Learning*", "*Classification*" e "*Automated Data Collection*". Percebe-se assim uma predominância na utilização das técnicas de IA para apoiar a detecção de evidências de Pornografia Infantojuvenil.

Percebendo essa tendência de utilizar IA com Computação Forense e VC, a partir de 2013 e intensificado nos anos posteriores, realizou-se uma análise nas publicações sobre Pornografia

Infantojuvenil que mencionam as seguintes palavras-chave: “*Artificial Intelligence*”, “*Natural Language Processing*”, “*Pattern Recognition*”, “*Robotic*” e “*Machine Learning*”. Das 129 publicações selecionadas nesta RSL, 28 publicações utilizaram técnicas de IA. As 28 publicações são descritas no Apêndice A deste trabalho. Um mapa de palavras-chave das publicações que abordam Pornografia Infantojuvenil e IA é ilustrado na figura 30.

Figura 30 – Mapa de Palavras-Chave das publicações que abordam Pornografia Infantojuvenil e IA



Fonte: o Autor (2024).

Na figura 30, percebe-se que as publicações que abordam Pornografia Infantojuvenil e IA possuem como as palavras com as maiores ocorrências: “*Child Pornography*” e “*Deep Learning*”. Desde antes de 2016, as publicações mencionam a utilização da IA para apoiar a detecção de evidências de Pornografia Infantojuvenil.

As primeiras palavras-chave destacam a prática de detecção de nudez por meio da classificação de cor de pele nos pixels das imagens e a análise de cenas de crimes. Já as publicações datadas entre 2018 e 2022 abordam a detecção de objetos e a estimação de idade com “*Deep Learning*” relacionadas com as áreas: “*Artificial Intelligence*”, “*Data Science*” e “*Digital Forensics*”. Já as publicações mais recentes datadas a partir de 2022 em diante, abordam as CNN, em português, RNC, além de “*Machine Learning*” e “*ChatLogs*”. Assim, percebe-se que além da detecção de evidências de pornografia infantojuvenil em arquivos de imagens com as RNCs, as publicações buscam investigar conteúdo textual também relacionado com este crime cibernético em locais como Chats de mídias sociais e outras plataformas disponíveis na internet.

Para utilizar as técnicas de IA com VC e Computação Forense na detecção de evidências de pornografia infantojuvenil, é necessário em boa parte das vezes treinar a IA que será utilizada. No caso de detecção de evidências de pornografia infantojuvenil, a posse de arquivos com este conteúdo é definida pela lei como crime cibernético. Verificou-se nestas publicações como foi feito o treinamento das técnicas de IA, mais especificamente, que tipos de imagens foram utilizadas. Essa informação é descrita na tabela 22.

Tabela 22 – Tipos de Imagens utilizadas para Treinar as técnicas de IA

Treinamento	Total	%
Imagens Reais de Pornografia Infantojuvenil?	7	25%
Imagens de Pornografia em Geral?	6	21,5%
Imagens Sintéticas?	**12**	**42,8%**
Não utilizou nenhuma Imagem - Somente Surveys e Revisões da Literatura	3	10,7%

Fonte: o Autor (2024).

Ao analisar a tabela 22, entende-se que a maior concentração das publicações utilizou imagens sintéticas que não estão diretamente relacionados com pornografia infantojuvenil. Este treinamento representa 42,8% das publicações identificadas. Estas publicações utilizaram por exemplo, bases de imagens com indivíduos aleatórios e bases de cores de pele. Já a segunda maior concentração com 25% das publicações descreve o uso de imagens reais de pornografia infantojuvenil no treinamento da IA. Nestas publicações, ocorreram a participação direta de uma entidade policial, seja como autor ou como supervisor. Destaca-se que das 7 publicações identificadas, 6 são estudos brasileiros, enquanto a outra publicação é um estudo alemão.

Há também as publicações que utilizaram pornografia em geral para o treinamento da IA proposta em seus estudos. Representando 21,5%, estas publicações tentam detectar utilizando elementos que são comuns em ambos os casos de pornografia, como a identificação de pessoas, faces e gênero. Por fim, há as publicações que não realizaram treinamento para IA. Estas publicações se caracterizam como *Surveys* e Revisões e apenas mencionam o uso da IA. Esta última, representa 10,7% com um total de 3 publicações.

Por fim, há também as publicações que fazem referência ao uso da IA na detecção de conteúdo textual relacionado a Pornografia Infantojuvenil. Nesta RSL, identificou-se duas publicações conduzidas pelos autores Frank, Westlake e Bouchard (2010) e Wang et al. (2023) que listam as principais palavras-chave relacionadas com Pornografia Infantojuvenil. As

palavras-chave identificadas nestas publicações são descritas na Tabela 23, sendo que as palavras-chave com asterisco (*) podem representar qualquer caractere a partir deste símbolo.

Tabela 23 – Palavras-Chave relacionais com Pornografia Infantojuvenil

Grupo	Palavras-Chave
Pornografia Infantojuvenil (36)	cjb, ddoggprn, gomon, halyavapictures, hmv, hussyfan, kdquality, kdv, kidzilla, kinder*, kingpass, komorka, jagget, lsm, lso*, mafiasex, nimphet*, nympet*, paedo*, pedfilia, pedo*, pedphilia, pjk, phtc, propthc, ptsc, qqazz, QWERTY, R@ygold, raygold, rbv, reelkiddymov, t4c, tihjj, yamad, youngvideomodels.
Símbolos Chineses (14)	萝 莉(loli), 幼(jovem), 初 中(colegial), 高 中(ensino médio), 中 学(ensino fundamental), 小(jovem/pequeno), 岁(idade/ano), 童(criança), 年轻 (jovem/adolescente), 少(jovem), 妹(irmã), 弟(irmão), 孩(criança), 未 成年 (menor de idade).
Idade (9)	“X y”, “X-yo”, “Xyo”, “X year”, “X years”, “X years old”, “X y”, “X ano”, “X y/o”, Sendo X um valor entre 0 e 17, ou mesmo o número por extenso.
Público Infantojuvenil (40)	adolescent, angel*, babe*, baby*, bebe, boy*, chaby, child*, diaper, enfant, eurololita, fallenangelfuns, "florian boy", gamine, girl*, hairless, indecent, infant*, innocent, kid*, kindergarten, little, love, lola*, loli*, loll*, petite, post-pubescent, postpubescent, pre-pubescent, prepubescent, preteen*, pretten, school, smooth, teen*, thick, toddler, tween, underage, young*.
Ato Sexual (96)	abuse*, anal*, animalsex, anus, ass*, bath*, BDSM, bitch, blowjob, bondage, cock*, creampie, cum*, cunt, defloration, dfloration, dildo, doggy*, ejac*, erection, erotic, eurosex, exhib, facia*, fellation, fetish, fisting, fuck*, gangbang, gay, groupsex, handjob, hardcore, hentai, incest, inzest, jailbait, jacking off, jeezy, jizz, JOP, lesbian, lickin*, liluplanet, lingerie, masterb*, mastur*, naked, nakie, naturist, necrofilia, nse, nua, nude, nudit*, nudist*, oral, orgasm, orgy, pee, penetrat*, penis, piss, pnis, pntration, porn*, prostitu*, purenudism, pussy, rape*, sado*, sex*, shemale, shower, slut*, sodom*, soumise, spank*, sperm*, spread*, suce, suck*, swallow, torture, transexual, twink, upskirt, vagina, virgin, voyeur, whore, xxx, yasuda, zofilia, zoofilia, zoophilia.
Tecnologia (14)	"DarkNet", "DarkWeb", "DeepWeb", Anonymizer, BitTorrent, In-Private, Livestream, Onion, P2P, Peer-To-Peer, TOR, Torrent, Usenet, Webcam.

Fonte**:** Adaptado de Frank, Westlake e Bouchard (2010) e Wang et al. (2023)

Por fim, foram selecionados os artigos que mais contribuíram com o desenvolvimento deste trabalho. Dos 129 selecionados com o PRISMA, 18 foram os mais aderentes. A seleção se deu com base na importância dos trabalhos que exploraram o tema da Pornografia infantojuvenil, seja por meio de levantamentos bibliográfico, surveys e revisões da literatura, ou mesmo com experimentos, desenvolvimento de Estratégias e outras soluções para combater este tipo de crime cibernético.

As 18 publicações mais aderentes ao tema deste trabalho são descritas na tabela 24.

Tabela 24 – As 18 publicações mais aderentes ao tema deste trabalho

ID	Ano	Título	Publicação	Descrição	Autores
01	2018	A Benchmark Methodology for Child Pornography Detection	31st SIBGRAPI Conference on Graphics, Patterns and Images	Detecção de Evidências de Pornografia Infantojuvenil por meio da detecção de faces, cor de pele e estimativa de idade.	(MACEDO; COSTA; DOS SANTOS, 2018)
02	2018	A Machine Learning-based Forensic Discriminator of Pornographic and Bikini Images	International Joint Conference on Neural Networks	Detecção de Evidências de Pornografia Infantojuvenil por meio da detecção de cor de pele e formas de biquini.	(MOREIRA; FECHINE, 2018)
03	2020	Evaluating Performance of an Adult Pornography Classifier for Child Sexual Abuse Detection	Computer Vision and Pattern Recognition	Detecção de Evidências de Pornografia Infantojuvenil por meio da Análise do título do arquivo, detecção de órgãos sexuais, faces, gênero, estimativa de idade e valores Hash.	(AL-NABKI et al., 2020)
04	2020	Short Text Classification Approach to Identify Child Sexual Exploitation Material	Nature	Detecção de Evidências de Pornografia Infantojuvenil por meio da análise do conteúdo textual no título e no caminho de arquivos e seus diretórios.	(AL-NABKI et al., 2023)
05	2020	DeepUAge: Improving Underage Age Estimation Accuracy to Aid CSEM Investigation	Forensic Science International: Digital Investigation	Detecção de Evidências de Pornografia Infantojuvenil por meio da estimativa de idade.	(ANDA; LE-KHAC; SCANLON, 2020)
06	2021	Digital forensics supported by machine learning for the detection of online sexual predatory chats	Forensic Science International: Digital Investigation	Detecção de Evidências de Pornografia Infantojuvenil por meio da análise do conteúdo textual em chats de mídias sociais.	(NGEJANE et al., 2021)
07	2017	Forensic Image Inspection Assisted by Deep Learning	ARES '17: International Conference on Availability, Reliability and Security	Detecção de Evidências de Pornografia Infantojuvenil por meio da detecção de cor de pele, formas de biquini e órgãos sexuais.	(MAYER; STEINEBACH, 2017)
08	2010	NuDetective: a Forensic Tool to Help Combat Child Pornography through Automatic Nudity Detection	Workshops on Database and Expert Systems Applications	Detecção de Evidências de Pornografia Infantojuvenil por meio da detecção de cor de pele.	(POLASTRO; DA SILVA ELEUTERIO, 2010)
09	2021	Pornographic content classification using deep-learning	DocEng '21: 21st ACM Symposium on Document Engineering	Detecção de Evidências de Pornografia Infantojuvenil por meio da detecção de órgãos sexuais.	(TABONE et al., 2021)
10	2023	Comprehensive Review of Cybercrime Detection Techniques	IEEE Access	Revisão da Literatura sobre as principais técnicas de Computação Forense utilizadas para detectar evidências de crimes cibernéticos.	(AL-KHATER et al., 2020)

ID	Ano	Título	Publicação	Descrição	Autores
11	2020	Detecting child sexual abuse material: A comprehensive survey	Forensic Science International: Digital Investigation	Survey sobre a detecção de evidências de Pornografia Infantojuvenil.	(LEE et al., 2020)
12	2022	Investigation, Detection and Prevention of Online Child Sexual Abuse Materials: A Comprehensive Survey	International Conference on Computing and Communication Technologies	Survey sobre a investigação, prevenção e detecção de evidências de Pornografia Infantojuvenil.	(NGOX et al., 2022)
13	2023	Learning Strategies for Sensitive Content Detection	Eletronics	Survey sobre os tipos de Estratégias existentes na literatura para detecção de conteúdo sensível, incluindo a materialidade de Pornografia Infantojuvenil	(POVEDANO ÁLVAREZ et al., 2023)
14	2022	A survey of artificial intelligence strategies for automatic detection of sexually explicit videos	Multimedia Tools and Applications	Revisão sobre as Estratégias existentes na literatura com IA para detecção de conteúdos sexualmente explícitos em vídeos, incluindo a materialidade da Pornografia Infantojuvenil.	(CIFUENTES; SANDOVAL OROZCO; GARCÍA VILLALBA, 2022)
15	2017	Pornography and Child Sexual Abuse Detection in Image and Video: A Comparative Evaluation	8th International Conference on Imaging for Crime Detection and Prevention	Revisão da literatura sobre as Estratégias existentes na literatura para detectar a materialidade de Pornografia Infantojuvenil	(GANGWAR et al., 2017)
16	2022	Seeing without Looking: Analysis Pipeline for Child Sexual Abuse Datasets	FAccT '22: ACM Conference on Fairness, Accountability, and Transparency	Revisão sobre como as Estratégias de detecção da materialidade de pornografia infantojuvenil podem explorar bases com este conteúdo e também propor modelos de acesso a este tipo de base.	(LARANJEIRA DA SILVA et al., 2022)
17	2021	The challenges of identifying and classifying child sexual exploitation material: Moving towards a more ecologically valid pilot study with digital forensics analysts	Child Abuse & Neglect	Descrição dos principais desafios e limitações para detectar e classificar a materialidade de Pornografia Infantojuvenil	(KLOESS; WOODHAMS; HAMILTON-GIACHRITSIS, 2021)
18	2019	A Practitioner Survey Exploring the Value of Forensic Tools, AI, Filtering, & Safer Presentation for Investigating Child Sexual Abuse Material (CSAM)	Digital Investigation	Revisão da literatura sobre como a IA pode aumentar a performance de ferramentas e técnicas de Computação Forense, de modo a reduzir o número de falsos positivos nos resultados da detecção de evidências em uma investigação de Pornografia Infantojuvenil	(SANCHEZ et al., 2019)

Fonte**:** o Autor (2024).

Na tabela 24 estão descritas as 18 publicações que contribuíram para o desenvolvimento deste trabalho. Todas as publicações estão destacadas em quatro cores diferentes: Amarelo, Laranja, Azul e Verde, indicando que:

- As publicações com os IDs 01 até 09 destacadas em amarelo referem-se ao uso de técnicas e Estratégias aplicadas na detecção de Pornografia Infantojuvenil;
- As publicações com os IDs 10 até 15 destacadas em azul trata-se de levantamentos bibliográficos, revisões da literatura e *surveys* sobre Pornografia Infantojuvenil;
- A publicação com o ID 16 destacada em laranja refere-se as formas de se manusear bases de imagens com pornografia infantojuvenil e;
- As publicações com os IDs 17 e 18 destacadas na cor verde discutem os desafios e limitações relacionadas a detecção de Pornografia Infantojuvenil e como superá-las.

Ao analisar a tabela 24, percebe-se que não foi abordado até então o desenvolvimento de Estratégias para detectar imagens alteradas ou similares, identificar pessoas em imagens através da detecção de cor de pele utilizando uma base de cores de pele enriquecida com outros espaços de cores, além de RGB, a extração e estruturação de metadados e conteúdo textual em imagens com OCR e PLN e a aplicação de aumento de dados e detecção de objetos para encontrar objetos relacionados a crimes envolvendo o público infantojuvenil. Isto revela a importância deste trabalho, ao buscar contribuir para o preenchimento desta lacuna na literatura científica.

Os materiais e métodos utilizados neste trabalho, bem como a descrição dos experimentos realizados são apresentados no capítulo 3.

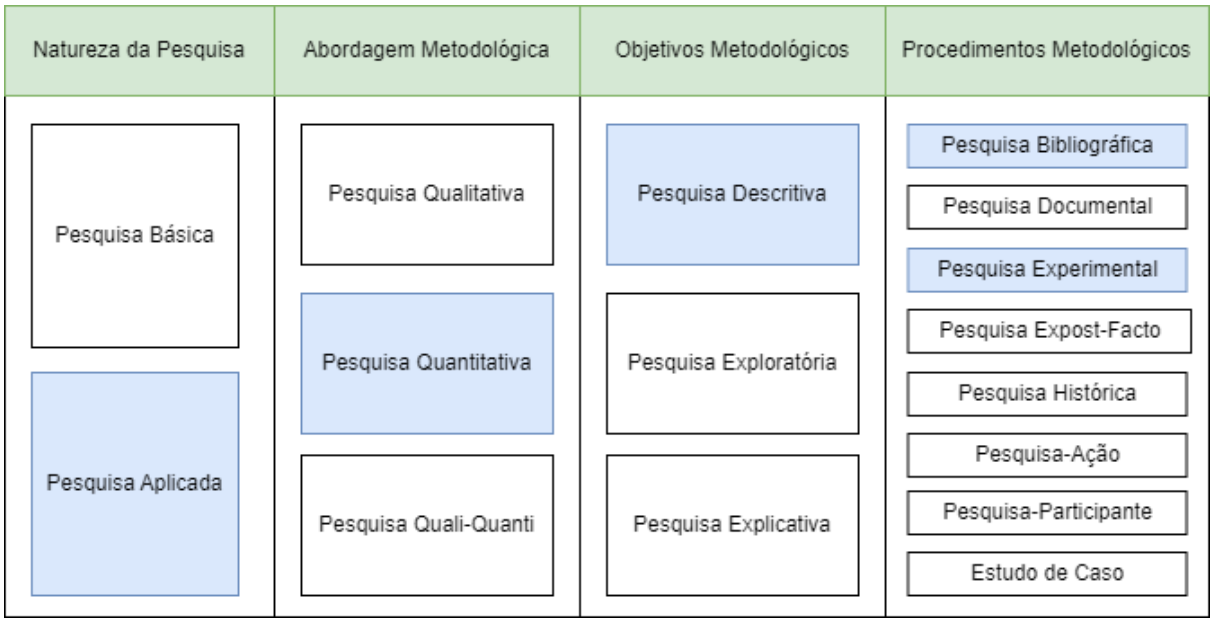
3. MATERIAIS E MÉTODOS

Nesta seção são descritos os materiais e métodos usados para a realização deste trabalho.

3.1. CARACTERIZAÇÃO METODOLÓGICA

A figura 31 apresenta a caracterização metodológica, e os elementos destacados em azul foram os aplicados neste trabalho

Figura 31 – Caracterização Metodológica



Fonte: o Autor (2024).

A metodologia de pesquisa deste trabalho é definida, com base em sua natureza, como pesquisa aplicada. Este tipo de metodologia tem como objetivo solucionar problemas do mundo real ao produzir conhecimento novo. Em relação a abordagem metodológica, este trabalho é classificado como quantitativo. A Pesquisa quantitativa usa diversas técnicas estatísticas para metrificar os resultados obtidos e assim, descrever as causas de um fenômeno, e até as relações entre variáveis que produzem este fenômeno (KUMAR, 2018).

Sobre os objetivos metodológicos, este trabalho é do tipo descritivo. A pesquisa descritiva tem como objetivo descrever as características de uma população ou fenômeno, ou estabelecer relações entre variáveis. Quanto aos procedimentos técnicos, esta pesquisa caracteriza-se como experimental. A pesquisa experimental consiste em determinar um objeto de estudo e selecionar as variáveis que podem influenciá-lo. Para isso, define-se os controles e como serão observados os fenômenos que as variáveis produzem no objeto de estudo (KUMAR, 2018).

3.2. BASE DE DADOS E PLATAFORMA DE ENSAIOS

Os experimentos computacionais foram realizados em um Notebook Samsung Book X55 com as seguintes configurações: Processador Intel Core i7-10510U, 16 Gigabytes de memória RAM, Disco rígido de 1 Terabyte de armazenamento e a Placa de vídeo Nvidia Geforce Mx110 com 2 Gigabytes de memória de vídeo. Os códigos usados nesse trabalho foram desenvolvidos com a linguagem Python. Escolheu-se esta linguagem de programação devido a variedade de recursos disponíveis para as áreas: Computação Forense, VC e IA. Os softwares utilizados são descritos na tabela 25.

Tabela 25 – Softwares utilizados

Software	**Descrição**	**Utilização**	**URL**
Binarscii	Biblioteca para conversão de números decimais em ASCII	Converter os valores Hash para ASCII	https://docs.python.org/3/library/binascii.html
ColorMath	Biblioteca para Manipulação de Espaços de Cores	Converter de RGB para Outros Espaços de Cores	https://python-colormath.readthedocs.io/en/latest/
ColorSys	Biblioteca para Manipulação de Espaços de Cores	Converter de RGB para Outros Espaços de Cores	https://docs.python.org/pt-br/3/library/colorsys.html
Darknet	Biblioteca Customizada do Yolo	Aplicar Transfer Learning para Ganho de Desempenho no treinamento da RNC	https://github.com/AlexeyAB/darknet
EasyOCR	Biblioteca para Aplicação de OCR	Aplicar OCR para Extração de Conteúdo Textual de Imagens	https://github.com/JaidedAI/EasyOCR
ImageHash	Biblioteca para Cálculo de Hash Perceptivo	Executar cálculos dos algoritmos de Hash Perceptivos	https://pypi.org/project/ImageHash/
Imgaug	Biblioteca para Aplicar o Aumento de Dados	Aplicar o Aumento de Dados com as Redes Adversárias Generativas.	https://pypi.org/project/imgaug/
Jupyter Notebook	IDE de Desenvolvimento em Python	Desenvolver códigos em Python	https://jupyter.org/
LabelMe	Biblioteca para Desenho de Caixas Delimitadoras	Desenhar as Caixas Delimitadoras para treinar as RNCs	https://github.com/labelmeai/labelme
Matplotlib	Biblioteca para Visualização de Dados em Python	Visualizar e manipular imagens.	https://matplotlib.org/
Ms Excel	Planilha Eletrônica	Desenvolver Gráficos e analisar os Resultados dos Experimentos	https://www.microsoft.com/pt-br/microsoft-365/excel
NLTK	Biblioteca para Aplicação de PLN	Pré-processar o Texto Extraído com OCR	https://www.nltk.org/
Numpy	Biblioteca para computação científica em Python	Executar tarefas de cálculo	https://numpy.org/

Software	Descrição	Utilização	URL
OpenCV	Biblioteca para Manipulação de Imagens	Executar tarefas de manipulação de imagens.	https://pypi.org/project/opencv-python/
Pandas	Biblioteca para análise de dados em Python	Executar cálculos e validações com os valores dos pixels da imagem.	https://pandas.pydata.org
Sklearn	Biblioteca para Aprendizagem de Máquina e IA	Desenvolver, executar e avaliar as técnicas de IA	https://scikit-learn.org/stable/
Tensorflow	Biblioteca para Aplicação de Técnicas de IA	Treinar a RNC	https://www.tensorflow.org/
Tesseract	Biblioteca para Aplicação de OCR	Aplicar OCR para Extração de Conteúdo Textual de Imagens	https://pypi.org/project/pytesseract/
Torchmetrics	Biblioteca para Aplicação de Métricas em Python	Calcular as Taxas de Erro de Palavras e de Erro de Caracteres	https://lightning.ai/docs/torchmetrics/stable/
Yolo	Sistema utilizado para Detecção de Objetos	Aplicar a RNC para Detectar Objetos	https://pjreddie.com/darknet/yolo/

Fonte: o Autor (2024).

Sobre ás bases usadas neste trabalho, foram selecionadas três, todas categorizadas como fontes secundárias. Isso significa que não há necessidade de submeter estas bases a um comitê de ética em pesquisa. Dados secundários referem-se àqueles que já foram coletados, tabulados, ordenados ou analisados com o objetivo de atender às necessidades de uma pesquisa (YU et al., 2024).

As três bases de dados utilizadas são apresentadas na tabela 26.

Tabela 26 – Relação das três Bases de Dados utilizadas

ID	Base de Dados	Estratégia	Total de Registros	Autoria	Utilização	Descrição da Base
01	Skin Segmentation	B	245.057	(BHATT; DHALL, 2012)	Treinar a técnica Floresta Aleatória para classificar as cores dos pixels em cor de pele e não-cor-de-pele.	A base é composta por 245.057 registros, das quais 50.859 são amostras de cor de pele e 194.198 são amostras de não-cor-de-pele. Os registros são formados por valores R, G e B coletados de imagens faciais de pessoas de diversas faixas etárias (Jovens, Adultos e Idosos), grupos raciais (Brancos, Negros e Asiáticos) e gêneros. A base foi desenvolvida no Laboratório de Envelhecimento Produtivo, Universidade do Texas em Dallas: https://pal.utdallas.edu/facedb/
02	RGB_HSV_YCBCR	B	245.057	Adaptado de (BHATT; DHALL, 2012)	Treinar a técnica Floresta Aleatória para classificar as cores dos pixels em cor de pele e não-cor-de-pele.	Trata-se da base *Skin Segmentation* enriquecida com outros 2 espaços de cores além do RGB. São eles: HSV e YCbCr. A base passou a ser composta por 245.057 registros e um total de 10 atributos.
03	All Layers	B	245.057	Adaptado de (BHATT; DHALL, 2012)	Treinar a técnica Floresta Aleatória para classificar as cores dos pixels em cor de pele e não-cor-de-pele.	Trata-se da base *Skin Segmentation* enriquecida com outros 11 espaços de cores além do RGB. São eles: CMY, CMYK, Xyz, yxY, Yiq, CIE-L*ab, CIE-Lch, CIE-Luv, HSL, HSV e YCbCr. A base passou a ser composta por 245.057 registros e um total de 38 atributos.

Fonte: o Autor (2024).

As dez bases de imagens utilizadas são apresentadas na tabela 27.

Tabela 27 – Relação das dez Bases de Imagens utilizadas

ID	Base de Imagens	Estratégia	Total de Imagens	Autoria	Utilização	Descrição da Base	Apêndice
01	Lenna Database	A	20	Adaptado de (GONZALEZ; WOODS, 2009)	Base utilizada para avaliar o desempenho dos algoritmos de Hash Perceptivo	A Base é composta por 20 imagens, sendo uma original da Lenna Forsén e as demais 19, variações da imagem original.	B
02	Washington Database	A	07	(GONZALEZ; WOODS, 2009)	Base utilizada para avaliar o desempenho dos algoritmos de Hash Perceptivo	A Base é composta por 07 imagens de satélite da cidade de Washington-USA produzidas em diferentes horários do dia.	C
03	Palace Database	A	31	(GUOJIA HOU et al., 2020)	Base utilizada para avaliar o desempenho dos algoritmos de Hash Perceptivo	A Base é composta por 31 imagens de um palácio, sendo uma Original e as demais variações com aplicações de filtros.	D
04	Mountain Database	A	30	(GUOJIA HOU et al., 2020)	Base utilizada para avaliar o desempenho dos algoritmos de Hash Perceptivo	A Base é composta por 30 imagens de uma montanha, sendo uma Original e as demais variações com aplicações de filtros.	E
05	Park Database	A	11	(TRALIC D. et al., 2013)	Base utilizada para avaliar o desempenho dos algoritmos de Hash Perceptivo	A Base é composta por 11 imagens de um parque, sendo uma Original e as demais variações com recortes e sobreposições.	F
06	Natural Images	B	986	(ROY et al., 2018)	Base utilizada na validação do Sistema de Segmentação de Cor de Pele	A Base é composta por 986 imagens de pessoas. Estas imagens são provenientes de outras duas bases combinadas: PubFig83 e LFW Dataset, ambas disponíveis no link: www.briancbecker.com/blog/research/pubfig83-lfw-dataset.	G

ID	Base de Imagens	Estratégia	Total de Imagens	Autoria	Utilização	Descrição da Base	Apêndice
07	FUNSD	C	199	(JAUME; KEMAL EKENEL; THIRAN, 2019)	Base utilizada na validação da extração de metadados e aplicação de OCR	A FUNSD (*Form Understanding in Noisy Scanned Documents*) é uma base composta por 199 imagens de formulários em inglês escaneados. A base está disponível no link: https://guillaumejaume.github.io/FUNSD/	H
08	FBI Symbols Document	D	13	(FEDERAL BUREAU OF INVESTIGATION, 2007)	Criação de uma base de Imagens com símbolos utilizados por criminosos	Boletim dos serviços de Inteligência do FBI sobre os símbolos utilizados por criminosos que realizam crimes contra o público infantojuvenil	I
09	FBI - SDE	D	74	Adaptado de (FEDERAL BUREAU OF INVESTIGATION, 2007)	Base será utilizada para treinar a CNN na Estratégia D	Foi gerada uma base por meio da aplicação do Aumento de Dados com as Redes Adversárias Generativas (RAGs) na base *FBI Symbols Document.* No total foram gerados 71 Imagens ao fornecer 3 imagens como entrada para as RAGs. Somando-as, gerou-se uma nova base formada por 74 imagens.	J
10	FBI - SDV	D	10	Adaptado de (FEDERAL BUREAU OF INVESTIGATION, 2007)	Base será utilizada para validar a CNN na Estratégia D	Foi gerada uma base de imagens extraídas da *FBI Symbols Document.* Das 13 imagens que formam a base *FBI Symbols Document*, 3 foram utilizadas para gerar a FBI-SDE e as outras 10, formam esta base: FBI-SDV.	K

Fonte: o Autor (2024).

3.3. DESENVOLVIMENTO DAS QUATRO ESTRATÉGIAS QUE FORMAM FENRIR

Fenrir é formado por quatro Estratégias aplicadas na detecção de evidências de Pornografia Infantojuvenil em imagens digitais. As Estratégias são formadas pela integração de diferentes técnicas computacionais integradas das áreas da Computação Forense, IA e VC. As quatro Estratégias que formam Fenrir são apresentadas e descritas na tabela 28, juntamente com as bases e as técnicas computacionais utilizadas.

Tabela 28 – Fenrir e suas Quatro Estratégias

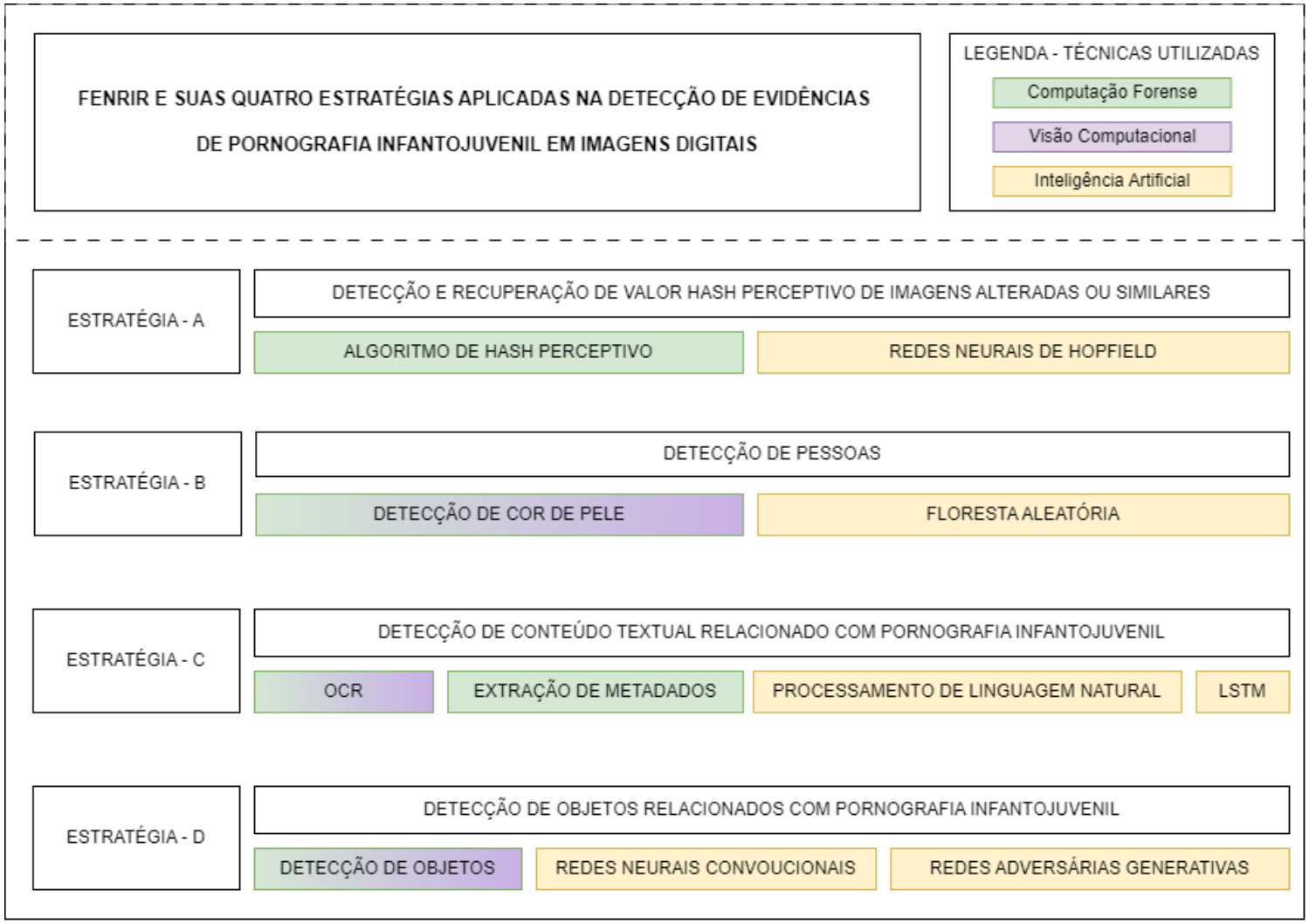
ID	Estratégia	Bases Utilizadas	Tipo de Base	Técnicas Computacionais
A	Detecção e Recuperação de Valor Hash Perceptivo de Imagens Alteradas ou Similares	- *Lenna Database* - *Washington Database* - *Palace Database* - *Mountain Database* - *Park Database*	Imagens	- Hash Perceptivo - RNH
B	Detecção de Pessoas	- *Skin Segmentation* - RGB_HSV_YCBCR - *All Layers* - *Natural Images*	Dados Imagens	- Detecção de Cor de Pele - Floresta Aleatória
C	Detecção de Conteúdo Textual relacionado com Pornografia Infantojuvenil	- FUNSD	Imagens	- OCR - Extração de Metadados - LSTM - PLN
D	Detecção de Objetos relacionados com Pornografia Infantojuvenil	- *FBI Symbols Document* - FBI – SDE - FBI - SDV	Imagens	- Detecção de Objetos - RNC - RAG

Fonte: o Autor (2024).

Resumidamente, na Estratégia A, objetiva-se detectar e recuperar valores Hash perceptivos alterados com o uso das RNH. Na Estratégia B, objetiva-se detectar pessoas por meio da detecção de cor de pele com a floresta aleatória. Na Estratégia C, objetiva-se detectar e estruturar conteúdo textual por meio da extração de metadados, OCR, LSTM e PLN e na Estratégia D, objetiva-se detectar objetos com as RAGs e as RNCs.

Fenrir e suas quatro Estratégias descritas na tabela 28 são ilustradas na figura 32, juntamente com as técnicas utilizadas.

Figura 32 – Fenrir com suas Quatro Estratégias Aplicadas na Detecção de Evidências de Pornografia Infantojuvenil em Imagens Digitais

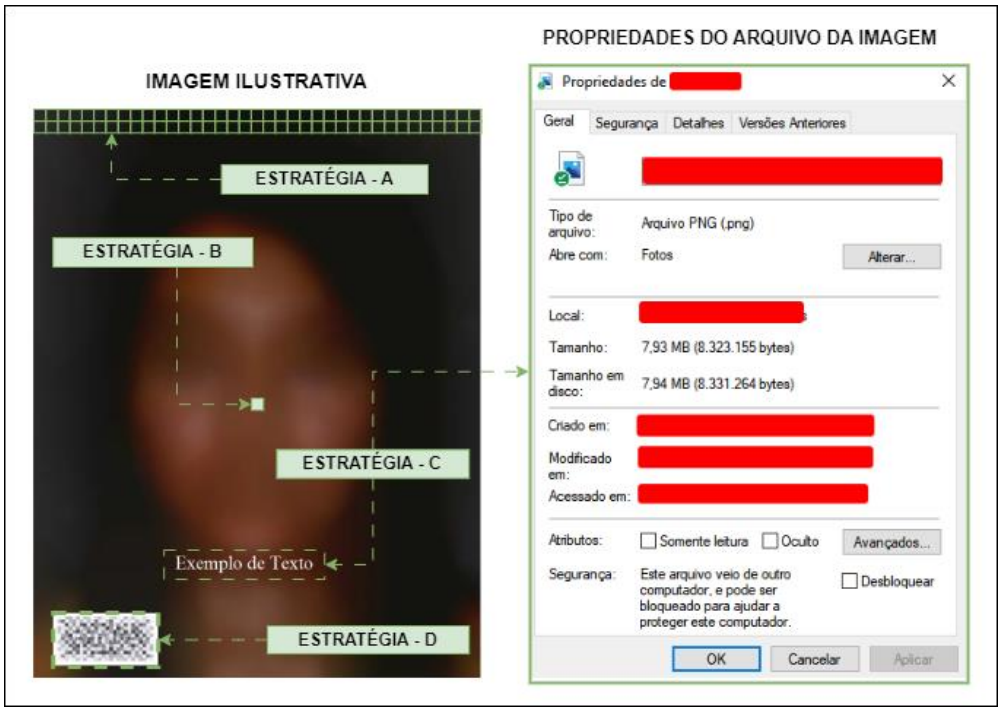


Fonte: o Autor (2024).

Analisando a figura 32, nota-se quais são as técnicas computacionais de cada Estratégia e quais áreas estas técnicas pertencem. No canto superior direito da figura 32, uma legenda é apresentada atribuindo cores que representam as áreas da Computação Forense, VC e IA, sendo elas verde, roxo e laranja respectivamente.

Desta forma, cada técnica é colorida de acordo com a área correspondente, como por exemplo as RNH, cuja coloração laranja informa se tratar de uma técnica da IA. Há também as técnicas que fazem parte de duas ou mais áreas, e assim, são coloridas com duas cores ou mais cores, como é o caso da detecção de cor de pele, que está colorida com as cores verde e roxo, indicando sua relação com as áreas da Computação Forense e VC. Na figura 33 ilustra-se onde estão localizadas as informações presentes em uma imagem digital que a aplicação de Fenrir poderá detectar.

Figura 33 – Arquivo de Imagem e suas propriedades



Fonte: o Autor (2024).

Ao analisar a figura 33, percebe-se que são exibidas duas imagens: Imagem Ilustrativa e as Propriedades do Arquivo da Imagem. Além disso, são dispostas as Estratégias que formam Fenrir. Na imagem ilustrativa, são apresentadas as quatro Estratégias apontando a localização das informações a serem detectadas.

Nas Estratégias A e B, as informações a serem detectadas estão presente nos valores de cada pixel de uma determinada imagem. Na Estratégia C, as informações a serem detectadas

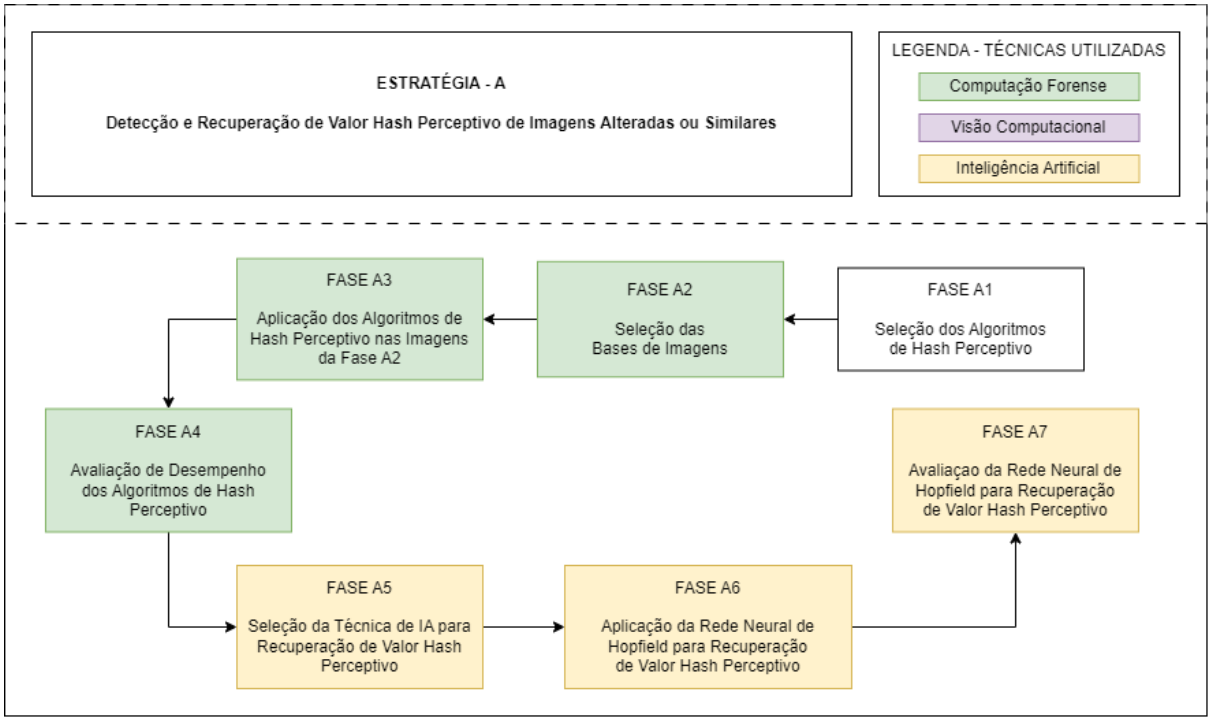
estão no formato de texto, tanto na Imagem Ilustrativa, quanto nas propriedades do Arquivo da Imagem. E na Estratégia D, as informações a serem detectadas estão presentes na imagem por meio de objetos.

As próximas seções descrevem com detalhes as fases que formam o desenvolvimento de cada Estratégia ilustrada na figura 32.

3.3.1. ESTRATÉGIA A

A Estratégia A é intitulada: **Detecção e Recuperação de Valor Hash Perceptivo de Imagens Alteradas ou Similares.** Seu objetivo é detectar imagens alteradas ou similares. A Estratégia A com suas sete fases são ilustradas na figura 34.

Figura 34 – Estratégia A e suas sete fases



Fonte: o Autor (2024).

As setes fases são descritas a seguir:

A1 - Seleção dos Algoritmos de Hash de Perceptivo: Foram definidos os algoritmos de Hash Perceptivo que serão utilizados nesta estratégia. Para isso, foi realizado uma pesquisa na literatura por algoritmos de Hash Perceptivo e softwares utilizados para aplicá-los.

A2 - Seleção das Bases de Imagens: Foi selecionado as bases de imagens que serão utilizadas para avaliar o desempenho dos algoritmos de Hash Perceptivo selecionados na Fase

A1. No total, foram selecionadas cinco bases de imagens, todas compostas por uma imagem original e as outras demais, variações da imagem original.

A3 - Aplicação dos Algoritmos de Hash Perceptivo nas Imagens da fase A2: Os algoritmos de Hash Perceptivo selecionados na Fase A1 foram aplicados nas bases de imagens selecionadas na fase A2. Esta aplicação gerou os valores Hash Perceptivo para cada imagem das bases. Ao término da aplicação, foi definido o limiar de similaridade, requisito para executar a tarefa de comparação de valores Hash Perceptivos (DU; HO; CONG, 2020).

O limiar de similaridade definido foi a Distância de Hamming. Desta forma, calculou-se a Distância de Hamming de todos os valores Hash gerados. Todas as distâncias de Hamming foram exportadas para um *Dataframe* para serem analisadas posteriormente na fase A4. Essa exportação foi realizada separadamente para cada base, gerando assim, cinco *Dataframes*.

A4 - Avaliação de Desempenho dos Algoritmos de Hash Perceptivo: Foi avaliado o desempenho dos Algoritmos de Hash Perceptivo aplicados nas bases de Imagens selecionadas na fase A2. Para isso, foram analisadas as distâncias de Hamming geradas na fase A3.

O objetivo desta avaliação foi verificar qual algoritmo de Hash Perceptivo teve o melhor desempenho e consequentemente, teve a menor distância de Hamming entre os valores Hash Perceptivo da imagem original e suas variações. Quanto mais próximo de zero os valores das Distâncias de Hamming forem, maior será a similaridade entre essas imagens.

A5 - Seleção da Técnica de IA para Recuperação de Valor Hash Perceptivo: Foi selecionado uma técnica de IA específica para recuperação de informação. O objetivo é por meio desta técnica, conseguir na próxima fase, recuperar valores Hash Perceptivos de imagens que sofreram alguma alteração. Para isso, foi pesquisado na literatura por técnicas de IA capazes de serem usadas em tarefas de recuperação de informação. Esta técnica deve ser capaz de, ao receber uma informação com ruído, retornar essa informação para seu estado original.

A técnica selecionada foi a Rede Neural de Hopfield (RNH), um tipo de RNA capaz de armazenar informações em seus neurônios artificiais, para posteriormente, recuperar estas informações ao receber valores similares (CHEN et al., 2023; XU; CHEN, 2022).

A6 - Aplicação da Rede Neural de Hopfield para Recuperação de Valor Hash Perceptivo: Foi aplicado a RNH na recuperação de valores Hash Perceptivo de uma imagem Original, ao receber como entrada o valor Hash Perceptivo de uma variação da imagem original.

Para isso, foi realizada a conversão dos valores Hash Perceptivo para o formato ASCII Binário. Em seguida, foi definido a arquitetura da RNH com 128 neurônios e a função de ativação bipolar com valores entre -1 e 1 (ALEMANNO et al., 2023). Com os valores Hash Perceptivo convertidos para ASCII Binário e a arquitetura da RNH definida, foi feito o treinamento da RNH e sua aplicação na recuperação de valores Hash Perceptivo.

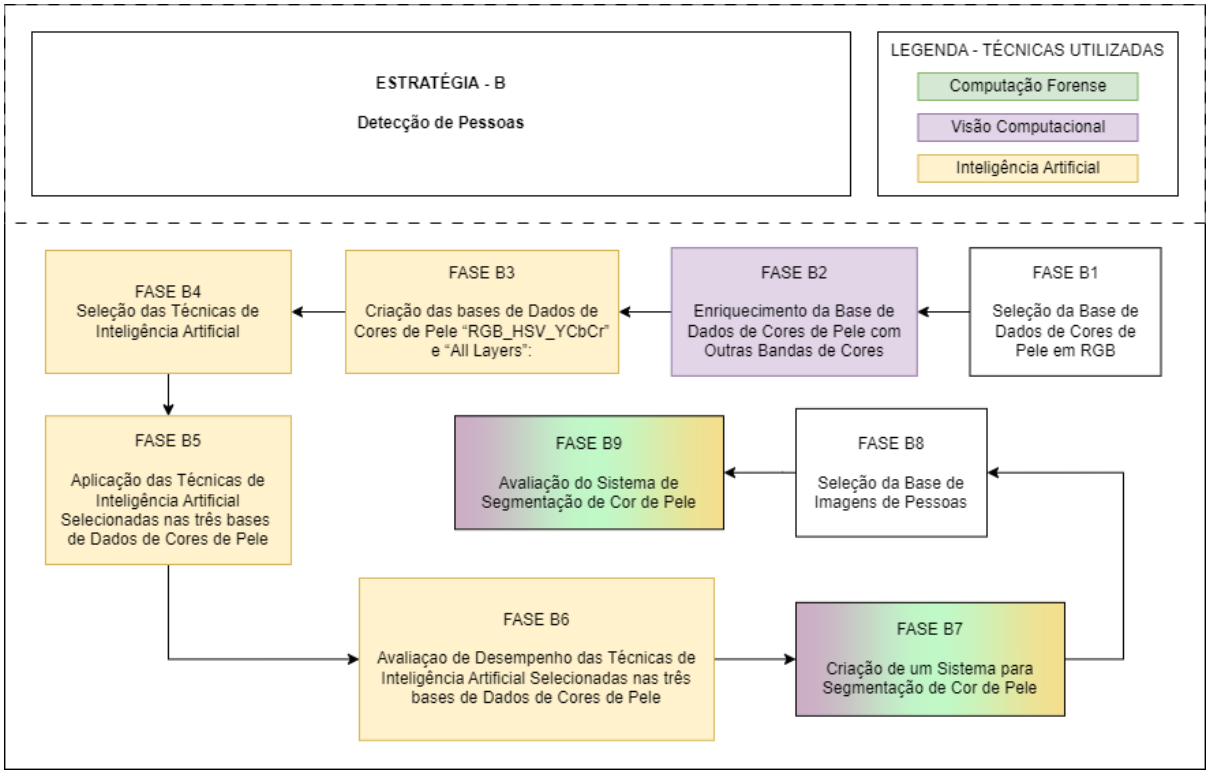
A7 - Avaliação das Rede Neural de Hopfield para recuperação de valor Hash Perceptivo: Foi avaliado o desempenho da RNH aplicada na recuperação de valores Hash Perceptivo na fase A6. Para tal, foi verificado a taxa de acerto.

O objetivo ao final do desenvolvimento e aplicação da **Estratégia A** é calcular e recuperar valores Hash Perceptivo para detectar imagens alteradas ou semelhantes.

3.3.2. ESTRATÉGIA B

A Estratégia B é intitulada: **Detecção de Pessoas.** Seu objetivo é detectar pessoas em imagens por meio da classificação das cores dos pixels em cor-de-pele e não-cor-de-pele. A Estratégia B e suas nove fases são ilustradas na figura 35.

Figura 35 – Estratégia B e suas nove fases



Fonte: o Autor (2024).

As nove fases são descritas a seguir:

B1 - Seleção da Base de Dados de Cores de Pele em RGB: Foi definida a base de cores de pele em RGB para ser utilizada nesta Estratégia. Para isso, foi realizada uma pesquisa na literatura e em repositórios de bases de dados por bases de cores de pele em RGB. Foi definido pelo RGB por ser o espaço de cor mais utilizado por dispositivos eletrônicos para produzir e armazenar imagens digitais (KOREN IVANČEVIĆ et al., 2023).

Sobre os repositórios de bases de dados, foram definidos: *UCI Machine Learning*, *Kaggle*, *Github* e o Portal Brasileiro de Dados Abertos.

B2 - Enriquecimento da Base de Dados de Cores de Pele com Outras Bandas de Cores: Foi realizado o enriquecimento da base de cores de pele definida na fase B1, com outros espaços de cores, inspirado pelos estudos de Ganesan et al. (2023) e Nasreen et al. (2023) que sugerem o desenvolvimento de novas formas para detectar cor de pele.

Para isso, foi realizada uma busca na literatura por ferramentas que realizem a conversão de valores em RGB para outros espaços de cores. Foram identificadas duas ferramentas: *ColorMath* e *ColorSys.* Por meio destas ferramentas, foi possível converter as cores em RGB para outros 11 espaços de cores: **CMY, CMYK, Xyz, yxY, Yiq, CIE-L*ab, CIE-Lch, CIE-Luv, HSL, HSV e YCbCr**. Os resultados desta conversão foram utilizados para enriquecer a base selecionada na fase B1.

B3 - Criação das bases de Cores de Pele "RGB_HSV_YCbCr" e "All Layers": Foi gerado duas bases de cores a partir da base *Skin Segmentation* enriquecida na fase B2. Estas bases serão usadas para medir o desempenho da técnica de IA que será selecionada na fase B4.

A primeira base denominada ***All Layers*** contém todos os 11 espaços de cores gerados no enriquecimento realizado na fase B2, além do atributo classificador *SkinColor*. A segunda base trata-se de uma cópia da ***All Layers***, posteriormente reduzida com o PCA (*Principal Component Analysis*). A aplicação do PCA teve por objetivo identificar quais os atributos mais importantes na base ***All Layers***.

B4 - Seleção das Técnicas de Inteligência Artificial: Foi realizado uma pesquisa na literatura por publicações relacionadas com a detecção de cor de pele que mencionem técnicas que possam ser utilizadas em tarefas de classificação. No total, foram selecionadas 7 técnicas

de IA: Árvore de Decisão, Floresta Aleatória, KNN, MLP, Naive Bayes, Regressão Logística e SVM (GANGWAR et al., 2017; MOREIRA; FECHINE, 2018; NASREEN et al., 2023).

B5 - Aplicação das Técnicas de Inteligência Artificial Selecionadas nas três bases de Dados de Cores de Pele: Foi aplicado as técnicas de IA selecionadas na fase B4 nas três bases de dados com informações sobre cores de pele. O objetivo desta aplicação foi descobrir qual técnica de IA possui o melhor desempenho na detecção de cor de pele nas três bases de cores de pele: **RGB**, **RGB_HSV_YCbCR** e ***All Layers***.

B6 - Avaliação de Desempenho das Técnicas de Inteligência Artificial Selecionadas nas três bases de Dados de Cores de Pele: Foi avaliado o desempenho das técnicas de IA aplicadas na fase B5. Para isso, foram utilizadas as seguintes métricas: Matriz de Confusão, Acurácia, Precisão, *Recall* e *F-Score* (NASREEN et al., 2023; SAMUELSSON, 2018).

B7 - Criação de um sistema para Segmentação de Cor de Pele: Foi criado um sistema de Segmentação de Cor de pele com a Floresta Aleatória, técnica de IA que obteve o melhor desempenho na avaliação realizada na fase B6. Este sistema de Segmentação de cor de pele será utilizado para avaliar qualitativamente a detecção de cor de pele.

B8 - Seleção de Base de Imagens de Pessoas: Foi selecionada uma base com imagens de pessoas para avaliar o desempenho do sistema de segmentação de cor de pele criado na fase B7. Para isso, foi realizada uma busca na literatura por bases formadas por imagens de pessoas com diferentes etnias, gêneros e idades.

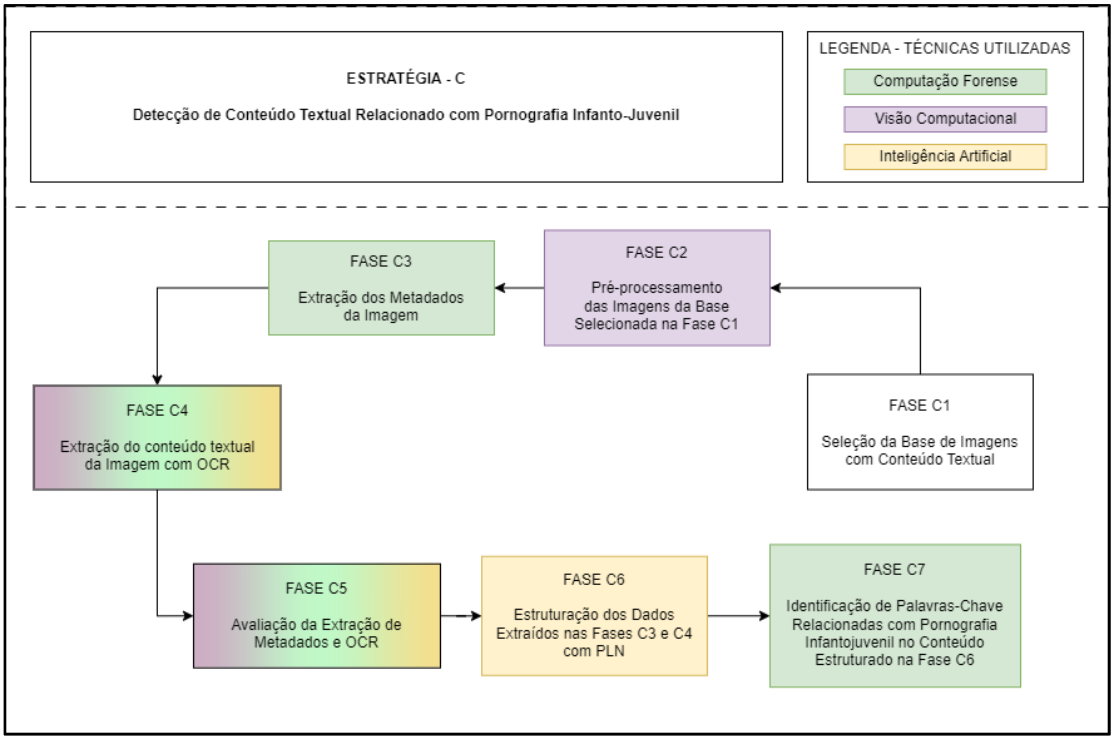
B9 - Avaliação do Sistema de Segmentação de Cor de Pele: Foi avaliado o desempenho do sistema de segmentação de cor de pele desenvolvido na fase B7 e aplicado em uma amostra de imagens de pessoas extraídas aleatoriamente da base selecionada na fase B8. O objetivo foi descobrir com qual, o sistema de Segmentação de Cor de Pele possui o melhor desempenho. Este desempenho será avaliado pela taxa de pixels detectados como cor de pele e o tempo de processamento.

O objetivo ao final do desenvolvimento e aplicação da **Estratégia B** é detectar pessoas em imagens por meio da identificação de cores de pele.

3.3.3. ESTRATÉGIA C

A Estratégia C é intitulada: **Detecção de Conteúdo Textual relacionado com Pornografia Infantojuvenil.** Seu objetivo é detectar conteúdo textual relacionado com Pornografia Infantojuvenil. A Estratégia C com sete fases são ilustradas na figura 36.

Figura 36 – Estratégia C e suas sete fases



Fonte: o Autor (2024).

As sete fases são descritas a seguir:

C1 - Seleção da Base de Imagens com Conteúdo Textual: Foi selecionada a base de imagens com conteúdo textual para ser utilizada no desenvolvimento desta estratégia. Para isso foi realizada uma pesquisa sobre bases de imagens utilizadas para extração de metadados e OCR nos seguintes repositórios de bases de dados e imagens: *Kaggle, UCI Machine Learning*, *Github* e o Portal Brasileiro de Dados Abertos.

C2 - Pré-processamento da base das Imagens selecionada na fase C1: Foi realizada o pré-processamento das imagens da base selecionada na fase C1. O objetivo foi obter um ganho de desempenho na detecção de conteúdo textual. Inicialmente, foi extraído uma amostra de forma aleatória da base selecionada na fase C1. Em seguida, foi executado o pré-processamento com as seguintes tarefas: Redimensionamento, Normalização, Redução de Ruídos, Conversão para Níveis de Cinza, Dilatação e Erosão, e a Limiarização.

C3 - Extração dos Metadados da Imagem: Foi extraído os metadados das imagens da amostra definida e pré-processada na fase C2. Para isto, desenvolveu-se um código em python que extrai os metadados de uma imagem digital e os armazena em uma *BagOfWords* (BoW).

C4 - Extração do Conteúdo Textual da Imagem com OCR: Foi extraído o conteúdo textual das imagens pré-processadas na fase C2. Para isto, foi desenvolvido um código em python que aplica o OCR para extrair o conteúdo textual da imagem e o armazena na mesma BoW gerada na fase C3. A aplicação do OCR foi realizada com as ferramentas: **Tesseract** e **EasyOCR** (SCHÖNFELDER et al., 2024).

C5 - Avaliação da Extração de Metadados e OCR: Foi avaliado o desempenho obtido nas extrações de Metadados e OCR realizadas nas fases C3 e C4. Esta avaliação foi realizada ao comparar o conteúdo destas extrações armazenadas na BoW com o arquivo de anotações da base de imagens selecionada na fase C1. Para avaliar ambas as extrações, foram utilizadas as seguintes métricas: Total de Palavras, Taxa de Erro de Caracteres (CER), Taxa de Erro de Palavras (WER) e a Taxa de Acerto (MULYANTO; HARTATI; WARDOYO, 2022).

C6 - Estruturação dos Dados Extraídos nas fases C3 e C4 com PLN: O conteúdo das extrações realizadas nas fases C3 e C4 e armazenadas em uma BoW foram estruturados com a utilização das seguintes tarefas de Processamento de Linguagem Natural (PLN): Conversão para minúsculas, tokenização, remoção de valores duplicados, ordenação alfabética, remoção de caracteres isolados e a remoção de stopwords.

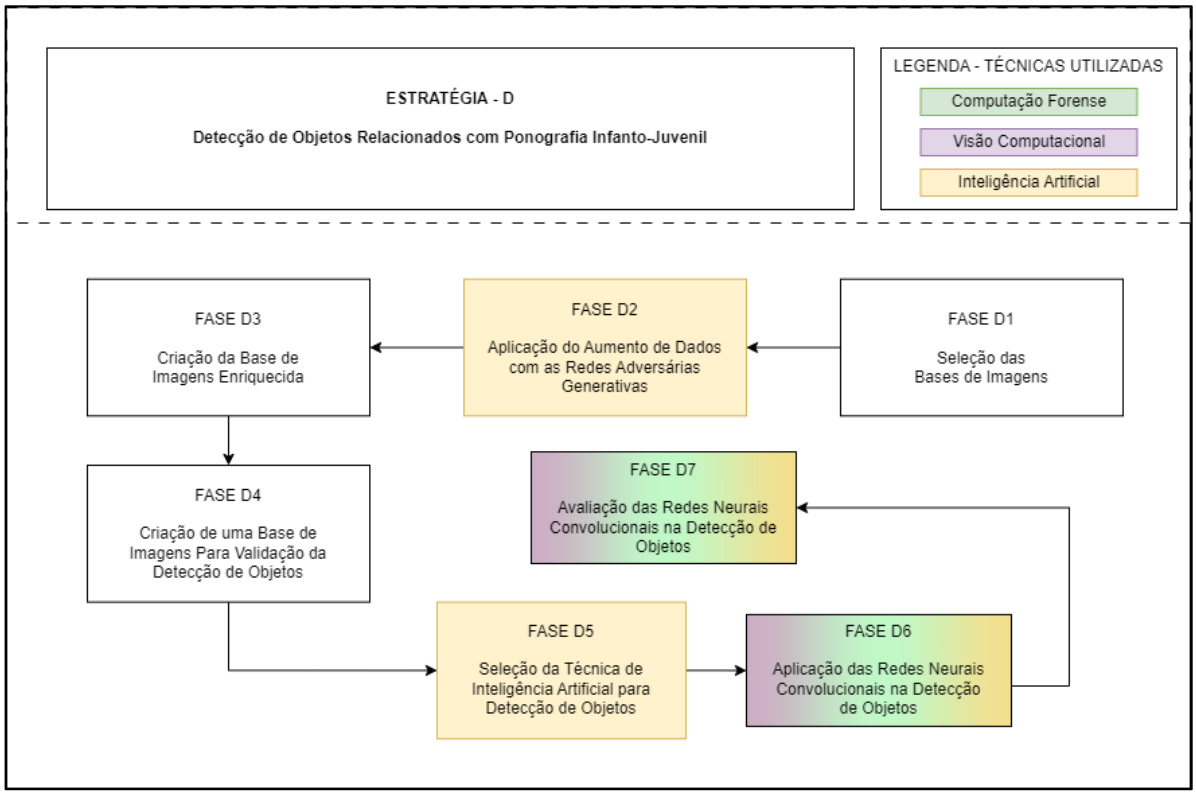
C7 - Identificação de Palavras-Chave relacionadas com Pornografia Infantojuvenil no conteúdo estruturado na fase C6: Foi desenvolvido um código em python para buscar no conteúdo estruturado na fase C6 com um conjunto de palavras-chave relacionadas à Pornografia Infantojuvenil. O conjunto de palavras-chave foi identificado na literatura nos estudos feitos por Frank, Westlake e Bouchard (2010) e Wang et al. (2023). Todas estas palavras-chave são descritas na Tabela 23 da RSL disponível na seção 2.6 deste trabalho. No total, o conjunto compreende 359 palavras-chave relacionadas à Pornografia Infantojuvenil.

O objetivo ao final do desenvolvimento e aplicação da **Estratégia C** é conseguir detectar conteúdo textual em imagens relacionados com Pornografia Infantojuvenil através da extração de metadados e do OCR.

3.3.4. ESTRATÉGIA D

A Estratégia D é intitulada: **Detecção de Objetos Relacionados com Pornografia Infantojuvenil.** Seu objetivo é detectar objetos relacionados com Pornografia Infantojuvenil em imagens. Estes objetos são símbolos utilizados por criminosos para identificar arquivos de pornografia infantojuvenil. A Estratégia D e suas sete fases são ilustradas na figura 37.

Figura 37 – Estratégia D e suas sete fases



Fonte: o Autor (2024).

As sete fases são descritas a seguir:

D1 - Seleção das Bases de Imagens: Foi selecionado uma base de imagens de contendo símbolos relacionados com Pornografia Infantojuvenil. Para isso, foi realizada uma pesquisa na literatura em bases de dados e imagens, além de publicações de autoridades policiais sobre símbolos utilizados em arquivos com Pornografia Infantojuvenil.

D2 - Aplicação do Aumento de Dados com as Redes Adversárias Generativas: Foi aplicado o Aumento de Dados com as Redes Adversárias Generativas (RAGs) nos símbolos selecionados para treinamento na fase D1. O objetivo do Amento de Dados foi produzir novos símbolos, e assim, gerar uma base para treinar a técnica de IA que será utilizada posteriormente.

D3 - Criação da Base de Imagens Enriquecida: Foi criado uma base de imagens enriquecida. A base criada denominada **FBI – SDE** é formada pelos 3 símbolos selecionados para treinamento na fase D1, juntamente com os 71 símbolos gerados pelo Aumento de Dados na fase D2, totalizando 74 símbolos.

D4 - Criação de uma Base de Imagens com Símbolos Para Validação da Detecção de Objetos: Foi criado uma base de imagens para a validação da Detecção de Objetos. A detecção de objetos será conduzida pela técnica de IA, cuja seleção será feita na fase D5. Esta base de imagens criada para validação foi denominada **FBI – SDV,** e é formada pelos 10 símbolos definidos na fase D1.

D5 - Seleção da Técnica de Inteligência Artificial para Detecção de Objetos: Foi selecionado a técnica de IA que será utilizada para detectar objetos. Para isso, buscou-se na literatura por estudos que mencionem a utilização de técnicas de IA para detectar objetos. A técnica de IA selecionada foi a Rede Neural Convolucional (RNCs). Trata-se de um tipo de RNA de aprendizado profundo comumente utilizada em tarefas com imagens digitais, como no pré-processamento e detecção de objetos (SANGHVI et al., 2021).

D6 - Aplicação das Redes Neurais Convolucionais na Detecção de Objetos: Foi aplicado a técnica da RNC na detecção de objetos. Para isso, foi utilizado as imagens da base **FBI – SDE** como treinamento da RNC, e as imagens da base **FBI – SDV** foram utilizadas para validar o desempenho da RNC. O treinamento da RNC incluiu as tarefas de Transferência de Aprendizagem, Desenho de Caixas Delimitadoras e a Parada Antecipada. Ao término do treinamento, foi aplicado a RNC na base **FBI – SDV** para detectar objetos.

D7 - Avaliação das Redes Neurais Convolucionais na Detecção de Objetos: Foi avaliado o desempenho da RNCs aplicadas na detecção de objetos na fase D6 com as métricas: Interseção sobre União (IoU) e a Confiança das Classes existentes nas imagens de treinamento.

O objetivo final do desenvolvimento e aplicação da **Estratégia D** é conseguir detectar objetos relacionados com Pornografia Infantojuvenil em imagens digitais.

No próximo capítulo, são apresentados e discutidos os resultados obtidos com o desenvolvimento e aplicação das Estratégias que formam Fenrir.

4. APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

Neste capítulo, são apresentados e discutidos os resultados obtidos do desenvolvimento das Estratégias que formam Fenrir, aplicadas na detecção de evidências de Pornografia Infantojuvenil em imagens digitais, apresentadas na seção 3.3.

4.1. ESTRATÉGIA A

Denominada **Detecção e Recuperação de Valor Hash Perceptivo de Imagens Alteradas ou Similares**, esta Estratégia tem como objetivo detectar imagens alteradas ou similares. Na tabela 29, resumidamente são apresentadas as Bases e Técnicas Computacionais utilizadas no desenvolvimento e aplicação desta estratégia.

Tabela 29 – Bases e Técnicas Computacionais utilizadas na Estratégia A

ID	Estratégia	Bases	Tipo de Base	Técnicas Computacionais
A	Detecção e Recuperação de Valor Hash Perceptivo de Imagens Alteradas ou Similares	- *Lenna Database* - *Washington Database* - *Palace Database* - *Mountain Database* - *Park Database*	Imagens	- Hash Perceptivo - RNH

Fonte: o Autor (2024).

A Estratégia A é composta por sete fases, são elas:

A1 - Seleção dos Algoritmos de Hash de Perceptivo: Foram definidos os algoritmos de Hash Perceptivo que serão usados nesta estratégia. Para isso, foi realizado uma busca na literatura sobre tipos de algoritmos de Hash Perceptivo e softwares para aplicá-los.

Foi identificado um total de cinco algoritmos de Hash Perceptivo. São eles: *Average Hash*, *Perceptual Hash*, *Differential Hash*, *Wavelet Hashing* e *Crop-resistance Hash*. O funcionamento dos cinco algoritmos está descrito na Tabela 1 deste trabalho. Quanto ao software selecionado para executar os algoritmos de Hash Perceptivo foi o ImageHash.

A2 - Seleção das Bases de Imagens: Foram selecionadas as bases de imagens utilizadas para avaliar o desempenho dos Algoritmos de Hash Perceptivo selecionados na Fase A1. No total, foram selecionadas cinco bases de imagens, todas formadas por uma imagem original e as demais, variações desta imagem original. As bases selecionadas foram: *Lenna Database*,

Washington Database, Palace Database, Mountain Database e *Park Database*. Na Tabela 27 são descritas as informações sobre a quantidade de imagens, autoria e descrição destas bases.

A3 - Aplicação dos Algoritmos de Hash Perceptivo nas Imagens da fase A2: Os Algoritmos de Hash Perceptivo selecionados na Fase A1 foram aplicados nas bases de imagens selecionadas na fase A2. Em cada aplicação, foi utilizado duas imagens como entrada: Uma original e uma variação desta imagem original, ambas importadas no código com a utilização da biblioteca OpenCV.

Então, para cada base de imagem selecionada na fase A2, foi aplicado o código *n* vezes, sendo *n* a quantidade de variações existentes naquela base de imagens. Por exemplo, a base de imagens *Lenna Database* é composta por 20 imagens, sendo uma Original e as outras 19, variações desta imagem original. Estas variações incluem rotação, inversão, alteração nos níveis de contraste e brilho, adição de ruído, filtros, além da inserção, remoção e substituição de espaços de cores. Para a base *Lenna Database*, foram necessárias 19 execuções, ou seja, o mesmo número de variações existentes na base. O total de execuções de cada base de imagens é descrita na tabela 30.

Tabela 30 – Total de Execuções dos Algoritmos de Hash Perceptivos nas Bases de Imagens

ID	Base de Imagens	Total de Imagens	Total de Variações da Imagem Original	Total de Execuções
01	Lenna Database	20	19	**19**
02	Washington Database	07	06	**06**
03	Palace Database	31	30	**30**
04	Mountain Database	30	29	**29**
05	Park Database	11	10	**10**

Fonte: o Autor (2024)

Cada execução foi realizada da seguinte forma: Importou duas imagens, a original e uma variação desta imagem original, e em seguida, foi aplicado os cinco algoritmos de Hash Perceptivos selecionados na fase A1 em ambas as imagens.

Ressalta-se que ao aplicar o algoritmo de Hash Perceptivo *Crop-Resistance*, foi gerado como saída, uma lista composta por *n* valores Hash, sendo *n* o total de reduções feitas em sua execução. O funcionamento do algoritmo de Hash Perceptivo *Crop-Resistance* é descrito na

Tabela 1. Uma amostra dos valores Hash gerados pela aplicação dos algoritmos de Hash Perceptivo em duas imagens da base *Lenna Database* é ilustrada na Tabela 31.

Tabela 31 – Amostra dos Valores Hash após aplicar os algoritmos de Hash Perceptivo em duas imagens da base *Lenna Database*

Algoritmo de Hash Perceptivo	**Imagem Original**	**Variação da Imagem Original**
Average Hash	b69cbd890b0b8f8c	b61cbd890b0b8f8c
Perceptual Hash	99c6562d7533a296	99c6562d7533a296
Differential Hash	7670795b33135a38	7670795b33135a38
Wavelet Hashing	be98bd890b0b8f8c	be98bd890b0b8f8c
Crop-Resistance Hash	1838bc3c3c3cd8cc cce5f172e767767a 67c6808082e23019 eede5bc79e67676f 016558c4f1f9f4fe d8b1270c193376ac 07370f07071fe3f1 6c999932f2362644	1c38bc3c3c3cd8cc cce5f172e767767a 67c6808082e23099 eede5b471e67676f 416558c4f1f9f4fe d8b1270c193376ac 07770707071fe3f1 6c999932f2362644

Fonte: o Autor (2024).

Concluída a aplicação dos algoritmos de Hash Perceptivo nas cinco bases de imagens, foi definido o limiar de similaridade para realizar a comparação de valores Hash Perceptivo. Foi definido a Distância de Hamming como limiar de similaridade por ser uma métrica comumente utilizada na comparação de valores Hash (DU; HO; CONG, 2020).

Calculou-se a Distância de Hamming entre os valores Hash Perceptivo das imagens originais e de suas variações para cada uma das cinco bases de imagens selecionadas na fase A2. Uma amostra com as Distâncias de Hamming calculadas em duas imagens da base *Lenna Database* é apresentada na Tabela 32.

Tabela 32 – Amostra da Distância de Hamming calculada entre duas imagens da base *Lenna Database*

Algoritmo de Hash Perceptivo	**Imagem Original**	**Variação da Imagem Original**	**Distância de Hamming**
Average Hash	b69cbd890b0b8f8c	b61cbd890b0b8f8c	1
Perceptual Hash	99c6562d7533a296	99c6562d7533a296	0
Differential Hash	7670795b33135a38	7670795b33135a38	0
Wavelet Hashing	be98bd890b0b8f8c	be98bd890b0b8f8c	0
Crop-Resistance Hash	1838bc3c3c3cd8cc	1c38bc3c3c3cd8cc	7,04

Algoritmo de Hash Perceptivo	Imagem Original	Variação da Imagem Original	Distância de Hamming
	cce5f172e767767a	cce5f172e767767a	
	67c6808082e23019	67c6808082e23099	
	eede5bc79e67676f	eede5b471e67676f	
	016558c4f1f9f4fe	416558c4f1f9f4fe	
	d8b1270c193376ac	d8b1270c193376ac	
	07370f07071fe3f1	07770707071fe3f1	
	6c999932f2362644	6c999932f2362644	

Fonte: o Autor (2024).

Com a Distância de Hamming calculada, foi possível determinar qual algoritmo de Hash Perceptivo se aproximou mais do valor Hash Perceptivo da imagem Original, no caso, valor 0.

Sobre o algoritmo *Crop-Resistance*, como sua aplicação gera *n* valores Hash Perceptivo, a distância de Hamming foi calculada em todos os *n* valores Hash Perceptivo gerados, e posteriormente, calculada a média. Assim, se a aplicação do Algoritmo *Crop-Resistance* gerar oito valores Hash Perceptivo, será calculado as oito distâncias de Hamming e posteriormente, a média destas distâncias, conforme demonstra a equação (41):

$$\boldsymbol{Dist_{CropResistance}} = \frac{\sum \left| x_i - y_i \right|}{\boldsymbol{n}} \tag{41}$$

Na qual ***n***, representa o total de valores Hash gerados pela aplicação do *Crop-Resistance*. Finalmente, com todas as distâncias de Hamming calculadas, incorporou-se todos os valores em diferentes *Dataframes*, um para cada base de imagem. A geração destes *Dataframes* foi realizada com a biblioteca Pandas. Em seguida, exportou-se estes *Dataframes* em formato .csv. Definiu-se este formato para possibilitar que os *Dataframes* sejam importados em uma planilha Excel para uma análise nas fases posteriormente.

A4 - Avaliação de Desempenho dos Algoritmos de Hash Perceptivo: Foi avaliado o desempenho dos Algoritmos de Hash Perceptivo aplicados nas bases de Imagens selecionadas na fase A2. Para isso, foram analisadas as distâncias de Hamming calculadas na fase A3.

Inicialmente, importou-se os *Dataframes* gerados na fase A3 para uma planilha eletrônica com o software Excel. Em seguida, foi adicionado na planilha um vetor chamado de "*Original_Array*", com *n* itens, sendo *n* a quantidade de imagens na base a ser avaliada. Este vetor representa a Distância de Hamming da imagem Original, com todos os valores dos *n*

elementos iguais a zero. Este vetor permitirá verificar o quão similar são os valores Hash Perceptivos gerados na fase A3.

Então, a avaliação de desempenho dos algoritmos de Hash Perceptivos foi realizada através de cálculos de distâncias entre os resultados das distâncias de Hamming de cada Algoritmo de Hash Perceptivo e o vetor *Original_Array*". As distâncias definidas foram a Euclidiana e Manhattan por serem métricas comumente usadas para calcular a distância entre dois vetores (Du; Ho; Cong, 2020). Nos apêndices L, M, N, O e P são descritos os *Dataframes* de cada base de imagem selecionada na fase A2, juntamente com o vetor "*Original_Array*".

Na Tabela 33, são apresentadas as distâncias Euclidiana e de Manhattan de cada um dos algoritmos de Hash Perceptivos. Ambas as distâncias possibilitam esclarecer qual algoritmo de Hash Perceptivo gerou valores Hash Perceptivos mais próximos do Valor Hash Perceptivo da imagem original. Desta forma, quanto menor forem os valores das Distâncias Euclidiana e de Manhattan, maior será a similaridade dos valores Hash Perceptivo.

Tabela 33 – Distâncias Euclidiana e de Manhattan de Cada Algoritmo de Hash Perceptivo

Base de Imagem	**Algoritmo de Hash Perceptivo**	**Distância Euclidiana**	**Distância de Manhattan**
Lenna Database	A-Hash	24,49	56
	P-Hash	23,66	52
	D-Hash	**17,86**	**37**
	W-Hash	22,20	47
	CP-Hash	36,68	110
Washington Database	**A-Hash**	**20,44**	**42**
	P-Hash	24,55	51
	D-Hash	23	50
	W-Hash	21	44
	CP-Hash	37	93
Palace Database	A-Hash	26,85	71
	P-Hash	27,31	74
	D-Hash	**25,09**	**69**
	W-Hash	28,40	75
	CP-Hash	82,68	452,8
Mountain Database	**A-Hash**	**7,14**	**17**
	P-Hash	21,16	92
	D-Hash	12,24	51
	W-Hash	19,59	92
	CP-Hash	81,40	438
Park Database	A-Hash	13,41	30

Base de Imagem	Algoritmo de Hash Perceptivo	Distância Euclidiana	Distância de Manhattan
	P-Hash	14,35	32
	D-Hash	**7,34**	**18**
	W-Hash	8,94	20
	CP-Hash	75,97	202,25

Fonte: o Autor (2024).

Ao analisar a Tabela 33, percebe-se que o Algoritmo de Hash Perceptivo que teve o melhor desempenho foi o *Differential Hash* (*D-Hash)*, sendo o mais eficiente em três bases de imagens: *Lenna Database*, *Palace Database* e *Park Database*. O segundo algoritmo de Hash Perceptivo que teve o melhor desempenho foi o *Average-Hash (A-Hash)*, sendo o mais eficiente em duas bases de imagens: *Washington Database* e *Mountain Database*.

Já os algoritmos de Hash Perceptivo *Perceptual Hash* (*P-Hash)* e o *Wavelet Hash (W-Hash)* não tiveram a menor distância em nenhuma das cinco bases de imagens avaliadas. Por fim, o *Crop-Resistance Hash (CPR-Hash)* foi o Algoritmo de Hash Perceptivo que teve o pior desempenho dos cinco avaliados. Então, foi definido o *Differential Hash (D-Hash)* para ser o algoritmo de Hash Perceptivo utilizado nesta Estratégia, pois obteve o melhor desempenho em três das cinco bases de imagens, incluindo a base *Lenna Database*, a única que contém imagens de pessoas em sua composição.

A5 - Seleção da Técnica de IA para Recuperação de Valor Hash Perceptivo: Foi selecionado uma técnica de IA específica para recuperação de informação. O objetivo é por meio desta técnica, conseguir na próxima fase, recuperar valores Hash Perceptivos de imagens que sofreram alguma alteração. Para isso, foi pesquisado na literatura por técnicas de IA capazes de serem usadas em tarefas de recuperação de informação. Esta técnica deve ser capaz de, ao receber uma informação com ruído, retornar essa informação para seu estado original.

A técnica selecionada foi a Rede Neural de Hopfield (RNH), um tipo de RNA capaz de armazenar informações em seus neurônios artificiais, para posteriormente, recuperar estas informações ao receber valores similares (CHEN et al., 2023; XU; CHEN, 2022).

A6 - Aplicação da Rede Neural de Hopfield para Recuperação de Valor Hash Perceptivo: Foi aplicado a RNH na recuperação de valores Hash Perceptivo de uma imagem Original, ao receber como entrada o valor Hash Perceptivo de uma variação da imagem original.

Para a aplicação da RNH, os valores Hash Perceptivo das imagens originais das cinco bases foram utilizados para treinamento, enquanto os valores Hash Perceptivo das variações das imagens originais foram utilizados como teste.

Assim, 5 valores Hash Perceptivo foram usados para treinamento e 94 valores Hash Perceptivo foram usados para teste. Pelo fato de a RNH ser um tipo de RNA que utiliza somente com valores 0 e 1, foi necessário converter os valores Hash Perceptivos para um valor formado apenas por 0 e 1. Foi definido o formato ASCII Binário, inspirado pelo estudo de Sun et al. (2023) que converte caracteres alfanuméricos em números. No formato ASCII binário, cada caractere é representado por um conjunto de oito números, todos podendo assumir dois valores: 0 ou 1. É apresentado na Tabela 34, dois exemplos de conversão de texto para ASCII Binário.

Tabela 34 – Exemplos de Conversão de Texto para ASCII Binário

Texto	**Texto Convertido para ASCII Binário**
RAFAEL	10011101 10001100 10010001 10001100 10010000 10010111
UNINOVE10	10100000 10011001 10010100 10011001 10011010 10100001 10010000 01111100 01111011

Fonte: o Autor (2024)

Então, foi aplicado a conversão para ASCII binário em todos os valores Hash Perceptivo. Como o valor Hash Perceptivo gerado pelo algoritmo *Differential Hash* é formado por 16 caracteres, a sua conversão para ASCII binário gerou uma saída formada por 128 caracteres numéricos. Concluída a conversão, foi definido a arquitetura da RHN.

A RNH foi construída com 128 neurônios artificiais, um neurônio para cada caractere do valor Hash Perceptivo convertido para ASCII Binário. Já a função de ativação, foi definido a ativação bipolar com os valores entre -1 e 1 por ser comumente usada em tarefas de recuperação de informação ruidosas (ALEMANNO et al., 2023).

Definido a arquitetura da RNH, foi realizado o seu treinamento. A tabela 35 apresenta os valores Hash Perceptivos convertidos para ASCII Binário utilizados para treinar a RNH.

Tabela 35 – Valores Hash Perceptivos Convertidos para ASCII Binário utilizados para treinar a RNH

Base de Imagem	Valor Hash Perceptivo da Imagem Original	Valor Hash Perceptivo Convertido para ASCII Binário
Lenna Database	7670795b33135a38	0 0 1 1 0 1 1 1 0 0 1 1 0 1 1 0 0 0 1 1 0 1 1 1 0 0 1 1 0 0 0 0 0 0 1 1 0 1 1 1 0 0 1 1 1 0 0 1 0 0 1 1 0 1 0 1 0 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 0 1 0 0 1 1 0 0 1 1 0 0 1 1 0 1 0 1 0 1 1 0 0 0 0 1 0 0 1 1 0 0 1 1 0 0 1 1 1 0 0 0
Washington Database	d3d85833daeab5a9	0 1 1 0 0 1 0 0 0 0 1 1 0 0 1 1 0 1 1 0 0 1 0 0 0 0 1 1 1 0 0 0 0 0 1 1 0 1 0 1 0 0 1 1 1 0 0 0 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 1 1 0 0 1 0 0 0 1 1 0 0 0 0 1 0 1 1 0 0 1 0 1 0 1 1 0 0 0 0 1 0 1 1 0 0 0 1 0 0 0 1 1 0 1 0 1 0 1 1 0 0 0 0 1 0 0 1 1 1 0 0 1
Palace Database	e6ce8e991c149694	0 1 1 0 0 1 0 1 0 0 1 1 0 1 1 0 0 1 1 0 0 0 1 1 0 1 1 0 0 1 0 1 0 0 1 1 1 0 0 0 0 1 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 0 1 1 1 0 0 1 0 0 1 1 0 0 0 1 0 1 1 0 0 0 1 1 0 0 1 1 0 0 0 1 0 0 1 1 0 1 0 0 0 0 1 1 1 0 0 1 0 0 1 1 0 1 1 0 0 0 1 1 1 0 0 1 0 0 1 1 0 1 0 0
Mountain Database	402416531b191a1f	0 0 1 1 0 1 0 0 0 0 1 1 0 0 0 0 0 0 1 1 0 0 1 0 0 0 1 1 0 1 0 0 0 0 1 1 0 0 0 1 0 0 1 1 0 1 1 0 0 0 1 1 0 1 0 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 0 1 0 1 1 0 0 0 1 0 0 0 1 1 0 0 0 1 0 0 1 1 1 0 0 1 0 0 1 1 0 0 0 1 0 1 1 0 0 0 0 1 0 0 1 1 0 0 0 1 0 1 1 0 0 1 1 0
Park Database	4659d98bcbcb9639	0 0 1 1 0 1 0 0 0 0 1 1 0 1 1 0 0 0 1 1 0 1 0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1 0 0 0 0 1 1 1 0 0 1 0 0 1 1 1 0 0 0 0 1 1 0 0 0 1 0 0 1 1 0 0 0 1 1 0 1 1 0 0 0 1 0 0 1 1 0 0 0 1 1 0 1 1 0 0 0 1 0 0 0 1 1 1 0 0 1 0 0 1 1 0 1 1 0 0 0 1 1 0 0 1 1 0 0 1 1 1 0 0 1

Fonte: o Autor (2024)

Ao analisar a Tabela 35, percebe-se que a conversão para ASCII Binário possibilitou que o valor Hash da Imagem Original fosse transformado em um valor composto somente por 0 e 1 para ser utilizado no treinamento da RNH. Concluído o treinamento, foi aplicado a RNH em todos os valores Hash Perceptivo das variações das imagens originais.

Então, 5 valores Hash Perceptivo foram utilizados para treinamento e 94 valores Hash Perceptivo foram utilizados para teste.

A7 - Avaliação das Rede Neural de Hopfield para recuperação de valor Hash Perceptivo: Foi avaliado o desempenho da RNH aplicada na recuperação de valores Hash Perceptivo na fase A6. Para tal, foi verificado a taxa de acerto.

Os resultados gerados pela aplicação da RNH são descritos na Tabela 36.

Tabela 36 – Resultados gerados na Aplicação da RNH

Base de Imagem	Total de Imagens	Total de Acertos	Total de Erros	Taxa de Acerto (%)
Lenna Database	19	18	1	94,74%
Washington Database	6	4	2	66,67%
Palace Database	30	23	7	76,67%
Mountain Database	29	29	0	100%
Park Database	10	10	0	100%
Total	**94**	**84**	**10**	**89,36%**

Fonte: o Autor (2024)

Analisando a tabela 36, percebe-se que em todas as bases de imagens, a RNH obteve mais acertos do que erros na tarefa de recuperação de Valores Hash Perceptivos. De 94 valores Hash Perceptivo, foi possível recuperar 84 valores de Hash Perceptivo da imagem original, o que representa um total de 89,36% de acerto.

Nas bases *Park Database* e *Mountain Database*, a RNH conseguiu recuperar o valor Hash Perceptivo de todas as variações. Na base *Lenna Database*, não foi possível recuperar o valor Hash Perceptivo de uma variação, enquanto na base *Washington Database*, não foi possível recuperar o valor Hash Perceptivo de duas variações.

A base em que a RNH teve o pior desempenho foi a *Palace Database*. Nesta base, a RNH não conseguiu recuperar sete variações. As alterações nas imagens destas sete variações foram as mais significativas, e consequentemente, geraram a maior distância de Hamming. Todas estas variações em que a RNH não conseguiu recuperar o valor Hash Perceptivo obteve um valor de Distância de Hamming a partir de 8 caracteres. Isso significa que em um valor Hash Perceptivo de 16 caracteres, caso a metade destes caracteres seja diferente, não será possível recuperá-los com as RNH.

Os resultados obtidos com a aplicação da Estratégia A foram comparados com o estudo de Sabahi; Omair Ahmad e Swamy (2018) que usou RNH e *Perceptual Hashing* para recuperar conteúdo visual de imagens digitais. Os autores obtiveram um resultado com uma taxa de acerto 85,26% na recuperação de conteúdo visual. Entende-se assim, que os resultados obtidos na Estratégia A foram considerados bons, dada a taxa de acerto de 89,36% obtida na recuperação de valores Hash com o algoritmo de *Differential Hash* e a RNH.

Sobre a detecção de evidências de pornografia infantojuvenil, a aplicação da Estratégia A formada pelo *Differential Hash* e a RNH possibilita a detecção de imagens semelhantes as já detectadas como pornografia infantojuvenil. Além disso, essa tarefa pode ser acrescida de uma segunda etapa, onde o valor Hash Perceptivo da imagem semelhante pode ser recuperado para o valor Hash da imagem original.

Na tabela 37 é apresentado um resumo das execuções e dos resultados obtidos nas fases da Estratégia A.

Tabela 37 – Resumo das execuções e dos resultados das fases da Estratégia A

Fase	Título	Resultados
A1	Seleção dos Algoritmos de Hash de Perceptivo	Foi identificado cinco algoritmos de Hash Perceptivo: *Average Hash, Perceptual Hash, Differential Hash, Wavelet Hashing* e *Crop-resistance Hash.*
A2	Seleção das Bases de Imagens	Foi identificado um total de cinco bases de imagens: *Lenna Database, Washington Database, Palace Database, Mountain Database* e *Park Database*.
A3	Aplicação dos Algoritmos de Hash Perceptivo nas Imagens da fase A2	Foi aplicado os Algoritmos de Hash Perceptivo nas bases de imagens selecionadas na fase A2. Também foi calculado a distância de Hamming de cada aplicação.
A4	Avaliação de Desempenho dos Algoritmos de Hash Perceptivo	Foi calculado as distâncias Euclidiana e de Manhattan de todos os valores obtidos pelo cálculo da distância de Hamming. O algoritmo que obteve o melhor desempenho foi o *Differential Hash.*
A5	Seleção da Técnica de IA para Recuperação de Valor Hash Perceptivo	Foi identificado as Redes Neurais de Hopfield (RNH)
A6	Aplicação da Rede Neural de Hopfield para Recuperação de Valor Hash Perceptivo	Foi realizada a conversão dos valores Hash Perceptivo para ASCII binário. Em seguida, foi definido a arquitetura da RNH. Por fim, foi realizado o treinamento e a aplicação da RNH para recuperar valores Hash Perceptivo.
A7	Avaliação da Rede Neural de Hopfield para recuperação de valor Hash Perceptivo	Foi avaliado o desempenho da RNH na recuperação de valores Hash Perceptivos. A RNH teve acerto em 84 de 94 imagens, o que representa uma taxa de acerto de 89,36%

Fonte: o Autor (2024).

Desta forma, ao desenvolver e aplicar a Estratégia A formada pelo *Differential Hash* e a RNH, foi possível detectar arquivos semelhantes ou iguais que sofreram alguma alteração, e posteriormente, recuperar o valor Hash Perceptivo original.

A seguir são apresentados os resultados da Estratégia B.

4.2. ESTRATÉGIA B

Denominada **Detecção de Pessoas**, esta Estratégia tem como objetivo detectar pessoas em imagens por meio da classificação das cores dos pixels em cor de pele e não cor de pele. Na tabela 38, resumidamente são apresentadas as Bases e Técnicas Computacionais utilizadas no desenvolvimento e aplicação desta Estratégia.

Tabela 38 – Bases e Técnicas Computacionais utilizadas na Estratégia B

ID	Estratégia	Bases	Tipo de Base	Técnicas Computacionais
B	*Detecção de Pessoas*	- *Skin Segmentation* - RGB_HSV_YCBCR - *All Layers* - *Natural Images*	Dados Imagens	- Detecção de Cor de Pele - Floresta Aleatória

Fonte: o Autor (2024).

A Estratégia B é composta por nove fases, são elas:

B1 - Seleção da Base de Dados de Cores de Pele em RGB: Foi definida a base de cores de pele em RGB para ser utilizada nesta Estratégia. Para isso, foi realizada uma pesquisa na literatura e em repositórios de bases de dados por bases de cores de pele em RGB. Foi definido pelo RGB por ser o espaço de cor mais utilizado por dispositivos eletrônicos para produzir e armazenar imagens digitais (KOREN IVANČEVIĆ et al., 2023).

Em relação aos repositórios de bases de dados, foram definidos: *UCI Machine Learning*, *Kaggle*, *Github* e o Portal Brasileiro de Dados Abertos. Foi identificado no repositório *UCI Machine Learning* a base ***Skin Segmentation***. Trata-se de uma base formada por registros classificados em cor-de-pele e não-cor-de-pele. A base possui 245.057 registros e 4 atributos: R, G, B e *SkinColor*. Nos atributos R, G e B, seus valores são números inteiros entre 0 e 255. Já o atributo *SkinColor* é um classificador com dois possíveis estados: 1 que significa cor-de-pele e o valor 2 que significa não-cor-de-pele. Uma amostra da base é ilustrada na Tabela 39.

Tabela 39 – Amostra da base *Skin Segmentation*

R	G	B	SkinColor
168	189	244	1
170	190	247	1
91	36	21	2

Fonte: o Autor (2024)

Os atributos R, G e B representam respectivamente as bandas vermelho, verde e azul. No apêndice M são apresentados os histogramas com a distribuição dos valores dos pixels das bandas R, G e B na base *Skin Segmentation*.

B2 - Enriquecimento da Base de Dados de Cores de Pele com Outras Bandas de Cores: Foi realizado o enriquecimento da base de cores de pele definida na fase B1, com outros espaços de cores, inspirado pelos estudos de Ganesan et al. (2023) e Nasreen et al. (2023) que sugerem o desenvolvimento de novas formas para detectar cor de pele.

Para isso, foi realizada uma busca na literatura por ferramentas que realizem a conversão de valores em RGB para outros espaços de cores. Foram identificadas duas ferramentas: *ColorMath* e *ColorSys.* Por meio destas ferramentas, foi possível converter as cores em RGB para outros 11 espaços de cores: **CMY, CMYK, Xyz, yxY, Yiq, CIE-L*ab, CIE-Lch, CIE-Luv, HSL, HSV e YCbCr**. Os resultados desta conversão foram utilizados para enriquecer a base selecionada na fase B1.

Antes, os registros na base possuíam um total de 4 valores: R, G, B e *SkinColor*. Com a conversão para os outros 11 espaços de cores, cada registro passou a ter um total de 37 valores. São eles: **R, G, B, C, M, Y, C2, M2, Y2, K, X, y3, z, y4, x2, Y5, Y6, i, q, L, A, B2, L2, C3, H, L3, u, v, H2, s, l4, H3, s2, v2, Y7, Cb, Cr e *SkinColor***.

Algumas letras referentes aos espaços de cores foram acrescidas de um número no título dos atributos nesse enriquecimento, por exemplo Y5 e Y6, pois já aparecem em outros espaços de cores. Isto permitiu não repetir o título dos atributos, já que alguns espaços de cores usam as mesmas letras, como é o caso do CMY e Xyz, onde ambos utilizam a letra Y.

Concluída a conversão e o enriquecimento da base, um registro RGB que antes possuía um total de 4 atributos, passou a ter um total de 38 atributos. Toda essa informação será utilizada para gerar duas novas bases de cores na próxima fase.

B3 - Criação das bases de Cores de Pele "RGB_HSV_YCbCr" e "All Layers": Foi gerado duas bases de cores a partir da base *Skin Segmentation* enriquecida na fase B2. Estas bases serão usadas para medir o desempenho da técnica de IA que será selecionada na fase B4.

A primeira base denominada ***All Layers*** contém todos os espaços de cores gerados no enriquecimento realizado na fase B2, mais o atributo classificador *SkinColor*. A segunda base foi gerada a partir de uma cópia da ***All Layers*** e, posteriormente reduzida com o PCA (*Principal Component Analysis*). A aplicação do PCA teve por objetivo identificar quais os atributos mais importantes na base ***All Layers***.

O PCA é um método usado na redução de dimensionalidade e na descoberta dos atributos mais relevantes em bases de dados (Berenguer et al., 2023). Ao aplicar o PCA, descobriu-se que os atributos considerados relevantes na base fazem parte dos espaços de cores RGB, HSV e YCbCr. Assim, gerou-se uma terceira base denominada **RGB_HSV_YCbCr** com os espaços de cores: RGB, HSV e YCbCr, além do atributo classificador *SkinColor*.

É apresentado na Tabela 40 as características das três bases: a base RGB e as duas novas bases geradas a partir do enriquecimento: **RGB_HSV_YCBCR** e **All Layers**.

Tabela 40 – Características das Bases RGB, RGB_HSV_YCBCR e All Layers

Base	Descrição	Total de Registros	Total de Atributos
RGB	Base extraída da UCI		**4**
RGB_HSV_YCBCR	Base enriquecida com os espaços de cores HSV e YCbCr	245.057	**10**
All Layers	Base enriquecida com 11 espaços de cores		**38**

Fonte: o Autor (2024).

Importante destacar que os atributos identificados como relevantes com a aplicação do PCA foram os mesmos identificados na RSL apresentada na subseção 2.6 deste trabalho. Esta informação é ilustrada na Figura 29 deste trabalho.

B4 - Seleção das Técnicas de Inteligência Artificial: Foi realizado uma pesquisa na literatura por publicações relacionadas com a detecção de cor de pele que mencionem técnicas que possam ser utilizadas em tarefas de classificação. No total, foram selecionadas 7 técnicas de IA: Árvore de Decisão, Floresta Aleatória, KNN, MLP, Naive Bayes, Regressão Logística e SVM (GANGWAR et al., 2017; MOREIRA; FECHINE, 2018; NASREEN et al., 2023).

B5 - Aplicação das Técnicas de Inteligência Artificial Selecionadas nas três bases de Dados de Cores de Pele: Foi aplicado as técnicas de IA selecionadas na fase B4 nas três bases de dados com informações sobre cores de pele. A primeira base foi a selecionada na fase B1, e as outras duas foram as bases foram geradas com o enriquecimento realizado na fase B3.

O objetivo desta aplicação foi descobrir qual técnica de IA possui o melhor desempenho na detecção de cor de pele nas três bases de cores de pele: **RGB**, **RGB_HSV_YCbCR** e ***All Layers***. Para realizar estas aplicações, as bases foram divididas da seguinte forma: 70% para treinamento e 30% para teste, o que representa um total de 171.539 registros para o treinamento e 73.518 registros para teste.

Em cada uma das aplicações, calculou-se as seguintes métricas para avaliar o desempenho de cada técnica da IA: Matriz de Confusão, Precisão, *Recall* e *F-Score* (Nasreen et al., 2023; Samuelsson, 2018). A avaliação do desempenho de cada técnica de IA é descrita na fase B6.

B6 - Avaliação de Desempenho das Técnicas de Inteligência Artificial Selecionadas nas três bases de Dados de Cores de Pele: Foi avaliado o desempenho das técnicas de IA aplicadas na fase B5. Para isso, foram utilizadas as seguintes métricas: Matriz de Confusão, Acurácia, Precisão, *Recall* e *F-Score* (NASREEN et al., 2023; SAMUELSSON, 2018).

Na tabela, são apresentados os resultados obtidos com a aplicação das técnicas de IA selecionadas na fase B4 e aplicadas na fase B5 nas três bases: **RGB**, **RGB_HSV_YCbCR** e ***All Layers.***

Tabela 41 – Avaliação das técnicas de Inteligência Artificial aplicadas nas bases: RGB, RGB_HSV_YCbCR e *All Layers*

Técnica	**Arquitetura**	**Base Utilizada**	**Acurácia**	**Precisão**		**Recall**		**F-Score**		**Matriz de Confusão**	
				1	**2**	**1**	**2**	**1**	**2**	**VP + VN**	**FP + FN**
Árvore de Decisão	Entropia como critério de decisão para o classificador	RGB	0,9991566691150460	1,000	0,998	0,999	0,998	0,999	0,998	73456	62
		RGB_HSV_YCbCR	0.9995783345575233	1,000	0,999	1,000	1,000	1,000	0,999	73487	31
		All Layers	0.9994695176691423	1,000	0,999	1,000	0,999	1,000	0,999	73479	39
KNN	Para as três bases, o número de K com o melhor desempenho foi 4	RGB	0.9994015071139041	0,997	1,000	1,000	0,999	0,999	1,000	73474	44
		RGB_HSV_YCbCR	0.9994559155580947	0,997	1,000	1,000	0,999	0,999	1,000	73478	40
		All Layers	0,9994559155580940	0,997	1,000	1,000	0,999	0,999	1,000	73478	40
Regressão Logística	Arquitetura binária e kernel “lbfgs”	RGB	0,9189994287113360	0,791	0,954	0,826	0,943	0,808	0,949	67563	5955
		RGB_HSV_YCbCR	0,9612611877363360	0,843	0,999	0,998	0,952	0,914	0,975	70670	2848
		All Layers	0,9942055006937070	0,978	0,998	0,994	0,994	0,986	0,996	73092	426
MLP	Arquitetura de 15 camadas com 15 neurônios cada, kernel lbfgs e 1000 épocas	RGB	0.9979868875649501	0,992	1,000	0,999	0,998	0,995	0,999	73370	148
		RGB_HSV_YCbCR	0.9994831197801899	0,998	1,000	0,999	0,999	0,999	1,000	73480	38
		All Layers	0.9995103240022851	0,998	1,000	1,000	0,999	0,999	1,000	73482	36
Naive Bayes	Arquitetura com Kernel de Estimação de Densidade	RGB	0,9241138224652460	0,876	0,934	0,737	0,973	0,801	0,953	63939	5579
		RGB_HSV_YCbCR	0,9912266383742750	0,965	0,998	0,994	0,991	0,974	0,994	72873	645
		All Layers	0,9943687260262790	0,975	0,999	0,998	0,993	0,987	0,996	73104	414
Floresta Aleatória	Entropia como critério de decisão e 3 árvores de decisão em sua arquitetura	RGB	0,9998231725563800	0,999	1,000	1,000	1,000	1,000	1,000	73505	13
		RGB_HSV_YCbCR	0,9997959683342850	0,999	1,000	1,000	1,000	1,000	1,000	73503	15
		All Layers	**0,9998639788895230**	**0,999**	**1,000**	**1,000**	**1,000**	**1,000**	**1,000**	**73508**	**10**
SVM	Arquitetura com Kernel “rbf”	RGB	0,9983541445632360	0,992	1,000	1,000	0,998	0,996	0,999	73397	121
		RGB_HSV_YCbCR	0,9980140917870450	0,992	0,999	0,998	0,998	0,995	0,999	71372	146
		All Layers	0,998027693898093	0,995	0,999	0,998	0,998	0,995	0,999	73373	145

Fonte: o Autor (2024).

A técnica de IA que obteve o melhor desempenho na detecção de cor de pele nas três bases de foi a Floresta aleatória, destacada em verde na Tabela 41. A Floresta aleatória obteve uma acurácia de **0,9998639788895230**, a maior acurácia entre as técnicas avaliadas. Sobre os resultados das métricas de Precisão, *Recall* e *F-Score*, a técnica da Floresta Aleatória obteve 1.000 em todas as demais métricas, com exceção da Precisão para o valor 1, que recebeu o valor de 0,999 em todas as três bases.

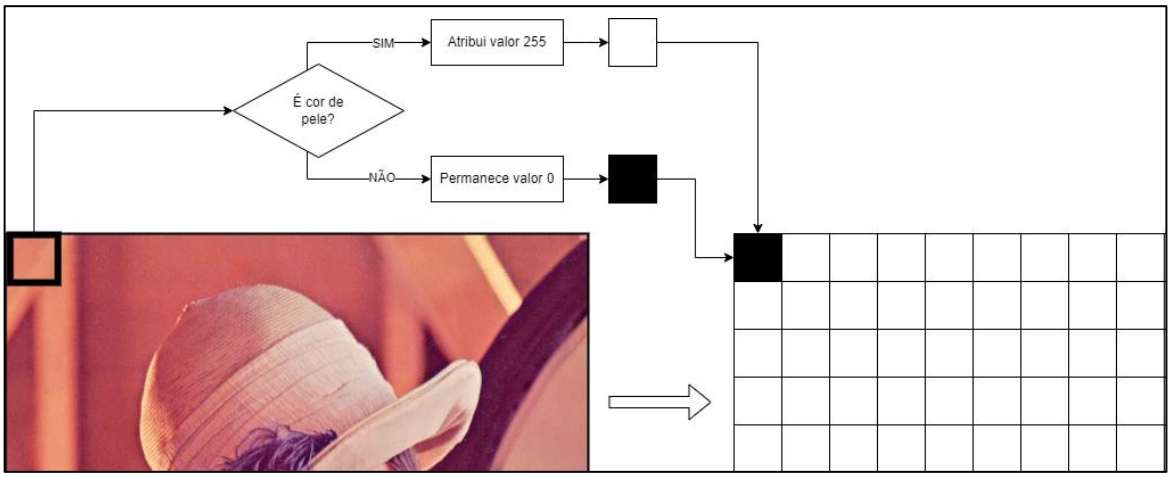
Em relação a Matriz de Confusão, a tabela 41 apresenta as seguintes métricas: **VP + VN** e **FP + FN**. Enquanto VP + VN representa a soma dos acertos pela diagonal dos verdadeiros positivos e verdadeiros negativo**s**, **FP + FN** representa a soma de erros pela diagonal dos falsos positivos e falsos negativos. A Floresta Aleatória foi a técnica de IA que melhor classificou os registros com 73.508 na base ***All Layers***, 73.503 na base ***RGB_HSV_YCbCR*** e 73.505 na base ***RGB***. Assim, definiu-se pela Floresta Aleatória para dar continuidade com as próximas fases.

B7 - Criação de um sistema para Segmentação de Cor de Pele: Foi criado um sistema de Segmentação de Cor de pele com a Floresta Aleatória, técnica de IA que obteve o melhor desempenho na avaliação realizada na fase B6. Este sistema de Segmentação de cor de pele será utilizado para avaliar qualitativamente a detecção de cor de pele.

Um sistema de segmentação de cor de pele tem por objetivo, destacar os pixels com cores de pele em uma imagem fornecida como entrada. Para isto, gera-se uma máscara da mesma dimensão da imagem fornecida como entrada, e em seguida, preenche-se pixels desta máscara na mesma posição da imagem fornecida como entrada com as cores branca e preta.

Quando a cor do pixel é detectada como cor de pele, aquele pixel é preenchido com a cor branca na máscara na mesma posição, entretanto, quando a cor do pixel é detectada como não-cor-de-pele, aquele pixel é preenchido com a cor preta na máscara na mesma posição (Ding; Liu; Lei, 2023; Ly et al., 2020). O funcionamento do sistema de Segmentação de cor de pele é ilustrado na figura 38.

Figura 38 – Sistema de segmentação de cor de pele



Fonte: o Autor (2024).

O sistema de segmentação de cor de pele ilustrado na Figura 38 funciona da seguinte forma: Ao receber uma imagem como entrada, gera-se uma máscara de mesma dimensão. Em seguida, preenche-se todos os pixels da máscara com o valor 0 para não deixar valores nulos. Por fim, inicia-se o processo de classificação de cor de pele com a Floresta Aleatória. Para isso, coleta-se os valores RGB de cada pixel da imagem fornecida como entrada e converte para os espaços de cores definidos na fase B2. Esta conversão permite avaliar o sistema de segmentação de cor de pele com as três bases: **RGB**, **RGB_HSV_YCbCr** e ***All Layers***.

B8 - Seleção de Base de Imagens de Pessoas: Foi selecionada uma base com imagens de pessoas para avaliar o desempenho do sistema de segmentação de cor de pele criado na fase B7. Para isso, foi realizada uma busca na literatura por bases formadas por imagens de pessoas com diferentes etnias, gêneros e idades.

Encontrou-se no repositório *Kaggle*, a base de imagens: ***Natural Images.*** Trata-se de uma base composta por 6899 imagens divididas em 8 grupos: Aviões, Carros, Gatos, Cães, Flores, Frutas, Motos e Pessoas. O grupo Pessoas possui um total de 986 imagens, e tem como origem outras duas bases de imagens distintas: **PubFig83** e **LFW Dataset**.

Selecionada a base de imagens de pessoas, extraiu-se uma amostra aleatória. Esta amostra é composta por 20 imagens com pessoas de diferentes gêneros, etnias e idades. O objetivo dessa amostra é avaliar o desempenho do sistema de segmentação de cor de pele criada na fase B7.

B9 - Avaliação do Sistema de Segmentação de Cor de Pele: Foi avaliado o desempenho do sistema de segmentação de cor de pele desenvolvido na fase B7 e aplicado em uma amostra de imagens de pessoas extraídas aleatoriamente da base selecionada na fase B8.

Para cada uma das 20 imagens extraídas da base ***Natural Images***, foi executado três vezes o sistema de segmentação de cor de pele, cada execução com uma base de cor de pele diferente: **RGB**, **RGB_HSV_YCbCr** e ***All Layers***. O objetivo foi descobrir com qual base, o sistema de segmentação de cor de pele possui o melhor desempenho. Este desempenho será medido pelo total de pixels detectados como cor de pele e o tempo médio de execução.

Além do preenchimento dos pixels da máscara com as cores branca e preta, o sistema de segmentação de cor de pele exibe a resolução da imagem fornecida como entrada, o total de pixels da imagem, o total de pixels detectados como cor de pele e como não-cor-de-pele. As 20 imagens selecionadas possuem uma resolução de 256x256, ou seja, possuem um total de 65.536 pixels. É apresentado na tabela 42 a avaliação do sistema de segmentação de cor de pele.

Tabela 42 – Avaliação do Sistema de Segmentação de cor de pele

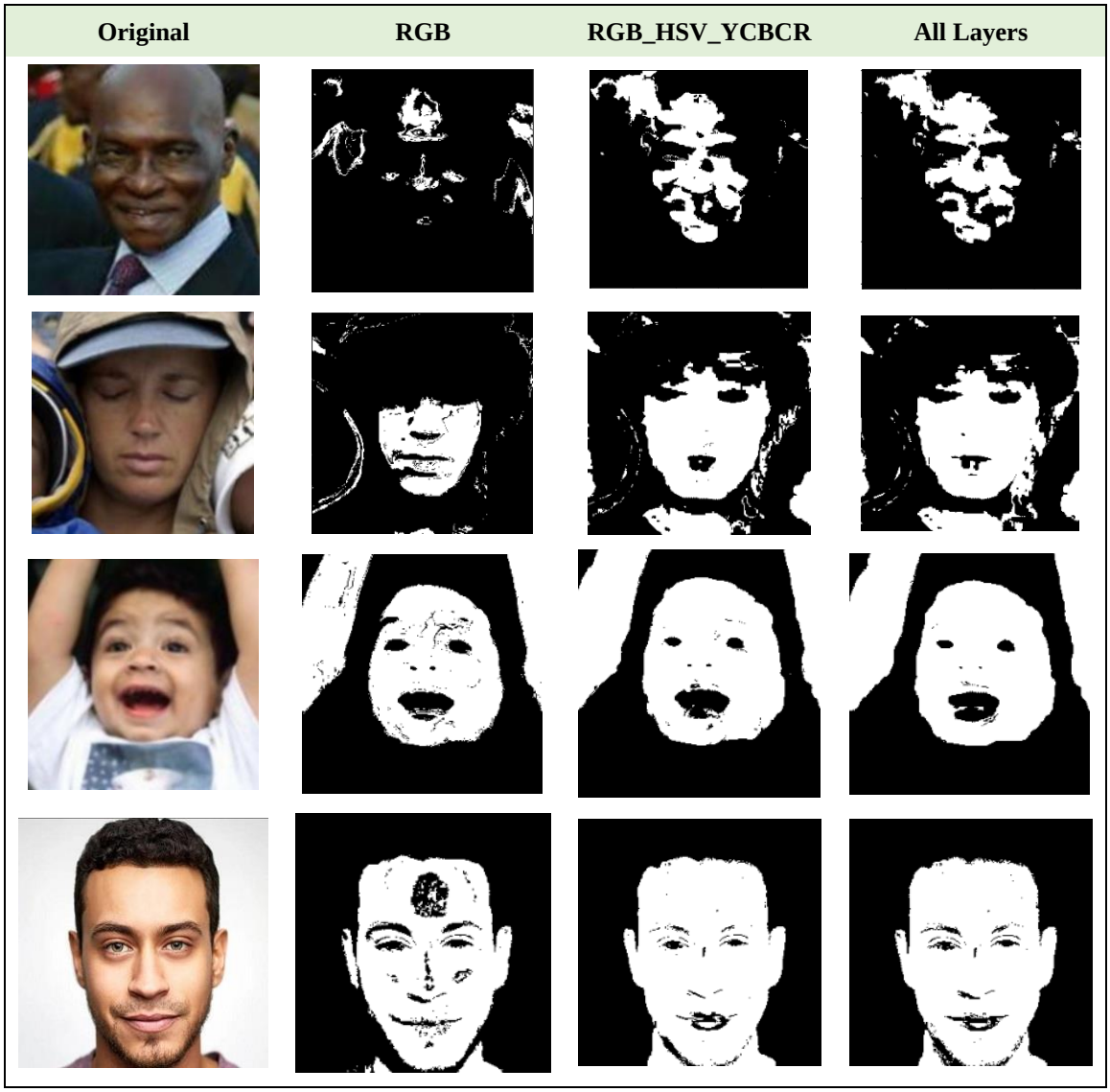
Nome da Imagem	**Taxa de Pixels Identificados como Cor de Pele (%)**		
	Base RGB	**Base RGB_HSV_YCbCr**	**Base All Layers**
img (1)	6,7 %	17,78 %	17,15 %
img (2)	15,15 %	31,33 %	32,43 %
img (3)	42,6 3%	46,86 %	46,63 %
img (4)	33,59 %	39,62 %	38,69 %
img (5)	24,58 %	30,76 %	29,80 %
img (6)	55,11 %	61,09 %	58,41 %
img (7)	38,20 %	49,81 %	50,58 %
img (8)	23,68 %	30,50 %	31,01 %
img (9)	42,27 %	53,67 %	49,59 %
img (10)	32,58 %	40,91 %	40,52 %
img (11)	7,19 %	14,37 %	14,01 %
img (12)	31,68 %	41,07 %	36,33 %
img (13)	4,08 %	19,30 %	19,33 %
img (14)	18,24 %	23,60 %	21,13 %
img (15)	23,13 %	31,58 %	30,32 %
img (16)	21,39 %	26,43 %	27,24 %
img (17)	33,42 %	38,36 %	38,30 %
img (18)	29,52 %	43,77 %	40,91 %
img (19)	31,70 %	35,70 %	34,28 %
img (20)	14,14 %	14,54 %	16,64 %

Fonte: o Autor (2024)

Na tabela 42 são apresentadas as taxas de pixels detectados como cor de pele pelo sistema de segmentação de cor de pele aplicado nas 20 imagens selecionadas. O sistema de segmentação de cor de pele obteve o melhor resultado com a base de cor de pele **RGB_HSV_YCbCr.**

Ao utilizar a base **RGB_HSV_YCbCr,** o sistema de segmentação de cor de pele detectou mais pixels em 14 imagens, Já quando utilizou a base ***All Layers***, detectou-se mais pixels com cor de pele em 6 imagens. Por fim, quando se utilizou a base **RGB**, não se detectou mais pixels de cores de pele do que nenhuma das outras duas bases. Na figura 39, são ilustradas as quatro primeiras imagens da amostra gerada na fase B8 e suas três máscaras geradas pelo sistema de segmentação de cor de pele com cada uma das bases de cores de pele.

Figura 39 – Máscaras geradas pelo sistema de segmentação de cor de pele com as bases de cores de pele: RGB, RGB_HSV_YCbCr e *All Layers*



Fonte: o Autor (2024).

Ao analisar a figura 39, evidencia-se os problemas para detectar cores de pele ao utilizar somente a base RGB. As regiões de cores de pele que aparecem nas máscaras com manchas na cor preta estão relacionadas a itens como iluminação e brilho. Já as bases **RGB_HSV_YCBCR** e **All Layers** tiveram resultados similares e considerados relevantes

Outra métrica usada para avaliar o desempenho do sistema de segmentação de cor de pele foi o tempo de processamento. Utilizou-se essa métrica com o objetivo de descobrir com qual base, o sistema de segmentação de cor de pele irá gerar uma máscara com menor tempo: **RGB**, **RGB_HSV_YCbCr** e ***All Layers.*** O tempo de processamento é considerado relevante porque esta Estratégia de Detecção de Pessoas tem por objetivo apoiar a execução de exames periciais na detecção de evidências de pornografia infantojuvenil, e o tempo de detecção é determinante para impedir possíveis propagações (AL-NABKI et al., 2020).

É apresentado na tabela 43 o tempo de processamento do sistema de segmentação de cor de pele com as bases: **RGB_HSV_YCbCr** e ***All Layers***. Como a base RGB não detectou mais pixels de cores de pele do que nenhuma das outras duas bases, não foi considerado o seu tempo de processamento.

Tabela 43 – Tempo de processamento do Sistema de Segmentação de Cor de Pele com as bases: RGB_HSV_YCbCr e *All Layers*.

Base	Tempo de Processamento do Sistema de Segmentação de Cor de Pele
RGB_HSV_YCBCR	**28 segundos**
All Layers	1 minuto e 29 segundos

Fonte: o Autor (2024).

Analisando a tabela 43, percebe-se que ao utilizar a base **RGB_HSV_YCBCR,** o sistema de segmentação de cor de pele obteve um tempo de processamento menor, com 28 segundos, enquanto ao utilizar a base ***All Layers,*** obteve um tempo de processamento de 1 minuto e 29 segundos. Assim, pode-se concluir que quantos mais espaços de cores forem adicionados na base RGB, maior será o tempo de processamento.

Os resultados obtidos com a aplicação da Estratégia B foram comparados com os estudos de Dhivyaa et al. (2020) e Gangwar et al. (2017) que detectaram pessoas com um sistema de segmentação de cor de pele formado pela Floresta Aleatória. Dhivyaa et al. (2020) obteve uma acurácia de 98,14%, enquanto Gangwar et al. (2017) obteve uma acurácia de 97,30%.

Ao comparar os resultados obtidos nessa Estratégia B com os estudos de Dhivyaa et al. (2020) e Gangwar et al. (2017), entende-se que os resultados obtidos foram bons, dada a acurácia de 99,98% obtida com a Floresta Aleatória e a base de cores de pele RGB enriquecida com os espaços de cores HSV e YCbCr: a base **RGB_HSV_YCBCR**.

Sobre a detecção de evidências de pornografia infantojuvenil, a utilização desta Estratégia possibilitou uma precisão interessante na detecção de pessoas em arquivos de imagens digitais. Além disso, combinar a técnica Floresta Aleatória e a base RGB enriquecida com os espaços de cores HSV e YCbCr possibilitou o desenvolvimento de um sistema de segmentação de cor de pele com um tempo de processamento considerado interessante.

Na tabela 44 é apresentado um resumo das execuções e dos resultados obtidos nas fases da Estratégia B.

Tabela 44 – Resumo das Atividades realizadas na Estratégia B

Fase	Título	Resultados
B1	Seleção da Base de Cores de Pele em RGB	Foi identificado no repositório *UCI Machine Learning* a base *Skin Segmentation*
B2	Enriquecimento da Base de Cores de Pele com Outras Bandas de Cores	Foi realizado o enriquecimento da base *Skin Segmentation* com outros 11 espaços de cores: **CMY, CMYK, Xyz, yxY, Yiq, CIE-L*ab, CIE-Lch, CIE-Luv, HSL, HSV** e **YCbCr**
B3	Criação das bases de Cores de Pele "RGB_HSV_YCbCr" e "All Layers":	Foi gerado duas novas bases de cor de pele: a base **RGB_HSV_YCbCr** com os espaços de cores RGB, HSV e YCbCr. E a base ***All Layers*** com todos os outros 11 espaços de cores gerados na fase B2.
B4	Seleção das Técnicas de Inteligência Artificial	Foram selecionadas 7 técnicas de IA: **Árvore de Decisão, Floresta Aleatória, KNN, Naive Bayes, Regressão Logística, SVM** e **MLP**.
B5	Aplicação das Técnicas de Inteligência Artificial Selecionadas nas três bases de Dados de Cores de Pele	Foi aplicado as 7 técnicas de IA selecionadas na fase B4 e aplicados nas três bases: **RGB**, **RGB_HSV_YCbCr** e ***All Layers***
B6	Avaliação de Desempenho das Técnicas de Inteligência Artificial Selecionadas nas três bases de Dados de Cores de Pele	Foi avaliado o desempenho das técnicas de IA aplicadas na fase B5 com as seguintes métricas: Acurácia, Precisão, Recall, F-Score e Matriz de Confusão. A técnica que teve o melhor desempenho foi a Floresta Aleatória, com uma acurácia de 99,98%.
B7	Criação de um sistema para Segmentação de Cor de Pele	Foi criado um sistema de segmentação de cor de pele com a técnica da Floresta Aleatória
B8	Seleção de Base de Imagens de Pessoas	Foi selecionado no repositório *Kaggle*, a base ***Natural Images***. A base possui um total de 986 imagens de pessoas. Em seguida, foi extraído uma amostra aleatória formada por 20 imagens para ser usada na próxima fase.

Fase	Título	Resultados
B9	Avaliação do Sistema de Segmentação de Cor de Pele	Foi avaliado o sistema de segmentação de cor de pele aplicado na base de imagens de pessoas selecionada na fase B8 com as seguintes métricas: Taxa de pixels detectados como cor de pele e o tempo de processamento. O sistema de Segmentação de cor de pele obteve um melhor desempenho ao utilizar a base RGB_HSV_YCbCr, pois detectou mais pixels como cor de pele em 14 das 20 imagens, e obteve o menor tempo de processamento: 28 segundos.

Fonte: o Autor (2024).

Desta forma, ao desenvolver e aplicar a Estratégia B formada pela Detecção de cor de pele, a Floresta Aleatória e a base de cor de pele *Skin Segmentation* em RGB enriquecida com os espaços de cores HSV e YCbCr, foi possível detectar pessoas em imagens.

A seguir são apresentados os resultados da Estratégia C.

4.3. ESTRATÉGIA C

Denominada: **Detecção de Conteúdo Textual relacionado com Pornografia Infantojuvenil**, esta Estratégia tem como objetivo detectar conteúdo textual relacionado com Pornografia Infantojuvenil. Na tabela 45, resumidamente são apresentadas as Bases e Técnicas Computacionais utilizadas no desenvolvimento e aplicação desta estratégia.

Tabela 45 – Bases e Técnicas Computacionais utilizadas na Estratégia C

ID	Estratégia	Bases Utilizadas	Tipo de Base	Técnicas Computacionais
C	Detecção de Conteúdo Textual relacionado com Pornografia Infantojuvenil	FUNSD	Imagens	- OCR - Extração de Metadados - LSTM - PLN

Fonte: o Autor (2024).

A Estratégia C é composta por sete fases, são elas:

C1 - Seleção da Base de Imagens com Conteúdo Textual: Foi selecionada a base de imagens com conteúdo textual para ser utilizada no desenvolvimento desta estratégia. Para isso foi realizada uma pesquisa sobre bases de imagens utilizadas para extração de metadados e

OCR nos seguintes repositórios de bases de dados e imagens: *Kaggle, UCI Machine Learning*, *Github* e o Portal Brasileiro de Dados Abertos.

A base selecionada foi a FUNSD (*Form Understanding in Noisy Scanned Documents*), composta por 199 imagens contendo diversos formulários, textos, prescrições médicas e outros documentos com ruídos, distorções, sombras e outras alterações (JAUME; KEMAL EKENEL; THIRAN, 2019).

C2 - Pré-processamento da base das Imagens selecionada na fase C1: Foi realizada o pré-processamento das imagens da base selecionada na fase C1. O objetivo foi obter um ganho de desempenho na detecção de conteúdo textual.

Inicialmente extraiu-se uma amostra aleatória de imagens da base selecionada na fase C1. Essa amostra é composta por um total de 6 imagens de textos com as mais diversas variações, como inclinação, rotação, ruídos, textos parcialmente apagados, textos em manuscritos, marcas d'água, dentre outros. Essa amostra pode ser consultada no apêndice H deste trabalho.

Definida a amostra de imagens, o próximo passo foi definir quais tarefas serão utilizadas para pré-processar estas imagens. O pré-processamento tem como objetivo promover um ganho de desempenho na execução das próximas fases: C3 e C4 (Matsuzaka; Yashiro, 2023). No total, foram realizadas 6 tarefas no pré-processamento, todas descritas na tabela 46.

Tabela 46 – Tarefas utilizadas no pré-processamento das imagens

Tarefa	Descrição
Redimensionar	Redimensionamento de imagens por meio da Interpolação Bicúbica (42), técnica que utiliza polinômios cúbicos em duas direções (horizontal e vertical) Desta forma, é possível estabelecer novos valores para os pixels da imagem ao modificar suas dimensões (Altura e Largura). $$p(x,y) = \sum_{i=0}^{3}\sum_{j=0}^{3} a_{ij}\, x^i y^j \quad (42)$$
Normalização	Ajuste nos valores de intensidade dos pixels para mantê-los dentro de um intervalo desejado com o objetivo de padronizar a escala destes valores. Para isso, foi utilizada a Normalização Linear com Min-Max (43), comumente utilizada em tarefas de pré-processamento de imagens para ganho de desempenho (BILLA et al., 2024). $$I' = \frac{I - I_{min}}{I_{max} - I_{min}} * (b - a) + a \quad (43)$$

Tarefa	Descrição
Redução de Ruídos	Ajuste nos valores de intensidade dos pixels ao atribuir um valor médio ponderado semelhante aos valores dos pixels vizinhos. Uma forma de realizar essa redução de ruídos é utilizar o Algoritmo de Médias Não-Locais ou NL-Means (44) que considera tanto a proximidade espacial, quanto à similaridade de intensidade. $$\hat{I}(x) = \frac{\sum_{y\in\Omega} w(x,y)I(y)}{\sum_{y\in\Omega} w(x,y)} \quad (44)$$
Conversão para Níveis de Cinza	A conversão para níveis de cinza é um processo que transforma uma imagem colorida composta por três ou quatro bandas, em uma única banda em tons de cinza. A conversão de RGB para níveis de cinza (45) é uma tarefa comumente utilizada para pré-processar imagens antes de submetê-las a técnicas de IA (FAN et al., 2021). $$grayscale = (0.299 * R) + (0.587 * G) + (0.114 * B) \quad (45)$$
Dilatação e Erosão	Trata-se de operações morfológicas que buscam manipular a estrutura de objetos em uma imagem binária. A combinação da Dilatação e Erosão é comumente utilizada para tratar buracos, corrigir ruídos e separar os objetos conectados. Enquanto a dilatação (46) busca expandir as regiões brancas, a erosão (47) busca encolher as regiões brancas (DETSIKAS; MITIANOUDIS; PAPAMARKOS, 2024). $$Dil = (I \oplus B)(x) = max_{b\epsilon B} I(x-b) \quad (46)$$ $$Ers = (I \ominus B)(x) = min_{b\epsilon B} I(x+b) \quad (47)$$
Limiarização por OTSU	Separação das cores dos pixels em duas classes distintas (1 e 0) baseada na análise do histograma da imagem. O objetivo é encontrar um valor de limiar (48) que minimiza a variância intraclasse ou, alternativamente, maximiza a variância interclasse (OTSU, 1979). $$\sigma_b^2(T) = {}_{w0}\ (T)_{w1}(T)[_{\mu 0}(T) - _{\mu 1}(T)]^2 \quad (48)$$

Fonte: o Autor (2024).

C3 - Extração dos Metadados da Imagem: Foi extraído os metadados das imagens da amostra pré-processada na fase C2. Para isto, desenvolveu-se um código em python que extrai os metadados de uma imagem digital e os armazena em uma *BagOfWords* (BoW). Foi definido pelo uso de uma BoW para armazenar os metadados extraídos devido ao uso de Processamento de Linguagem Natural (PLN) nas próximas fases (UKWEN; KARABATAK, 2021).

Foi desenvolvido um código em Python para extrair dois tipos de metadados de arquivos de imagens digitais: Básicos e Avançados. Os metadados básicos são dados relacionados com as propriedades de um arquivo de imagem digital. Já os metadados EXIF (*Exchangeable Image File Format*), chamados neste trabalho de avançados, são específicos para imagens digitais geradas por câmeras digitais e outros dispositivos eletrônicos. Na Tabela 47, são apresentadas os metadados Básicos e Avançados que serão utilizados nesse trabalho.

Tabela 47 – Metadados Básicos e Avançados

Tipo de Metadado	Metadados Utilizados
Básico	Nome, Altura, Largura, Tamanho, Formato e Quantidade de Frames existentes na imagem
Avançado	Fabricante e Modelo do dispositivo eletrônico que gerou a imagem, Caminho da imagem no armazenamento do dispositivo eletrônico, data e hora da geração da imagem, descrição, comentários e links anexados ao arquivo

Fonte: o Autor (2024).

Concluída a extração dos metadados e o armazenamento deste conteúdo na BoW, seguiu-se para a próxima extração, a extração do conteúdo textual da imagem com o OCR (*Optical Character Recognition).*

C4 - Extração do Conteúdo Textual da Imagem com OCR: Foi extraído o conteúdo textual das imagens pré-processadas na fase C2. Para isto, foi desenvolvido um código em python que aplica o OCR para extrair o conteúdo textual da imagem e o armazena na mesma BoW gerada na fase C3.

A aplicação do OCR foi realizada com a utilização de duas ferramentas: o **Tesseract** e o **EasyOCR**. Estas ferramentas foram selecionadas por serem específicas para OCR e possuírem arquiteturas distintas. Enquanto o Tesseract usa as redes LSTM em conjunto com automações, o EasyOCR utiliza em conjunto as redes LSTM e CNN. A utilização destas ferramentas foi inspirada pelo estudo de Schönfelder et al. (2024) que descreve os ganhos de desempenho ao utilizá-las em conjunto. Ao término da aplicação do OCR, a BoW gerada na fase C3 passou a ter os Metadados básicos e avançados, mais o conteúdo textual extraído pela aplicação do OCR.

C5 - Avaliação da Extração de Metadados e OCR: Foi avaliado o desempenho obtido nas extrações de Metadados e OCR realizadas nas fases C3 e C4. Esta avaliação foi realizada ao comparar o conteúdo destas extrações armazenadas na BoW com o arquivo de anotações da base de imagens selecionada na fase C1. Este arquivo de anotações é do tipo JSON e possui todo o conteúdo textual existente nas imagens, com comentários e localização de cada palavra.

A comparação do conteúdo textual da BoW e do arquivo de anotações foi realizada com as seguintes métricas: Total de Palavras, Taxa de Erro de Caracteres (CER), Taxa de Erro de Palavras (WER) e a Taxa de Acerto. Estas métricas foram definidas por serem comumente utilizadas para avaliar o desempenho de tarefas usadas em análises textuais (Mulyanto; Hartati;

Wardoyo, 2022). Na tabela 48, é apresentado os resultados obtidos das métricas utilizadas na avaliação das extrações dos metadados e OCR.

Tabela 48 – Avaliação das Extrações de Metadados e OCR

ID	Nome da Imagem	Total de Palavras	Taxa de Erro de Caracteres (CER)	Taxa de Erro de Palavras (WER)	Taxa de Acerto %
01	660978	71	0,9973	0,9558	**95,77%**
02	00865872	98	1,2440	0,9861	73,47%
03	00920294	63	1,0554	0,9	79,37%
04	01122115	163	1,0733	1,0	**90,18%**
05	81310636	52	1,1074	0,9761	80,77%
06	82573104	102	1,1651	1,0	88,24%

Fonte: o Autor (2024)

Ao analisar a tabela 48, percebe-se que as imagens que tiveram a maior taxa de acerto foram as: 660978 e 01122115 com 95,77% e 90,18% respectivamente. Em ambas as imagens, a taxa de acerto foi maior que 90%. Em seguida, com uma taxa de acerto entre 80% e 90%, as imagens 81310636 e 82573104 obtiveram 80,77% e 88,24% respectivamente. Por fim, as duas imagens que obtiveram a menor taxa de acerto, entre 70% e 80%, as imagens 00865872 e 00920294 obtiveram 73,47% e 79,37% respectivamente.

De acordo com as afirmações feitas por Mulyanto, Hartati e Wardoyo (2022), para as métricas CER e WER, valores próximos de 0 são classificados como excelentes, enquanto valores entre 1,0 e 10,0 são classificados como bons, principalmente ao lidar com imagens com baixa qualidade. Entende-se, então que os resultados obtidos ao pré-processar as imagens com as tarefas descritas na fase C2, para em seguida, extrair os metadados e o conteúdo textual com OCR foram bons.

Os resultados obtidos com as extrações dos Metadados e OCR apresentados na Tabela 48 foram comparados com outro estudo identificado na literatura que também extraiu conteúdo textual com as ferramentas Tesseract e EasyOCR. Os autores Pandey et al. (2023) obtiveram uma taxa de acerto entre 78,95% e 87,53% em suas extrações, e também embasados pelas afirmações de Mulyanto, Hartati e Wardoyo (2022), consideraram estes resultados bons.

Entende-se assim que os resultados obtidos com a taxa de acerto entre 95,77% e 73,47%, e taxas de erro CER e WER entre 0,9 e 1,25 com as com as extrações realizadas nas fases C3 e C4 nas imagens pré-processadas na fase C2 foram considerados bons.

C6 - Estruturação dos Dados Extraídos nas fases C3 e C4 com PLN: O conteúdo das extrações realizadas nas fases C3 e C4 e armazenadas em uma BoW foram estruturados com a utilização de tarefas de PLN. Na tabela 49 são descritas as técnicas e tarefas de PLN usadas para estruturar o conteúdo textual da BoW, juntamente com sua descrição.

Tabela 49 – Técnicas e Tarefas de PLN utilizadas para estruturar o conteúdo textual da BoW

Item	Tipo	Descrição
Conversão para Minúsculas	Tarefa	Garantir a uniformidade dos dados ao deixar todos os caracteres em minúsculos.
Tokenização	Técnica	Transformar o texto em uma lista de palavras para permitir a análise de cada palavra separadamente.
Remoção de Valores Duplicados	Tarefa	Reduzir a redundância de palavras
Ordenação Alfabética	Tarefa	Auxiliar a visualização e organização das palavras existentes em uma BoW ao ordená-las de forma alfabética
Remoção de Caracteres isolados	Tarefa	Remover palavras compostas por um único caractere que não possuem um significado.
Remoção de Stopwords	Técnica	Remover palavras que não possuem um significado.

Fonte: o Autor (2024)

Concluída a aplicação das tarefas de PLN descritas na Tabela 49, foi possível estruturar o conteúdo das BoW, tornando todas as letras minúsculas, removendo duplicatas, ordenando as palavras, e limpando símbolos soltos, palavras compostas por um único caractere, marcadores de lista e abreviações. Estas tarefas foram definidas por serem comumente recomendadas e utilizadas como preparação para análises textuais, como busca de palavras-chave, modelagem de tópicos e classificação de texto (MONTASARI, 2023; UKWEN; KARABATAK, 2021).

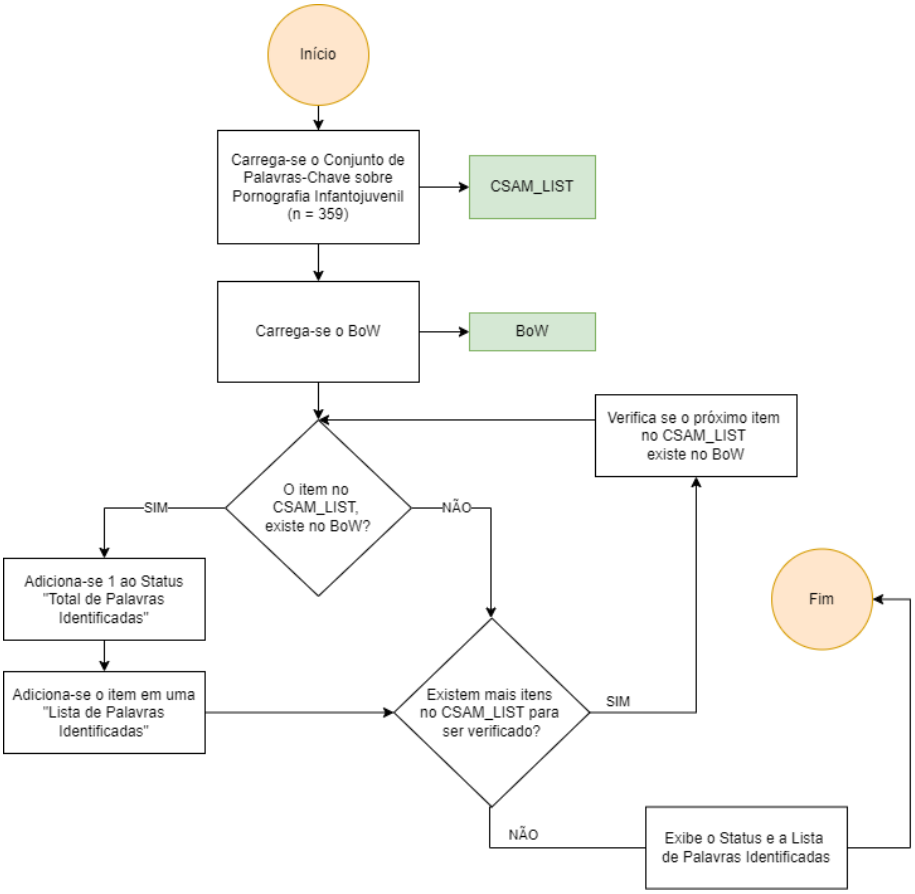
C7 - Identificação de Palavras-Chave relacionadas com Pornografia Infantojuvenil no conteúdo estruturado na fase C6: Foi desenvolvido um código em python para buscar no conteúdo estruturado na fase C6 com um conjunto de palavras-chave relacionadas à Pornografia Infantojuvenil.

O conjunto de palavras-chave foi identificado na literatura nos estudos realizados por Frank, Westlake e Bouchard (2010) e Wang et al. (2023). Os autores descreveram as principais palavras-chave relacionadas com Pornografia Infantojuvenil. Estas palavras-chave são descritas na Tabela 23 da RSL disponível na seção 2.6 deste trabalho. No total, o conjunto compreende 359 palavras-chave relacionadas à Pornografia Infantojuvenil.

Definido o conjunto de palavras-chave e o conteúdo das BoW estruturado com PLN na fase C6, foi desenvolvido um código que identifica se uma palavra existe em ambos. No código, o conjunto de palavras-chave relacionadas com Pornografia Infantojuvenil é denominado: **CSAM_LIST,** enquanto o conteúdo estruturado na fase C6 é denominado **BoW**. De forma resumida, o código desenvolvido verifica se as palavras da **CSAM_LIST** existem na **BoW**. Em caso positivo, detecta-se conteúdo textual relacionado com Pornografia Infantojuvenil.

Na figura 40, é ilustrado o funcionamento da detecção de conteúdo textual relacionado com Pornografia Infantojuvenil no conteúdo estruturado com PLN.

Figura 40 – Funcionamento da detecção de conteúdo textual relacionado com Pornografia Infantojuvenil no conteúdo estruturado com PLN



Fonte: o Autor (2024).

Ao analisar a figura 40, compreende-se que o funcionamento do código se inicia com o carregamento da **CSAM_LIST** e do **BoW.** Em seguida, é verificado a existência do primeiro item do **CSAM_LIST** no **BoW**. Caso positivo, incrementa-se 1 ao Status "Total de Palavras Identificadas" e o item é adicionado a uma "Lista de Palavras Identificadas". Caso contrário, o código prossegue para verificar a existência dos outros itens da **CSAM_LIST**. Quando todos os itens tiverem sido verificados, é exibido o status final com o total de palavras identificadas e a lista das palavras identificadas.

Entende-se que os resultados obtidos ao pré-processar imagens com as tarefas descritas na fase C2, e a extração de metadados básicos e avançados, bem como a do conteúdo textual com OCR, permitiram a obtenção total do conteúdo textual de uma imagem. Em seguida, ao estruturar este conteúdo textual com PLN, foi possível verificar a existência de conteúdo textual relacionado com Pornografia Infantojuvenil ao comparar com as palavras-chave identificadas na literatura nos estudos de Frank, Westlake e Bouchard (2010) e Wang et al. (2023).

Na tabela 50 é apresentado um resumo das execuções e dos resultados obtidos nas fases da Estratégia C.

Tabela 50 – Resumo das Atividades realizadas na Estratégia C

Fase	Título	Resultados
C1	Seleção da Base de Imagens com Conteúdo Textual	Foi identificado a base **FUNSD** *(Form Understanding in Noisy Scanned Documents).*
C2	Pré-processamento da base das Imagens selecionada na fase C1	Foi executado as seguintes tarefas de pré-processamento: Redimensionamento, Normalização, Redução de Ruídos, Conversão para Níveis de Cinza, Dilatação e Erosão, e Limiarização com OTSU
C3	Extração dos Metadados da Imagem	Foi extraído os metadados Básicos e Avançados das imagens pré-processadas na fase C2. O conteúdo extraído foi armazenado em uma BoW
C4	Extração do Conteúdo Textual da Imagem com OCR	Foi extraído o conteúdo textual com OCR das imagens pré-processadas na fase C2. Este conteúdo foi armazenado na mesma BoW gerada na fase C3.
C5	Avaliação da Extração de Metadados e OCR	Foi avaliado o desempenho das extrações realizadas nas fases C3 e C4 com as seguintes métricas: WER, CER e a Taxa de Acerto. Os valores obtidos na Taxa de Acerto estão em um intervalo entre 73%, e 96%, e os valores das taxas CER e WER estão entre 0,1 e 10,0
C6	Estruturação dos Dados Extraídos nas fases C3 e C4 com PLN	Foi realizada a estruturação das extrações realizadas nas fases C3 e C4 com as seguintes tarefas de PLN: Conversão para Minúsculas, Tokenização, Remoção de Valores Duplicados, Ordenação Alfabética Remoção de Valores com 1 Caractere e de Stopwords

Fase	Título	Resultados
C7	Identificação de Palavras-Chave relacionadas com Pornografia Infantojuvenil no conteúdo estruturado na fase C6	Comparou-se o conteúdo textual das 359 palavras-chave relacionadas à Pornografia Infantojuvenil identificadas na Literatura nos estudos realizados por Frank, Westlake e Bouchard (2010) e Wang et al. (2023). Em seguida, desenvolveu-se um código que verifica a existência de cada uma destas 359 palavras-chave no conteúdo estruturado na fase C6

Fonte: o Autor (2024).

Assim, ao desenvolver e aplicar a Estratégia C formada pela Extração de Metadados, OCR, LSTM e Processamento de Linguagem Natural, foi possível detectar conteúdo textual relacionado com pornografia infantojuvenil em imagens.

A seguir são apresentados os resultados da Estratégia D.

4.4. ESTRATÉGIA D

A Estratégia D é intitulada: **Detecção de Objetos Relacionados com Pornografia Infantojuvenil.** Seu objetivo é detectar objetos relacionados com Pornografia Infantojuvenil em imagens. Importante destacar que estes objetos são símbolos usados por criminosos para marcar arquivos de pornografia infantojuvenil ou indicar outro crime que tenha o púbico infantojuvenil como vítima. Na tabela 51, são apresentadas as Bases e Técnicas Computacionais utilizadas no desenvolvimento e aplicação desta estratégia.

Tabela 51 – Bases e Técnicas Computacionais utilizadas na Estratégia D

ID	Estratégia	Bases Utilizadas	Tipo de Base	Técnicas Computacionais
D	Detecção de Objetos relacionados com Pornografia Infantojuvenil	- *FBI Symbols Document* - FBI – SDE - FBI - SDV	Imagens	- Detecção de Objetos - RNC - RAG

Fonte: o Autor (2024).

A Estratégia D é composta por sete fases, são elas:

D1 - Seleção das Bases de Imagens: Foi selecionado uma base de imagens de contendo símbolos relacionados com Pornografia Infantojuvenil. Para isso, foi realizada uma pesquisa na literatura em bases de dados e imagens, além de publicações de autoridades policiais sobre símbolos utilizados em arquivos com Pornografia Infantojuvenil.

Foi identificado e selecionado a publicação ***FBI Symbols Document.*** Trata-se de um Boletim dos Serviços de Inteligência do FBI que apresenta símbolos utilizados por criminosos para marcarem arquivos com pornografia infantojuvenil, com o objetivo de atraírem pessoas interessadas neste tipo de conteúdo (Federal Bureau Of Investigation, 2007). A publicação ***FBI Symbols Document*** possui um total de 13 símbolos relacionados a pornografia infantojuvenil.

Para o desenvolvimento desta Estratégia, dividiu-se estes 13 símbolos da seguinte forma: 3 para treinamento e 10 para validação. Essa divisão é necessária para o uso da técnica de IA nas próximas fases. É ilustrado na figura 41 os 3 símbolos que serão usados para o treinamento da técnica de IA.

Figura 41 – Símbolos utilizados para Treinamento

Fonte: o Autor (2024)

Cada uma das três imagens ilustradas na Figura 41 representará uma classe. A imagem “Org (1)” representa a classe **Menino**, pois trata-se de um símbolo utilizado pelos criminosos para indicar suas preferências por meninos. Já as imagens “Org (2)” e “Org(3)” representam as classes **Menina01** e **Menina02** respectivamente, pois trata-se de símbolos utilizados pelos criminosos para indicar suas preferências por meninas.

D2 - Aplicação do Aumento de Dados com as Redes Adversárias Generativas: Foi aplicado o Aumento de Dados com as Redes Adversárias Generativas (RAGs) nos 3 símbolos selecionados para treinamento na fase D1. O objetivo do Amento de Dados foi produzir novos símbolos, e assim, gerar uma base enriquecida para treinar a técnica de IA que será utilizada nas próximas fases.

Foi definido a aplicação do Aumento de Dados com as RAGs devido aos poucos itens existentes na publicação ***FBI Symbols Document*** para realizar o treinamento da técnica de IA

que será utilizada nas próximas fases. Ao treinar uma técnica de IA com somente 3 imagens, é provável que esta técnica não aprenda o suficiente, e assim, gerar problemas de *Underfitting*.

Para aplicar o Aumento de Dados, utilizou-se as RAGs por meio da biblioteca imgaug. Inicialmente, foi necessário definir quais parâmetros serão usados para gerar os novos símbolos. Os parâmetros definidos foram os seguintes: Zoom, ruídos, recortes e filtros, rotação vertical, horizontal e em 45º graus, alterações de brilho, luminosidade e de Contraste. Em relação aos valores utilizados nos parâmetros, definiu-se todos como aleatório.

Sobre a arquitetura da RAG, utilizou-se os seguintes parâmetros: 500 épocas, taxa de aprendizagem para o Gerador e o Discriminador em 0.0001, funções de ativação ReLU para o Gerador e Discriminador com valores entre -1 e 1 (XIE et al., 2023).

Concluída a definição dos parâmetros, aplicou-se o Aumento de Dados com as RAGs utilizando como entrada os 3 símbolos selecionados que serão usados para o treinamento da técnica de IA nas próximas fases. Esta aplicação gerou 71 novos símbolos.

D3 - Criação da Base de Imagens Enriquecida: Foi criado uma base de imagens enriquecida com os símbolos produzidos pela aplicação do Aumento de Dados realizada com as RAGs na fase D2. O Aumento de Dados gerou 71 novos símbolos, a partir de 3 símbolos fornecidos como entrada.

Foi gerado uma base enriquecida, denominada de **FBI – SDE.** Esta base é formada pelos 3 símbolos selecionados para treinamento na fase D1, juntamente com os 71 símbolos gerados pelo Aumento de Dados na fase D2, totalizando 74 símbolos. A base enriquecida **FBI – SDE** pode ser consultada no apêndice J.

D4 - Criação de uma Base de Imagens com Símbolos Para Validação da Detecção de Objetos: Foi criado uma base de imagens para a validação da Detecção de Objetos. A detecção de objetos será conduzida pela técnica de IA, cuja definição será feita na fase D5. Esta base de validação é denominada **FBI – SDV,** e é formada pelos 10 símbolos definidos na fase D1. Esta base pode ser consultada no Apêndice K.

D5 - Seleção da Técnica de Inteligência Artificial para Detecção de Objetos: Foi selecionado a técnica de IA que será utilizada para detectar objetos. Para isso, buscou-se na literatura por estudos que mencionem a utilização de técnicas de IA para detectar objetos. A técnica de IA selecionada foi a Rede Neural Convolucional (RNCs). Trata-se de um tipo de

RNA de aprendizado profundo comumente utilizada em tarefas com imagens digitais, como no pré-processamento e detecção de objetos (SANGHVI et al., 2021).

D6 - Aplicação das Redes Neurais Convolucionais na Detecção de Objetos: Foi aplicado a técnica da RNC na detecção de objetos. Para isso, foi utilizado as imagens da base **FBI – SDE** como treinamento da RNC, e as imagens da base **FBI – SDV** foram utilizadas para validar o desempenho da RNC.

Sobre o treinamento da RNC, inspirado pelo estudo de Mishra, Gupta e Tanwar (2024), foram utilizadas as ferramentas Darknet, Tensorflow e Yolo para realizar uma "Transferência de Aprendizagem". A Transferência de Aprendizagem é um processo que possibilita utilizar modelos previamente treinados para melhorar o desempenho de uma técnica de IA e reduzir o tempo de treinamento

A Transferência de Aprendizagem foi feita com o arquivo: ***yolov4_custom_last.weights***. Este arquivo contém o treinamento de uma RNC sobre itens fundamentais relacionados com imagens, como traços e cores. As RNCs que incorporam em sua arquitetura pesos já treinados podem ser chamados de Redes Neurais Convolucionais Rápidas (RNC-R) ou F-CNN (*Faster – Convolutional Neural Networks*) (MISHRA; GUPTA; TANWAR, 2024).

Concluída a Transferência de Aprendizagem, realizou-se o processo de "Desenho das Caixas Delimitadoras", ou do inglês, *Bounding Boxes*. As caixas delimitadoras são utilizadas pelas RNC para informar onde estão localizados os objetos a serem detectados em uma imagem, além da classe a qual estes objetos pertencem. Um exemplo de caixa delimitadora é ilustrado na Figura 10 deste trabalho. Assim, foi realizado o desenho da caixa delimitadora ao redor dos objetos das bases **FBI – SDE** e **FBI – SDV.** A ferramenta utilizada para realizar o desenho das caixas delimitadoras foi a LabelMe.

Finalizado o desenho das caixas delimitadoras, foi iniciado o treinamento da RNC com os pesos obtidos pela Transferência de Aprendizagem, e as anotações das caixas delimitadoras nas imagens da base **FBI – SDE.** Neste treinamento, foi configurado um método chamado de Parada Antecipada, do inglês, "*Early Stopping*".

A Parada antecipada é uma técnica utilizada em treinamentos de RNAs para interrompê-lo automaticamente a partir do momento que o desempenho não melhora após um determinado número de épocas (Anda; Le-Khac; Scanlon, 2020). Sobre a taxa de perda de informação

durante o treinamento, o valor foi de 0.001300, considerado excelentes por estarem entre 0.0001 e 0.1 (Al-Nabki et al., 2023). Concluído o treinamento, foi aplicado a RNC nas imagens da base **FBI – SDV.** Na figura 42, é apresentado o resultado da aplicação da RNC.

Figura 42 – Resultado da Aplicação da RNC na detecção de Objetos

SymbolA_01	**SymbolA_02**	**SymbolA_03**
		
SymbolA_04	**SymbolA_05**	**SymbolA_06**
		
SymbolA_07	**SymbolA_08**	**SymbolAB_01**
		
	SymbolB_01	
		

Fonte: o Autor (2024).

Concluída a aplicação da RNC para detectar objetos, calculou-se as seguintes métricas para avaliar seu desempenho na próxima fase – D7: Interseção sobre União (IoU) e a Confiança das Classes existentes nas imagens de treinamento: **menino**, **menina01** e **menina02**.

D7 - Avaliação das Redes Neurais Convolucionais na Detecção de Objetos: Foi avaliado o desempenho da RNCs aplicadas na detecção de objetos na fase D6. Para isso, foram usadas as seguintes métricas: Interseção sobre União (IoU) e a Confiança das Classes existentes nas imagens de treinamento. Na tabela 52, são descritos os resultados obtidos com a aplicação da RNC para a detecção de Objetos.

Tabela 52 – Avaliação dos Resultados Obtidos com a Aplicação da RNC na Detecção de Objetos

ID	Nome da Imagem	Interseção sobre União (IoU)	Confiança da Classe Menino	Confiança da Classe Menina01	Confiança da Classe Menina02
01	SymbolAB_01	0.9782	0,0%	73,0%	1,0%
02	SymbolA_01	0.9428	40,0%	0,0%	1,0%
03	SymbolA_02	0.9571	13,0%	3,0%	8,0%
04	SymbolA_03	0.9427	4,0%	88,0%	0,0%
05	SymbolA_04	0.9714	60,0%	1,0%	0,0%
06	SymbolA_05	0.9685	26,0%	1,0%	8,0%
07	SymbolA_06	0.6524	29'%	2,0%	0,0%
08	SymbolA_07	0.7050	0,0%	0,0%	4,0%
09	SymbolA_08	X	0,0%	0,0%	0,0%
10	SymbolB_01	0.9465	16,0%	18,0%	3,0%

Fonte: o Autor (2024)

Ao analisar a tabela 52, percebe-se que a RNC detectou objetos corretamente em 6 das 10 imagens utilizadas para validação. O que representa um total de 60% de Taxa de Acerto nos experimentos. Nas 4 imagens que a RNC não obteve sucesso na detecção de objetos, 3 foram classificadas incorretamente, e 1 não teve o símbolo detectado.

Em relação a Interseção sobre União (IoU), segundo os autores Nasreen et al. (2023) e Samuelsson (2018), os valores entre 0,9264 e 1,0 são classificados como ótimos, entre 0,7330 e 0,9263 são classificados como bons, entre 0,4034 e 0,7329 são classificados como ruins, e abaixo de 0,4034 são classificados como muito ruins.

Baseando-se na métrica de IoU, 7 imagens podem ser classificadas como ótimas. Já as imagens SymbolA_06 e SymbolA_07 são classificados como ruins e a imagem SymbolA_08 como muito ruim. Ao analisar a Figura 42, percebe-se como as caixas delimitadoras inseridas

pela RNC nas figuras SymbolA_06 e SymbolA_07 não estão corretamente alinhadas, além da imagem SymbolA_08 não possui uma caixa delimitadora.

Resumidamente, na imagem SymbolA_08 não foi detectado nenhum símbolo, quando na verdade, há um símbolo da classe menino. Nas imagens SymbolA_03 e SymbolA_07, os símbolos detectados foram classificados como menina01 e menina02 respectivamente, quando na verdade ambos pertencem a classe Menino. Por fim, a imagem SymbolAB_01 possui os símbolos de duas classes: menino e menina01, mas a RNC detectou apenas o símbolo da classe menina01. A tabela 53 descreve a classificação de objetos realizada pela RNC

Tabela 53 – Classificação de Objetos realizada pela RNC

ID	Nome da Imagem	Classe Correta	Classe Informada pela RNC	Classificação foi correta?
01	SymbolAB_01	Menino e Menina01	Menina01	Incorreta
02	SymbolA_01	Menino	Menino	Correta
03	SymbolA_02	Menino	Menino	Correta
04	SymbolA_03	Menino	Menina01	Incorreta
05	SymbolA_04	Menino	Menino	Correta
06	SymbolA_05	Menino	Menino	Correta
07	SymbolA_06	Menino	Menino	Correta
08	SymbolA_07	Menino	Menina02	Incorreta
09	SymbolA_08	Menino	X	Incorreta
10	SymbolB_01	Menina01	Menina01	Correta

Fonte: o Autor (2024)

Analisando a figura 42, entende-se por que a RNC não conseguir detectar corretamente os símbolos em 4 imagens. Na imagem SymbolA_08, o símbolo é consideravelmente diferente dos utilizados no treinamento por possuir um formato com curvas. Na imagem SymbolA_07, existe um texto sobreposto ao símbolo, como uma marca d'água. Na imagem SymbolA_03, sua resolução é baixa e o símbolo possui diversos pontos em branco em suas extremidades. E a imagem SymbolAB_01 possui somente parte dos símbolos.

Os resultados foram comparados com os estudos de Chau et al. (2023), que utilizaram o valor de IoU para gerar novas métricas capazes de determinar se os objetos foram detectados corretamente. Foi obtida uma taxa de acerto de 60% dos objetos classificados corretamente, tanto com a IoU, quanto na identificação correta da classe. Entende-se assim que os resultados

obtidos com o desenvolvimento e aplicação desta Estratégia são considerados bons, baseando-se no estudo de Chau et al. (2023), que também obtiveram uma taxa de acerto de 60%.

Portanto, entende-se que os resultados alcançados com a aplicação do Aumento de Dados com as RAGs em uma base de imagens podem ser utilizados para treinar uma RNC. Ao utilizar a Transferência de Aprendizagem, o Desenho de Caixas Delimitadoras e a Parada Antecipada no treinamento da RNC, para posteriormente, aplicá-la na detecção de objetos, pode ser usado para detectar símbolos relacionados com Pornografia Infantojuvenil.

Na tabela 54 é apresentado um resumo das execuções e dos resultados obtidos nas fases da Estratégia D.

Tabela 54 – Resumo das Atividades realizadas na Estratégia D

Fase	Título	Resultados
D1	Seleção das Bases de Imagens	Foi selecionada a base ***FBI Symbols Document***
D2	Aplicação do Aumento de Dados com as Redes Adversárias Generativas	Foi aplicado o Aumento de Dados com as RAGs. Foi gerado um total de 71 novos símbolos.
D3	Criação da Base de Imagens Enriquecida	Foi criada uma base de imagens enriquecida denominada de **FBI – SDE,** com os 71 símbolos gerados pelo Aumento de Dados na fase D2, mais os 3 símbolos fornecidos como entrada para o Aumento de Dados, totalizando 74 símbolos.
D4	Criação de uma Base de Imagens com Símbolos Para Validação da Detecção de Objetos	Foi gerada uma base formada por 10 símbolos para validar a detecção de objetos. A base foi denominada de **FBI – SDV**
D5	Seleção da Técnica de Inteligência Artificial para Detecção de Objetos	A técnica de IA selecionada foi a Rede Neural Convolucional (RNC)
D6	Aplicação das Redes Neurais Convolucionais na Detecção de Objetos	No treinamento da RNC, foram realizadas as seguintes tarefas: Transferência de Aprendizagem, Desenho de Caixas Delimitadoras e a Parada Antecipada. O treinamento foi realizado com a base **FBI – SDE.** A aplicação da RNC para detectar objetos foi realizada com a base **FBI – SDV**.
D7	Avaliação das Redes Neurais Convolucionais na Detecção de Objetos	Foram utilizadas as seguintes métricas para avaliar a aplicação das RNCs na detecção de Objetos: Interseção sobre União (IoU) e a Confiança das Classes. A RNC foi capaz de detectar corretamente 6 das 10 imagens da base **FBI – SDV** gerada para validação. Sobre a IoU, 7 imagens foram classificadas como ótimas, enquanto as outras três foram classificadas como ruins. Quanto a confiança das classes, em 6 das 10 imagens foi detectado os objetos e suas classes corretamente.

Fonte: o Autor (2024).

5. CONCLUSÃO

Durante o desenvolvimento desse trabalho, verificou-se a importância do combate a pornografia infantojuvenil e suas possíveis formas de realizá-la, e que detectar evidências deste crime cibernético é fundamental para garantir sua identificação, realizar sua remoção e assim, impedir possíveis propagações deste conteúdo em redes como a internet.

Os impactos gerados pela propagação de pornografia infantojuvenil não estão limitadas às vítimas e podem se estender às suas famílias e a sociedade em geral, reforçando a necessidade de combater esse tipo de crime cibernético.

Sobre a atuação das autoridades policiais na detecção de pornografia infantojuvenil, a escassez de recursos, incluindo de financiamento e mão-de-obra, dificultam os esforços de investigação. Portanto, é fundamental desenvolver formas de apoiar o trabalho realizado pelas autoridades policiais.

No que se refere a detecção de evidências de Pornografia Infantojuvenil, é uma atividade realizada por autoridades policiais em um exame pericial. O principal desafio enfrentado neste contexto reside na detecção manual de evidências. Uma busca manual pode-se tornar uma tarefa exaustiva e complexa devido à quantidade e diversidade de arquivos presentes nos dispositivos a serem periciados.

Visando a necessidade de se desenvolver formas para detectar evidências de Pornografia Infantojuvenil, e compreendendo o empenho da comunidade acadêmica e das forças policiais dentro deste contexto, desenvolveu-se neste trabalho Fenrir, um conjunto de quatro Estratégias formadas por técnicas computacionais integradas das áreas da Computação Forense, IA e VC aplicadas na detecção de evidências de Pornografia Infantojuvenil com o objetivo de apoiar a execução de exames periciais.

Com base nesse cenário, este trabalho teve como objetivo geral desenvolver e aplicar Estratégias formadas por técnicas computacionais integradas das áreas da Computação Forense, Inteligência Artificial e Visão Computacional aplicadas na detecção de evidências pornografia infantojuvenil em imagens digitais, para apoiar a execução de exames periciais.

As quatro Estratégias aplicadas na detecção de evidências de Pornografia Infantojuvenil em imagens tiveram os seguintes objetivos: Na Estratégia A, o objetivo foi detectar e recuperar valores Hash perceptivos de imagens alteradas ou semelhantes. Na Estratégia B, o objetivo foi

detectar pessoas. Na Estratégia C, o objetivo foi detectar conteúdo textual relacionado com Pornografia Infantojuvenil. Na Estratégia D, o objetivo foi detectar objetos relacionados com Pornografia Infantojuvenil. As Estratégias A, C e D foram compostas por 7 fases, enquanto a Estratégia B foi composta por 9 fases.

Ressalta-se que as quatro Estratégias desenvolvidas que compõe Fenrir são diferentes das Estratégias encontradas na literatura para detectar evidências de pornografia infantojuvenil, conforme a RSL sobre pornografia infantojuvenil disponível na seção 2.6 deste trabalho

A Estratégia A foi formada pelo *Differential Hash* e a RNH. Sua aplicação possibilita a detecção de imagens semelhantes as já detectadas como pornografia infantojuvenil. A Estratégia B foi formada pela detecção de cor de pele, Floresta Aleatória e uma base de cores de pele em RGB enriquecida com os espaços de cores HSV e YCbCr. Sua aplicação possibilita a detecção de pessoas em imagens.

A Estratégia C foi formada pela Extração de Metadados, OCR, LSTM e o PLN. Sua aplicação possibilita a detecção de conteúdo textual relacionado com pornografia infantojuvenil em imagens. A Estratégia D foi formada pela detecção de objetos, RAGs e RNCs. Sua aplicação possibilita a detecção de objetos relacionados com pornografia infantojuvenil em imagens

As quatro Estratégias tiveram seus resultados avaliados com métricas já consolidadas na literatura, juntamente com a comparação com trabalhos próximos. Em todas as Estratégias, entendeu-se que os resultados obtidos foram considerados interessantes e promissores.

A utilização das Estratégias diminui o tempo consideravelmente para detectar evidências de pornografia infantojuvenil. Isso porque reduz o universo de imagens que serão analisadas, para somente: as imagens com valores Hash Perceptivos similares a arquivos que já foram detectados como pornografia infantojuvenil, ou que possuam cor de pele em seus pixels, ou que possuam conteúdo textual relacionados com Pornografia Infantojuvenil ou que possuam objetos relacionados com Pornografia Infantojuvenil

Conclui-se então que as estratégias que formam Fenrir desenvolvidas nesse trabalho obtiveram resultados promissores, quando aplicadas na detecção de evidências de pornografia infantojuvenil. Com isso, considera-se que o objetivo deste estudo foi atingido, e a questão de pesquisa, respondida.

Em relação as contribuições deste trabalho, são elas:

- Para a pesquisa acadêmica:
  - O desenvolvimento e aplicação de Fenrir na detecção de evidências de pornografia infantojuvenil para apoiar a execução de exames periciais.
  - A composição das Fases das estratégias. Há fases com avaliações de técnicas, busca por bases, enriquecimentos e outras tarefas que possibilitarão o desenvolvimento de novos estudos, seja com novas técnicas, bases, ou até propondo novas formas de enriquecimento e avaliação das fases.
  - O desenvolvimento da RSL apresentada na seção 2.6 deste trabalho, onde foram selecionadas 129 publicações sobre Pornografia Infantojuvenil que poderá servir de base o desenvolvimento de novos estudos.

- Para a sociedade e o cidadão:
  - Fenrir poderá promover um ambiente digital mais seguro e saudável ao detectar, para que posteriormente, seja retirado da internet e de outras redes de propagação, arquivos com pornografia infantojuvenil.
  - Fenrir poderá promover a responsabilidade digital entre os usuários na internet, ao detectar evidências de pornografia infantojuvenil, e assim, conscientizar as pessoas sobre os riscos ao acessar conteúdos ilícitos na internet.
  - Fenrir poderá fomentar uma cultura de vigilância no ambiente digital ao detectar evidências de pornografia infantojuvenil.

Vale destacar as limitações observadas no desenvolvimento deste trabalho, como a utilização de arquivos sintéticos para o desenvolvimento e aplicação de Fenrir. Recomenda-se que forças policiais que tenham em posse a materialidade do crime cibernético de pornografia infantojuvenil, utilizasse este conteúdo com Fenrir e avaliasse seu desempenho.

Como continuidade da pesquisa, considera-se os seguintes pontos:

- Desenvolver novas Estratégias aplicadas na detecção de Pornografia Infantojuvenil em outros tipos de arquivos multimídia, como Áudios e Vídeos, e posteriormente, adicioná-las a Fenrir;
- Aprimorar as Estratégias existentes na literatura aplicadas na detecção de Pornografia Infantojuvenil incluindo novas técnicas, ferramentas, bases de dados e imagens, além de novas formas de enriquecimentos das bases;

- Adicionar novos elementos, como distorção, texturas, objetos parciais e com diferentes tipos de iluminação, em tarefas de Aumento de Dados com as Redes Adversárias Generativas.
- A aplicação de *Embedding* nas Estratégias que formam Fenrir. Esta aplicação significa gerar uma métrica única que represente as saídas de todas as Estratégias.
- O uso de Inteligência de Fontes Abertas, uma atividade realizada para buscar informações em fontes disponíveis publicamente, como a internet, em conjunto com as Estratégias aplicadas na detecção de evidências de pornografia infantojuvenil. Isso garante que a aplicação das Estratégias se estenda à fontes abertas, como a internet.

Os estudos apresentados neste trabalho não tiveram a pretensão de saturar o assunto. Contrário a isso, buscou-se trazer contribuições com o desenvolvimento e aplicação de Fenrir na detecção de evidências de pornografia infantojuvenil para apoiar a execução de exames periciais.

REFERÊNCIAS

ABNT. **ABNT NBR ISO/IEC 27037:2013**. São Paulo., 2013. Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=307273&_ga=2.245746820.124810196.1702076603-620541868.1702076602>

AKHTAR, Z. et al. Optical character recognition (OCR) using partial least square (PLS) based feature reduction: an application to artificial intelligence for biometric identification. **Journal of Enterprise Information Management**, v. 36, n. 3, p. 767–789, 24 abr. 2023.

ALEMANNO, F. et al. Hopfield model with planted patterns: A teacher-student self-supervised learning model. **Applied Mathematics and Computation**, v. 458, 1 dez. 2023.

ALGHYALINE, S. Arabic Optical Character Recognition: A Review. **CMES - Computer Modeling in Engineering and Sciences**, v. 135, n. 3, p. 1825–1861, 23 nov. 2023.

AL-KHATER, W. A. et al. Comprehensive review of cybercrime detection techniques. **IEEE Access**, v. 8, p. 137293–137311, 2020.

ALKHOWAITER, M.; ALMUBARAK, K.; ZOU, C. Evaluating Perceptual Hashing Algorithms in Detecting Image Manipulation Over Social Media Platforms. **Proceedings of the 2022 IEEE International Conference on Cyber Security and Resilience, CSR 2022**, p. 149–156, 2022.

ALMEIDA, J. R. DE. **Transfer learning e convolutional neural networks para a classificação de imagens e reconhecimento de objetos no âmbito da perícia criminal**. Brasília, 2020. Disponível em: <https://repositorio.unb.br/handle/10482/40286>

AL-NABKI, M. W. et al. Evaluating Performance of an Adult Pornography Classifier for Child Sexual Abuse Detection. **Computer Vision and Pattern Recognition**, v. 1, n. 1, p. 1–4, 2020.

AL-NABKI, M. W. et al. Short text classification approach to identify child sexual exploitation material. **Scientific Reports 2023 13:1**, v. 13, n. 1, p. 1–9, 26 set. 2023.

AL-THANI, N. F. et al. **Framework Design for Similar Video Detection: A Graph Based Video Clustering Approach**. 2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). **Anais**...Ankara: Institute of Electrical and Electronics Engineers (IEEE), 14 nov. 2022. . Acesso em: 2 dez. 2022

ALZUBAIDI, L. et al. Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. **Journal of Big Data**, v. 8, n. 1, p. 1–74, 31 mar. 2021.

ANDA, F.; LE-KHAC, N. A.; SCANLON, M. DeepUAge: Improving Underage Age Estimation Accuracy to Aid CSEM Investigation. **Forensic Science International: Digital Investigation**, v. 32, p. 300921, 1 abr. 2020.

ANEJA, S.; CHANG, E.; OMURO, A. Applications of artificial intelligence in neuro-oncology. **Current Opinion in Neurology**, v. 32, n. 6, p. 850–856, maio 2019.

ANTIPOVA, E. S.; RASHKOVSKIY, S. A. Autoassociative hamming neural network. **Russian Journal of Nonlinear Dynamics**, v. 17, n. 2, p. 175–193, 2021.

APPATI, J. K.; LODONU, K. Y.; CHRIS-KOKA, R. A review of image analysis techniques for adult content detection: Child protection. **International Journal of Software Innovation**, v. 9, n. 2, p. 102–121, 1 jan. 2021.

APRUZZESE, G. et al. The Role of Machine Learning in Cybersecurity. **Digital Threats: Research and Practice**, v. 4, n. 1, 7 mar. 2023.

ARABAMERI, A. et al. Decision tree based ensemble machine learning approaches for landslide susceptibility mapping. **Geocarto International**, v. 37, n. 16, p. 4594–4627, 2022.

AVYODRI, R.; LUKAS, S.; TJAHYADI, H. Optical Character Recognition (OCR) for Text Recognition and its Post-Processing Method: A Literature Review. **Proceedings - 2022 1st International Conference on Technology Innovation and Its Applications, ICTIIA 2022**, p. 1–6, 2022.

BAO, W.; LIANJU, N.; YUE, K. Integration of unsupervised and supervised machine learning algorithms for credit risk assessment. **Expert Systems with Applications**, v. 128, p. 301–315, 15 ago. 2019.

BERENGUER, C. V. et al. Underlying Features of Prostate Cancer—Statistics, Risk Factors, and Emerging Methods for Its Diagnosis. **Current Oncology**, v. 30, n. 2, p. 2300–2321, 15 fev. 2023.

BHATT, R.; DHALL, A. **Skin Segmentation. UCI Machine Learning Repository**. UCI Machine Learning Repository, , 2012. Disponível em: <https://doi.org/10.24432/C5T30C>

BILLA, N. R. et al. CNN based image resizing forensics for double compressed JPEG images. **Journal of Information Security and Applications**, v. 81, p. 103693, 1 mar. 2024.

BISWAS, R. et al. A new perceptual hashing method for verification and identity classification of occluded faces. **Image and Vision Computing**, v. 113, p. 104245, 1 set. 2021.

BLANCHY, G. et al. Potential of natural language processing for metadata extraction from environmental scientific publications. **Soil**, v. 9, n. 1, p. 155–168, 14 mar. 2023.

BOUKHERS, Z.; BOUABDALLAH, A. Vision and natural language for metadata extraction from scientific PDF documents: A multimodal approach. **Proceedings of the ACM/IEEE Joint Conference on Digital Libraries**, n. 6, p. 1–5, 20 jun. 2022.

BRASIL. **Lei Nº 3.689, De 3 De Outubro De 1941**. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 2 dez. 2022.

BRASIL. **Lei Nº 11.829, De 25 De Novembro De 2008.** Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11829.htm#art1>. Acesso em: 2 dez. 2022.

BRASIL. **Lei Nº 12.737, de 30 de Novembro de 2012.** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 17 jun. 2023.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Disponível em: <https://legis.senado.leg.br/norma/31865675/publicacao/31866001>. Acesso em: 2 dez. 2022.

BREIDENBACH, U.; STEINEBACH, M.; LIU, H. Privacy-enhanced robust image hashing with bloom filters. **ACM International Conference Proceeding Series**, 25 ago. 2020.

BREIMAN, L. Random forests. **Machine Learning**, v. 45, n. 1, p. 5–32, 2001.

BURSZTEIN, E. et al. Rethinking the detection of child sexual abuse imagery on the internet. **The Web Conference 2019 - Proceedings of the World Wide Web Conference, WWW 2019**, p. 2601–2607, 2019.

CASTRO, J. V. DE; BULAWSKI, C. M. O Perfil do Pedófilo: Uma Abordagem da Realidade Brasileira. **Liberdades**, v. 1, n. 6, p. 3–26, jan. 2011.

ÇAVUŞOĞLU, Ü. S-Box-based video stenography application of variable-order fractional hopfield neural network (VFHNN). **European Physical Journal: Special Topics**, v. 231, n. 10, p. 2017–2035, 28 jan. 2022.

CENTORRINO, V.; BULLO, F.; RUSSO, G. Contraction Analysis of Hopfield Neural Networks with Hebbian Learning. **Proceedings of the IEEE Conference on Decision and Control**, v. 2022- Decem, p. 622–627, 2022.

CHANDRA, A.; SNOWE, M. J. A taxonomy of cybercrime: Theory and design. **International Journal of Accounting Information Systems**, v. 38, p. 100467, 1 set. 2020.

CHAU, R. C. W. et al. Accuracy of artificial intelligence-designed single-molar dental prostheses: A feasibility study. **Journal of Prosthetic Dentistry**, 9 jan. 2023.

CHAVAN, P.; JADHAV, D.; BORKAR, G. M. Challenges to Multimedia Privacy and Security Over Social Media. Em: Foggia: IGI Global, 2020. p. 118–131.

CHEN, C. et al. ReLU-type Hopfield neural network with analog hardware implementation. **Chaos, Solitons and Fractals**, v. 167, p. 113068, 1 fev. 2023.

CHEN, G. et al. **Discussion on the Talents Cultivation of Digital Forensics**. 2020 International Conference on Educational Training and Educational Phenomena (ICETEP2020). **Anais**...Scholar Publishing Group Ltd, 2020.

CHEN, L.; XIANG, F.; SUN, Z. Image deduplication based on hashing and clustering in cloud storage. **KSII Transactions on Internet and Information Systems**, v. 15, n. 4, p. 1448–1463, 1 abr. 2021.

CIFUENTES, J.; SANDOVAL OROZCO, A. L.; GARCÍA VILLALBA, L. J. A survey of artificial intelligence strategies for automatic detection of sexually explicit videos. **Multimedia Tools and Applications**, v. 81, n. 3, p. 3205–3222, 1 jan. 2022.

COSTA, F. R.; NETO, L. H.; JESUS, T. F. X. DE. **Manual de Requisições da Perícia Oficial**. 1. ed. Aracaju: Pericia Oficial Criminal do Estado de Sergipe, 2018. v. 1

COSTA, V. G.; PEDREIRA, C. E. Recent advances in decision trees: an updated survey. **Artificial Intelligence Review**, v. 56, n. 5, p. 4765–4800, 10 out. 2023.

COSTANTINI, S.; DE GASPERIS, G.; OLIVIERI, R. Digital forensics and investigations meet artificial intelligence. **Annals of Mathematics and Artificial Intelligence**, v. 86, n. 1–3, p. 193–229, 24 abr. 2019.

CZAJKOWSKI, M.; KRETOWSKI, M. Decision tree underfitting in mining of gene expression data. An evolutionary multi-test tree approach. **Expert Systems with Applications**, v. 137, p. 392–404, 15 dez. 2019.

DALIANIS, H. Evaluation Metrics and Evaluation. **Clinical Text Mining**, p. 45–53, 2018.

DE MARZO, G.; IANNELLI, G. Effect of spatial correlations on Hopfield Neural Network and Dense Associative Memories. **Physica A: Statistical Mechanics and its Applications**, v. 612, p. 128487, 15 fev. 2023.

DEORA, R. S.; CHUDASAMA, D. M. Brief Study of Cybercrime on an Internet. **Journal of Communication Engineering & Systems**, v. 11, n. 1, p. 1–6, 2021.

DETSIKAS, N.; MITIANOUDIS, N.; PAPAMARKOS, N. A Dilated MultiRes Visual Attention U-Net for historical document image binarization. **Signal Processing: Image Communication**, v. 122, p. 117102, 1 mar. 2024.

DHIVYAA, C. R. et al. Skin lesion classification using decision trees and random forest algorithms. **Journal of Ambient Intelligence and Humanized Computing**, 2020.

DÍAZ-PÉREZ, L. C. et al. A review of cross-border cooperation regulation for digital forensics in LATAM from the soft systems methodology. **Applied Computing and Informatics**, v. ahead-of-p, n. ahead-of-print, 2022.

DING, S.; LIU, Z.; LEI, Z. A color attention mechanism based on YES color space for skin segmentation. **Journal of Real-Time Image Processing**, v. 20, n. 3, p. 1–12, 1 jun. 2023.

DIWAN, T.; ANIRUDH, G.; TEMBHURNE, J. V. Object detection using YOLO: challenges, architectural successors, datasets and applications. **Multimedia Tools and Applications**, v. 82, n. 6, p. 9243–9275, 1 mar. 2023.

DONALDS, C.; OSEI-BRYSON, K. M. Toward a cybercrime classification ontology: A knowledge-based approach. **Computers in Human Behavior**, v. 92, p. 403–418, 1 mar. 2019.

DU, L.; HO, A. T. S.; CONG, R. Perceptual hashing for image authentication: A survey. **Signal Processing: Image Communication**, v. 81, p. 115713, 1 fev. 2020.

DU, X.; SCANLON, M. Methodology for the automated metadata-based classification of incriminating digital forensic artefacts. **ACM International Conference Proceeding Series**, p. 1–8, 26 ago. 2019.

DUNSIN, D. et al. A Comprehensive Analysis of the Role of Artificial Intelligence and Machine Learning in Modern Digital Forensics and Incident Response Article info. **Forensic Science International: Digital Investigation**, 2023.

ELEUTÉRIO, P. M. DA S.; MACHADO, M. P. **Desvendando a Computação Forense**. 1. ed. São Paulo: Novatec Editora, 2019. v. 1

ELGOHARY, H. M.; DARWISH, S. M.; ELKAFFAS, S. M. Improving Uncertainty in Chain of Custody for Image Forensics Investigation Applications. **IEEE Access**, v. 10, p. 14669–14679, 2022.

FAN, Y. et al. Digital image colorimetry on smartphone for chemical analysis: A review. **Measurement: Journal of the International Measurement Confederation**, v. 171, p. 108829, 1 fev. 2021.

FARID, H. An Overview of Perceptual Hashing. **Journal of Online Trust and Safety**, v. 1, n. 1, 28 out. 2021.

FEDERAL BUREAU OF INVESTIGATION. **FBI Symbols Document**. , 2007.

FLORENCIO, P. F. DE S. **Delegacia Eletrônica: uma inovação da polícia civil do estado de São Paulo**. [s.l.] UFSCar - Universidade de São Carlos, 2018.

FRANK, R.; WESTLAKE, B.; BOUCHARD, M. The structure and content of online child exploitation networks. **Proceedings of the ACM SIGKDD Workshop on Intelligence and Security Informatics 2010, ISI-KDD 2010**, 2010.

GANESAN, P. et al. HSV Model based Skin Color Segmentation using Uncomplicated Threshold and Logical AND Operation. **2023 9th International Conference on Advanced Computing and Communication Systems, ICACCS 2023**, p. 415–419, 2023.

GANGWAR, A. et al. Pornography and child sexual abuse detection in image and video: A comparative evaluation. **IET Seminar Digest**, v. 2017, n. 5, p. 37–42, 2017.

GANGWAR, A. et al. AttM-CNN: Attention and metric learning based CNN for pornography, age and Child Sexual Abuse (CSA) Detection in images. **Neurocomputing**, v. 445, p. 81–104, 20 jul. 2021.

GHORPADE, M. S.; BHAD, S. A.; KHAIRNAR, Y. S. Artificial Neural Network Using Machine Learning. **International Research Journal of Modernization in Engineering Technology and Science**, v. 5, n. 1, p. 816–821, 18 jan. 2023.

GONZALEZ, R. C.; WOODS, R. E. **Processamento Digital de Imagens**. 3. ed. [s.l.] Editora Blucher, 2009.

GOODFELLOW, I. et al. Generative adversarial networks. **Communications of the ACM**, v. 63, n. 11, p. 139–144, 10 jun. 2020.

GOODFELLOW, I. J. et al. Generative adversarial nets. **Advances in Neural Information Processing Systems**, v. 3, n. January, p. 2672–2680, 2014.

GRIGALIUNAS, S.; BRUZGIENE, R.; VENCKAUSKAS, A. Ontology-Driven Digital Profiling for Identification and Linking Evidence Across Social Media Platform. **IEEE Access**, v. 11, p. 2169–3536, 2023.

GUERRA, E.; WESTLAKE, B. G. Detecting child sexual abuse images: Traits of child sexual exploitation hosting and displaying websites. **Child Abuse and Neglect**, v. 122, p. 105336, 1 dez. 2021.

GUOJIA HOU et al. **SUID: Synthetic Underwater Image Dataset | IEEE DataPort**. Disponível em: <https://ieee-dataport.org/open-access/suid-synthetic-underwater-image-dataset>. Acesso em: 31 dez. 2023.

GUPTA, S.; KUMAR, M. Forensic document examination system using boosting and bagging methodologies. **Soft Computing**, v. 24, n. 7, p. 5409–5426, 1 abr. 2020.

HAMADOUCHE, M. et al. A comparative study of perceptual hashing algorithms: Application on fingerprint images. **CEUR Workshop Proceedings**, v. 2904, p. 217–228, 2021.

HAYES, D.; KYOBE, M. The Adoption of Automation in Cyber Forensics. **2020 Conference on Information Communications Technology and Society, ICTAS 2020 - Proceedings**, 1 mar. 2020.

HAYKIN, S. S. **Redes Neurais**. 2. ed. [s.l.] Bookman Companhia Ed, 2001.

HIEBL, M. R. W. Sample Selection in Systematic Literature Reviews of Management Research. **Organizational Research Methods**, v. 26, n. 2, p. 229–261, 1 abr. 2023.

HO, H.; KO, R.; MAZEROLLE, L. Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review. **Computers and Security**, v. 115, p. 102611, 1 abr. 2022.

HOCHREITER, S.; SCHMIDHUBER, J. Long Short-Term Memory. **Neural Computation**, v. 9, n. 8, p. 1735–1780, 15 nov. 1997.

HOLT, T. J. et al. Assessing the challenges affecting the investigative methods to combat online child exploitation material offenses. **Aggression and Violent Behavior**, v. 55, p. 101464, 1 nov. 2020.

HOPFIELD, J. J. Neural networks and physical systems with emergent collective computational abilities. **Proceedings of the National Academy of Sciences of the United States of America**, v. 79, n. 8, p. 2554–2558, 1 abr. 1982.

HUSSAIN, C. M. et al. **Handbook of Analytical Techniques for Forensic Samples: Current and Emerging ... - Chaudhery Hussain, Deepak Rawtani, Gaurav Pandey, Maithri Tharmavaram - Google Livros**. 1. ed. Cambridge: Elsevier, 2020. v. 1

IDREES, S.; HASSANI, H. Exploiting script similarities to compensate for the large amount of data in training tesseract lstm: Towards kurdish ocr. **Applied Sciences (Switzerland)**, v. 11, n. 20, p. 9752, 19 out. 2021.

JAIN, H. et al. Weapon Detection using Artificial Intelligence and Deep Learning for Security Applications. **Proceedings of the International Conference on Electronics and Sustainable Communication Systems, ICESC 2020**, p. 193–198, 1 jul. 2020.

JAIN, S. et al. Deep perceptual hashing algorithms with hidden dual purpose: When client-side scanning does facial recognition. **Proceedings - IEEE Symposium on Security and Privacy**, v. 2023- May, p. 234–252, 2023.

JAUME, G.; KEMAL EKENEL, H.; THIRAN, J.-P. FUNSD: A Dataset for Form Understanding in Noisy Scanned Documents. p. 1–6, 27 maio 2019.

JAVED, A. R. et al. A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions. **IEEE Access**, v. 10, p. 11065–11089, 2022.

JURINIC, J.; RAMLJAK, T. Sexual Exploitation or Child Pornography: Terminological Analysis in Criminal Codes of Southeast European Countries. **2021 44th International**

Convention on Information, Communication and Electronic Technology, MIPRO 2021 - Proceedings, p. 1502–1510, 2021.

KAYODE-AJALA, O. Applying Machine Learning Algorithms for Detecting Phishing Websites: Applications of SVM, KNN, Decision Trees, and Random Forests. **International Journal of Information and Cybersecurity**, v. 6, n. 1, p. 43–61, 8 mar. 2022.

KEBANDE, V. R. et al. Mapping digital forensic application requirement specification to an international standard. **Forensic Science International: Reports**, v. 2, p. 100137, 1 dez. 2020.

KHAIRUNNISAK, K.; WIDODO, W. Digital Forensic Tools And Techniques For Handling Digital Evidence. **Jurnal RESISTOR (Rekayasa Sistem Komputer)**, v. 6, n. 1, p. 1–11, 30 abr. 2023.

KHAN, S.; NAZIR, S.; KHAN, H. U. Analysis of Cursive Text Recognition Systems: A Systematic Literature Review. **ACM Transactions on Asian and Low-Resource Language Information Processing**, v. 22, n. 7, p. 1–30, 20 jul. 2023.

KINRA, A.; WALIA, W.; SHARANYA, S. A Comprehensive and Systematic Review of Deep Learning Based Object Recognition Techniques for the Visually Impaired. **ICCSC 2023 - Proceedings of the 2nd International Conference on Computational Systems and Communication**, 2023.

KLOESS, J. A.; WOODHAMS, J.; HAMILTON-GIACHRITSIS, C. E. The challenges of identifying and classifying child sexual exploitation material: Moving towards a more ecologically valid pilot study with digital forensics analysts. **Child Abuse and Neglect**, v. 118, p. 105166, 2021.

KOOSHA, S.; MAHYAR, A. **Machine Learning and Deep Learning: A Review of Methods and Applications**. **World Information Technology and Engineering Journal,-**, 2023. Disponível em: <https://papers.ssrn.com/abstract=4458723>. Acesso em: 2 dez. 2023

KOREN IVANČEVIĆ, T. et al. Manipulating Pixels in Computer Graphics by Converting Raster Elements to Vector Shapes as a Function of Hue. **Journal of Imaging**, v. 9, n. 6, p. 106, 1 jun. 2023.

KRUNDYSHEV, V.; KALININ, M. Generative Adversarial Network for Detecting Cyber Threats in Industrial Systems. **Smart Innovation, Systems and Technologies**, v. 220, p. 1–13, 2021.

KUMAR, R. **Research methodology: A step-by-step guide for beginners**. 4. ed. New Delhi: Sage, 2018.

KUNDAIKAR, T.; PAWAR, J. D. Multi-font devanagari text recognition using lstm neural networks. **Advances in Intelligent Systems and Computing**, v. 1045, p. 495–506, 2020.

LAPARRA, E. et al. Addressing structural hurdles for metadata extraction from environmental impact statements. **Journal of the Association for Information Science and Technology**, v. 74, n. 9, p. 1124–1139, 1 set. 2023.

LARANJEIRA DA SILVA, C. et al. Seeing without Looking: Analysis Pipeline for Child Sexual Abuse Datasets. **ACM International Conference Proceeding Series**, p. 2189–2205, 2022.

LE, W. T. et al. Overview of Machine Learning: Part 2: Deep Learning for Medical Image Analysis. **Neuroimaging Clinics of North America**, v. 30, n. 4, p. 417–431, 1 nov. 2020.

LECUN, Y. et al. Gradient-based learning applied to document recognition. **Proceedings of the IEEE**, v. 86, n. 11, p. 2278–2323, 1998.

LEE, H. E. et al. Detecting child sexual abuse material: A comprehensive survey. **Forensic Science International: Digital Investigation**, v. 34, p. 301022, 1 set. 2020.

LEE, S.-H.; KANG, I.; KIM, H.-W. Understanding cybercrime from a criminal's perspective: Why and how suspects commit cybercrimes? **Technology in Society**, v. 75, p. 102361, 1 nov. 2023.

LI, Y.; GUAN, Z.; XU, C. Digital Image Self Restoration Based on Information Hiding. **Chinese Control Conference, CCC**, v. 2018- July, p. 4368–4372, 5 out. 2018.

LIN, X. et al. Recent Advances in Passive Digital Image Security Forensics: A Brief Review. **Engineering**, v. 4, n. 1, p. 29–39, 1 fev. 2018.

LUO, B.; WANG, X.; ZHANG, Z. Application of Computer Vision Technology in UAV. **Journal of Physics: Conference Series**, v. 1881, n. 4, p. 042052, 2021.

LY, B. C. K. et al. Research Techniques Made Simple: Cutaneous Colorimetry: A Reliable Technique for Objective Skin Color Measurement. **Journal of Investigative Dermatology**, v. 140, n. 1, p. 3- 12.e1, 1 jan. 2020.

MACEDO, J.; COSTA, F.; DOS SANTOS, J. A. A Benchmark Methodology for Child Pornography Detection. **Proceedings - 31st Conference on Graphics, Patterns and Images, SIBGRAPI 2018**, p. 455–462, 2 jul. 2018.

MANI, R. G. et al. A Survey on Digital Image Forensics: Metadata and Image forgeries. **CEUR Workshop Proceedings**, v. 3142, p. 22–55, 2022.

MATSUZAKA, Y.; YASHIRO, R. AI-Based Computer Vision Techniques and Expert Systems. **Ai**, v. 4, n. 1, p. 289–302, 23 fev. 2023.

MAYER, F.; STEINEBACH, M. Forensic image inspection assisted by deep learning. **ACM International Conference Proceeding Series**, v. Part F1305, 29 ago. 2017.

MCCLUSKEY, Q. R. et al. Computer Forensics: Complementing Cyber Security. **IEEE International Conference on Electro Information Technology**, v. 2022- May, p. 507–512, 2022.

MCCORMACK, L.; LOWE, B. Making meaning of irreconcilable destruction of innocence: National humanitarian professionals exposed to cybercrime child sexual exploitation in the Philippines. **Child Abuse and Neglect**, v. 131, p. 105770, 1 set. 2022.

MCCULLOCH, W. S.; PITTS, W. A logical calculus of the ideas immanent in nervous activity. **The Bulletin of Mathematical Biophysics**, v. 5, n. 4, p. 115–133, dez. 1943.

MCKINNEL, D. R. et al. A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability assessment. **Computers and Electrical Engineering**, v. 75, p. 175–188, 1 maio 2019.

MEENALOCHINI, M. et al. Perceptual Hashing for Content Based image Retrieval. **Proceedings of the 3rd International Conference on Communication and Electronics Systems, ICCES 2018**, p. 235–238, 1 out. 2018.

MEMON, J. et al. Handwritten Optical Character Recognition (OCR): A Comprehensive Systematic Literature Review (SLR). **IEEE Access**, v. 8, p. 142642–142668, 2020.

MIJWIL, M. M.; SALEM, I. E.; ISMAEEL, M. M. The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review. **Iraqi Journal for Computer Science and Mathematics**, v. 4, n. 1, p. 87–101, 7 jan. 2023.

MISHRA, G.; GUPTA, P.; TANWAR, R. Target Recognition Using Pre-Trained Convolutional Neural Networks and Transfer Learning. **Procedia Computer Science**, v. 235, p. 1445–1454, 1 jan. 2024.

MOHAMMAD, R. M. **A Neural Network based Digital Forensics Classification**. Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA. **Anais**...IEEE, out. 2018. Disponível em: <https://ieeexplore.ieee.org/document/8612868/>

MOHAMMAD, R. M. A.; ALQAHTANI, M. A comparison of machine learning techniques for file system forensics analysis. **Journal of Information Security and Applications**, v. 46, p. 53–61, 1 jun. 2019.

MONTASARI, R. Artificial Intelligence and the Internet of Things Forensics in a National Security Context. **Advances in Information Security**, v. 101, p. 57–80, 2023.

MOREIRA, D. C.; FECHINE, J. M. A Machine Learning-based Forensic Discriminator of Pornographic and Bikini Images. **Proceedings of the International Joint Conference on Neural Networks**, v. 2018- July, 10 out. 2018.

MULLAN, P.; RIESS, C.; FREILING, F. Forensic source identification using JPEG image headers: The case of smartphones. **Digital Investigation**, v. 28, p. S68–S76, 1 abr. 2019.

MULYANTO, A.; HARTATI, S.; WARDOYO, R. Systematic Literature Review of Text Feature Extraction. **2022 7th International Conference on Informatics and Computing, ICIC 2022**, p. 1–6, 2022.

MUTHUKRISHNAN, N. et al. Brief History of Artificial Intelligence. **Neuroimaging Clinics of North America**, v. 30, n. 4, p. 393–399, 1 nov. 2020.

NASREEN, G. et al. Review: a comparative study of state-of-the-art skin image segmentation techniques with CNN. **Multimedia Tools and Applications**, v. 82, n. 7, p. 10921–10942, 1 mar. 2023.

NGEJANE, C. H. et al. Digital forensics supported by machine learning for the detection of online sexual predatory chats. **Forensic Science International: Digital Investigation**, v. 36, p. 301109, 1 mar. 2021.

NGOX, V. M. et al. Investigation, Detection and Prevention of Online Child Sexual Abuse Materials: A Comprehensive Survey. **Proceedings - 2022 RIVF International Conference on Computing and Communication Technologies, RIVF 2022**, p. 707–713, 2022.

NIE, Z. et al. Object-Based Perspective Transformation Data Augmentation for Object Detection. **Proceedings - 2022 International Conference on Frontiers of Artificial Intelligence and Machine Learning, FAIML 2022**, p. 186–190, 2022.

NIRVAN, A. et al. Child Pornography: The Filth of Society. **Advancements in Cybercrime Investigation and Digital Forensics**, p. 345–366, 6 out. 2023.

NOVAK, M. Digital Evidence in Criminal Cases Before the U.S. Courts of Appeal: Trends and Issues for Consideration. **The Journal of Digital Forensics, Security and Law**, v. 14, n. 4, p. 3, 6 abr. 2019.

OLADIPO, F. et al. The State of the Art in Machine Learning-Based Digital Forensics. **SSRN Electronic Journal**, 18 maio 2020.

OLIVEIRA, A. S. DE. **A new android malware detection method based on multimodal deep learning and hybrid analysis**. [s.l.] Universidade Nove de Julho - UNINOVE, 2022.

OMRANPOUR, H.; MOHAMMADI LEDARI, Z.; TAHERI, M. Presentation of encryption method for RGB images based on an evolutionary algorithm using chaos functions and hash tables. **Multimedia Tools and Applications**, p. 1–18, 1 set. 2022.

OTSU, N. Threshold Selection Method From Gray-Level Histograms. **IEEE Trans Syst Man Cybern**, v. SMC-9, n. 1, p. 62–66, 1979.

PADILHA, R. et al. A Inteligência Artificial e os desafios da Ciência Forense Digital no século XXI. **Estudos Avancados**, v. 35, n. 101, p. 111–138, 19 abr. 2021.

PAGE, M. J. et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. **Revista Panamericana de Salud Publica/Pan American Journal of Public Health**, v. 46, p. 1, 30 dez. 2022.

PANDEY, M. et al. AI-based Integrated Approach for the Development of Intelligent Document Management System (IDMS). **Procedia Computer Science**, v. 230, p. 725–736, 1 jan. 2023.

PANT, D. et al. Robust OCR Pipeline for Automated Digitization of Mother and Child Protection Cards in India. **ACM Journal on Computing and Sustainable Societies**, v. 1, n. 1, 22 set. 2023.

PATEL, J. A. Handwritten And Printed Text Recognition Using Tesseract-OCR. **International Journal of Creative Research Thoughts (IJCRT)**, v. 9, n. 9, p. 69–77, 2021.

PEREIRA, I. E. DE A. et al. **Manual de Solicitação de Perícia**. 1. ed. Maceió: Perícia Oficial do Estado de Alagoas, 2019. v. 1

POLASTRO, M. D. C.; DA SILVA ELEUTERIO, P. M. NuDetective: A forensic tool to help combat child pornography through automatic nudity detection. **Proceedings - 21st International Workshop on Database and Expert Systems Applications, DEXA 2010**, p. 349–353, 2010.

POVEDANO ÁLVAREZ, D. et al. Learning Strategies for Sensitive Content Detection. **Electronics (Switzerland)**, v. 12, n. 11, p. 2496, 1 jun. 2023.

PRAVEEN GUJJAR, J.; PRASANNA KUMAR, H. R.; GURU PRASAD, M. S. Advanced NLP Framework for Text Processing. **2023 6th International Conference on Information Systems and Computer Networks, ISCON 2023**, 2023.

QUAYLE, E. Online sexual deviance, pornography and child sexual exploitation material. **Forensische Psychiatrie, Psychologie, Kriminologie**, v. 14, n. 3, p. 251–258, 25 jun. 2020.

RAMIRO, L. S. et al. Online child sexual exploitation and abuse: A community diagnosis using the social norms theory. **Child Abuse and Neglect**, v. 96, p. 104080, 1 out. 2019.

REJÓN PIÑA, R. A.; MA, C. Classification Algorithm for Skin Color (CASCo): A new tool to measure skin color in social science research. **Social Science Quarterly**, v. 104, n. 2, p. 168–179, 1 mar. 2023.

RHOADS, J. Psychological Effects of Cybercrime on Minorities: Short-Term and Long-Term Impacts. **Journal of Empirical Social Science Studies**, v. 7, n. 1, p. 1–31, 17 fev. 2023.

ROY, P. et al. **Natural Images**. India, 2018. Disponível em: <https://www.kaggle.com/datasets/prasunroy/natural-images>

SABAHI, F.; OMAIR AHMAD, M.; SWAMY, M. N. S. Content-based image retrieval using perceptual image hashing and hopfield neural network. **Midwest Symposium on Circuits and Systems**, v. 2018- Augus, p. 352–355, 2 jul. 2018.

SABER, A. H.; KHAN, M. A.; MEJBEL, B. G. A survey on image forgery detection using different forensic approaches. **Advances in Science, Technology and Engineering Systems**, v. 5, n. 3, p. 361–370, 1 jun. 2020.

SAISUNDAR, A.; DEVI, T. Accurate Human Palm Recognition System in Cybercrime Analysis using Naive Bayes in comparison with Decision Tree. **Proceedings of the International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering, ICECONF 2023**, 2023.

SALAH, K. BEN; OTHMANI, M.; KHERALLAH, M. A novel approach for human skin detection using convolutional neural network. **Visual Computer**, v. 38, n. 5, p. 1833–1843, 1 maio 2022.

SAMANTA, P.; JAIN, S. Analysis of Perceptual Hashing Algorithms in Image Manipulation Detection. **Procedia Computer Science**, v. 185, p. 203–212, 1 jan. 2021.

SAMUELSSON, E. Classification of skin pixels in images: Using feature recognition and threshold segmentation. 2018.

SANCHEZ, L. et al. A Practitioner Survey Exploring the Value of Forensic Tools, AI, Filtering, & Safer Presentation for Investigating Child Sexual Abuse Material (CSAM). **Digital Investigation**, v. 29, p. S124–S142, 1 jul. 2019.

SANGHVI, K. et al. A Survey on Image Classification Techniques. **SSRN Electronic Journal**, 25 nov. 2021.

SARANG, P. Decision Tree. **Thinking Data Science**, p. 75–96, 2023.

SCHÖNFELDER, P. et al. Deep learning-based text detection and recognition on architectural floor plans. **Automation in Construction**, v. 157, p. 105156, 1 jan. 2024.

SEBYAN BLACK, INGE.; FENNELLY, L. J. **Investigations and the Art of the Interview**. 4th. ed. Cambridge: Butterworth-Heinemann, 2021.

SESHADRI SASTRY, K.; MADHUSUDHANA RAO, T. V.; PRAVEEN CHAKRAVARTHY, B. H. Classification and Detection of Skin Tones Using Big Data Machine Learning Algorithms under Rapidly Varying Illuminating Conditions. **Proceedings of the 2nd International Conference on Trends in Electronics and Informatics, ICOEI 2018**, p. 684–690, 29 nov. 2018.

SETIAWAN, N. et al. Impact of Cybercrime in E-Business and Trust. **International Journal of Civil Engineering and Technology (IJCIET)**, v. 9, n. 7, p. 652–656, 2018.

SHARMA, V. K.; MIR, R. N. A comprehensive and systematic look up into deep learning based object detection techniques: A review. **Computer Science Review**, v. 38, p. 100301, 1 nov. 2020.

SHERSTINSKY, A. Fundamentals of Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM) network. **Physica D: Nonlinear Phenomena**, v. 404, p. 132306, 1 mar. 2020.

SHEWALKAR, A.; NYAVANANDI, D.; LUDWIG, S. A. Performance Evaluation of Deep neural networks Applied to Speech Recognition: Rnn, LSTM and GRU. **Journal of Artificial Intelligence and Soft Computing Research**, v. 9, n. 4, p. 235–245, 1 out. 2019.

SONY, S. et al. A systematic review of convolutional neural network-based structural condition assessment techniques. **Engineering Structures**, v. 226, p. 111347, 1 jan. 2021.

STEEL, C. M. S. et al. An integrative review of historical technology and countermeasure usage trends in online child sexual exploitation material offenders. **Forensic Science International: Digital Investigation**, v. 33, p. 300971, 1 jun. 2020.

STEINEBACH, M.; LIU, H.; YANNIKOS, Y. Efficient cropping-resistant robust image hashing. **Proceedings - 9th International Conference on Availability, Reliability and Security, ARES 2014**, p. 579–585, 9 dez. 2014.

STÖHR, J. Classical Diffraction and Diffractive Imaging. **Springer Tracts in Modern Physics**, v. 288, p. 385–464, 2023.

STRUPPEK, L. et al. Learning to Break Deep Perceptual Hashing: The Use Case NeuralHash. **ACM International Conference Proceeding Series**, p. 58–69, 2022.

SULTAN, T. et al. Machine Learning in Cyberbullying Detection from Social-Media Image or Screenshot with Optical Character Recognition. **International Journal of Intelligent Systems and Applications**, v. 15, n. 2, p. 1–13, 8 abr. 2023.

SUN, X. et al. HEBCS: A High-Efficiency Binary Code Search Method. **Electronics (Switzerland)**, v. 12, n. 16, p. 3464, 16 ago. 2023.

SZANDAŁA, T. Review and comparison of commonly used activation functions for deep neural networks. **Studies in Computational Intelligence**, v. 903, p. 203–224, 2021.

TABONE, A. et al. Pornographic content classification using deep-learning. **DocEng 2021 - Proceedings of the 2021 ACM Symposium on Document Engineering**, v. 15, p. 1–10, 16 ago. 2021.

TAHIR, A.; AHMAD KHALID, S. K.; MOHD FADZIL, L. Child Detection Model Using YOLOv5. **Journal of Soft Computing and Data Mining**, v. 4, n. 1, p. 72–81, 25 maio 2023.

TRALIC D. et al. **CoMoFoD - Image Database for Copy-Move Forgery Detection**. Disponível em: <https://www.vcl.fer.hr/comofod/index.html>. Acesso em: 31 dez. 2023.

TRAN, N. T. et al. On Data Augmentation for GAN Training. **IEEE Transactions on Image Processing**, v. 30, p. 1882–1897, 2021.

UKWEN, D. O.; KARABATAK, M. Review of NLP-based Systems in Digital Forensics and Cybersecurity. **9th International Symposium on Digital Forensics and Security, ISDFS 2021**, p. 1–9, 28 jun. 2021.

VEZETEU, P. V. et al. Secure Transmission System for Personal Data Acquired Through Optical Character Recognition. **2018 IEEE 24th International Symposium for Design and Technology in Electronic Packaging, SIITME 2018 - Proceedings**, p. 349–354, 2 jul. 2019.

VITORINO, P. et al. Leveraging deep neural networks to fight child pornography in the age of social media. **Journal of Visual Communication and Image Representation**, v. 50, p. 303–313, 1 jan. 2018.

VOULODIMOS, A. et al. Deep Learning for Computer Vision: A Brief Review. **Computational Intelligence and Neuroscience**, v. 2018, p. 1–13, 2018.

WAELEN, R. **The power of computer vision : a critital analysis**. Enschede, The Netherlands: University of Twente, 27 set. 2023.

WANG, K. et al. Perspective Transformation Data Augmentation for Object Detection. **IEEE Access**, v. 8, p. 4935–4943, 2020.

WANG, X. et al. Perceptual hash-based coarse-to-fine grained image tampering forensics method. **Journal of Visual Communication and Image Representation**, v. 78, p. 103124, 1 jul. 2021.

WANG, Y. et al. Investigating the Availability of Child Sexual Abuse Materials in Dark Web Markets: Evidence Gathered and Lessons Learned. **ACM International Conference Proceeding Series**, p. 59–64, 14 jun. 2023.

WIRATAMA, M. R. et al. Pornography object detection using Viola-Jones algorithm and skin detection. **Proceedings - 2017 1st International Conference on Informatics and Computational Sciences, ICICoS 2017**, v. 2018- Janua, p. 29–34, 1 out. 2017.

WORDEN, K. et al. Artificial Neural Networks. Em: **Natural Computing Series**. [s.l: s.n.]. p. 161–204.

WU, T.; BREITINGER, F.; O'SHAUGHNESSY, S. Digital forensic tools: Recent advances and enhancing the status quo. **Forensic Science International: Digital Investigation**, v. 34, p. 300999, 1 set. 2020.

WU, Y. et al. A Novel Color Image Encryption Scheme Based on Hyperchaos and Hopfield Chaotic Neural Network. **Entropy**, v. 24, n. 10, p. 1474, 17 out. 2022.

XIE, B. et al. MLP-GAN for Brain Vessel Image Segmentation. p. 1–5, 5 maio 2023.

XU, X.; CHEN, S. An Optical Image Encryption Method Using Hopfield Neural Network. **Entropy**, v. 24, n. 4, p. 521, 7 abr. 2022.

YAO, G.; LEI, T.; ZHONG, J. A review of Convolutional-Neural-Network-based action recognition. **Pattern Recognition Letters**, v. 118, p. 14–22, 1 fev. 2019.

YOU, H. et al. Efficient and Low Color Information Dependency Skin Segmentation Model. **Mathematics**, v. 11, n. 9, p. 2057, 26 abr. 2023.

YU, A. S. O. et al. Tomada de decisão nas organizações: o que muda com a Inteligência Artificial? **Estudos Avançados**, v. 38, n. 111, p. 327–348, 30 ago. 2024.

YU, M. et al. Perceptual Hashing With Complementary Color Wavelet Transform and Compressed Sensing for Reduced-Reference Image Quality Assessment. **IEEE Transactions on Circuits and Systems for Video Technology**, v. 32, n. 11, p. 7559–7574, 1 nov. 2022.

ZEROUAL, I.; LAKHOUAJA, A. Data science in light of natural language processing: An overview. **Procedia Computer Science**, v. 127, p. 82–91, 1 jan. 2018.

ZHOU, J. et al. Evaluating the quality of machine learning explanations: A survey on methods and metrics. **Electronics (Switzerland)**, v. 10, n. 5, p. 1–19, 4 mar. 2021.

ZHU, W.; SANG, P.; HE, Y. Facial skin colour classification using machine learning and hyperspectral imaging data. **IET Image Processing**, v. 16, n. 2, p. 509–520, 1 fev. 2022.

ZOU, Z. et al. Object Detection in 20 Years: A Survey. **Proceedings of the IEEE**, v. 111, n. 3, p. 257–276, 13 maio 2023.

ANEXO A – CRIMES CIBERNÉTICOS

Neste anexo são descritos os crimes cibernéticos listados por agência internacionais de combate ao crime cibernético.

Crime Cibernético	Descrição
Ciberextorsão	Extorquir dinheiro para evitar um ataque.
Ciberterrorismo	Promoção da violência contra pessoas e organizações
Cryptojacking	Invasão a sistemas computacionais para mineração de criptomoedas.
Cyberbulling	Ato de praticar *bullying* através de plataformas digitais
Espionagem Cibernética	Acesso ao código-fonte e informações sensíveis de aplicações privadas.
Exploração de Vulnerabilidades	Explorar falha de segurança sem autorização.
Futro de identidade	Ato de se passar por outra pessoa com o uso de dados pessoais.
DoS / DDoS	Interromper o funcionamento de serviços informatizados.
Intrusão à redes de Telefone (PSTN)	Invasão a sistemas de telefonia.
Intrusão à redes de Computadores	Invasão a sistemas de computadores.
Jogos de Azar	Propagação, Divulgação e Incentivo a prática de jogos de azar.
Phishing	Envio de emails fraudulentos.
Pirataria de Software	Quebra e/ou exposição da Licença do software.
Pornografia Infantojuvenil	Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente.
Sequestro e Encriptação de Dados	Uso de *Ransomwares* para sequestro de arquivos.
Violação a Integridade de Redes	Sobrecarga da comunicação dos componentes conectados em rede.
Violação à privacidade	Acesso e/ou modificação de arquivos privados.

APÊNDICE A – PUBLICAÇÕES COM PORNOGRAFIA INFANTOJUVENIL E IA

Neste apêndice são descritas todas as publicações identificadas na RSL deste trabalho que abordam a Pornografia Infantojuvenil e Inteligência Artificial.

ID	Título	Autores	Ano
01	A Benchmark Methodology for Child Pornography Detection	MACEDO, Joao; COSTA, Filipe; DOS SANTOS, Jefersson A.	2018
02	A Machine Learning-based Forensic Discriminator of Pornographic and Bikini Images	MOREIRA, Danilo Coura; FECHINE, Joseana Macêdo.	2018
03	A Nudity Detection Algorithm for Web-based Online Networking Platform	DEWAN, Ritu et al.	2023
04	A Practitioner Survey Exploring the Value of Forensic Tools, AI, Filtering, & Safer Presentation for Investigating Child Sexual Abuse Material (CSAM)	SANCHEZ, Laura et al.	2019
05	A Preliminary Study of Lower Leg Geometry as a Soft Biometric Trait for Forensic Investigation	ISLAM, Md Rabiul; CHAN, Frodo Kin-Sun; KONG, Adams Wai-Kin.	2014
06	A Review of Age Estimation Research to Evaluate Its Inclusion in Automated Child Pornography Detection	MACLEOD, Lee; KING, David; DEMPSTER, Euan.	2020
07	Age and Gender Detection in the I-DASH Project	MEINEDO, Hugo; TRANCOSO, Isabel.	2011
08	An Experimental Approach for Hybrid Content-based Web Page Detection	GORRO, Ken; FELISCUZO, Larmie; STA. ROMANA, Cherry Lyn.	2022
09	Automated identification of relatively permanent pigmented or vascular skin marks (RPPVSM)	NURHUDATIANA, Arfika et al.	2013
10	Automatic detection of child pornography using color visual words	ULGES, Adrian; STAHL, Armin.	2011
11	Automatic Detection of CSA Media by Multi-modal Feature Fusion for Law Enforcement Support	SCHULZE, Christian et al.	2014
12	C³-Sex: A Chatbot to Chase Cyber perverts	MURCIA, Jossie et al.	2019
13	DeepUAge: Improving Underage Age Estimation Accuracy to Aid CSEM Investigation	ANDA, Felix; LE-KHAC, Nhien-An; SCANLON, Mark.	2020
14	Detection of Prone Areas of Crime Against Children using DBSCAN	CHANGALASETTY, Sreelasya et al.	2023
15	Digital forensics supported by machine learning for the detection of online sexual predatory chats	NGEJANE, Cynthia H. et al.	2021
16	Evaluating Performance of an Adult Pornography Classifier for Child Sexual Abuse Detection	AL-NABKI, Mhd Wesam et al.	2020
17	Forensic Image Inspection Assisted by Deep Learning	MAYER, Felix; STEINEBACH, Martin	2017

ID	Título	Autores	Ano
18	Improving Borderline Adulthood Facial Age Estimation through Ensemble Learning Felix	ANDA, Felix et al.	2019
19	Learning to Break Deep Perceptual Hashing: The Use Case NeuralHash	STRUPPEK, Lukas et al.	2022
20	Leveraging deep neural networks to fight child pornography in the age of social media	VITORINO, Paulo et al.	2018
21	NuDetective: A forensic tool to help combat child pornography through automatic nudity detection	DE CASTRO POLASTRO, Mateus; DA SILVA ELEUTERIO, Pedro Monteiro	2010
22	Obscenity Detection in Videos Through a Sequential ConvNet Pipeline Classifier	GAUTAM, Neil; VISHWAKARMA, Dinesh Kumar.	2023
23	Pornographic content classification using deep-learning	TABONE, André et al.	2021
24	Protecting Children from Online Exploitation: Can a Trained Model Detect Harmful Communication Strategies?	COOK, Darren et al.	2023
25	SBMYv3: Improved MobYOLOv3 a BAM attention-based approach for obscene image and video detection	SAMAL, Sonali et al.	2023
26	Short Text Classification Approach to Identify Child Sexual Exploitation Material	AL-NABKI, MHD Wesam et al.	2023
27	Statistical Sampling Approach to Investigate Child Pornography Cases Nikolaos	SARANTINOS, Nikolaos; AL-NEMRAT, Ameer; NAEEM, Usman	2013
28	Towards Automatic Detection of Child Pornography	SAE-BAE, Napa et al.	2014

APÊNDICE B – LENNA DATABASE

Neste apêndice, ilustra-se as vinte imagens que compõem a base de imagens *Lenna Database.*


bordas-enfat.


Gaussian 3x3


Gaussian 7x7

With text


Bin_with_otsu


Bmp_format

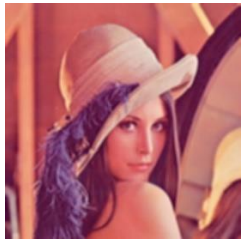

Escala_de_cinza


Mirror_efect


Salt_and_pepper


With Logos


Media 3x3


Media 7x7


Mediana 3x3


Mediana 7x7


Png_format


Tiff_format


Half-altered


High alter

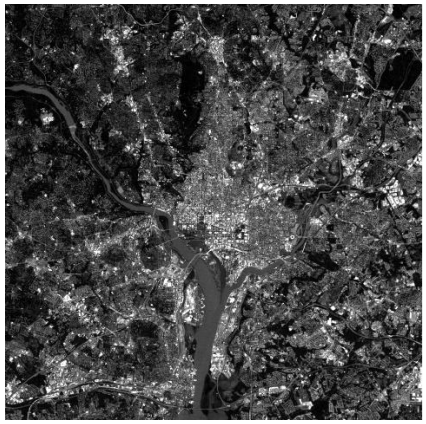

Low alter


Original

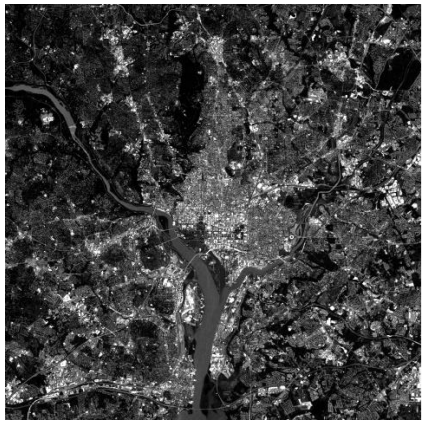
APÊNDICE C – WASHINGTON DATABASE

Neste apêndice, ilustra-se as sete imagens que compõem a base de imagens *Washington Database.*

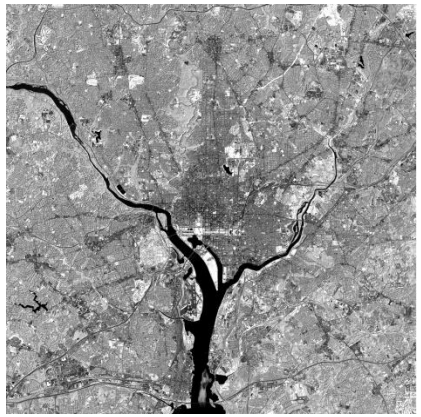
Original



Band_2

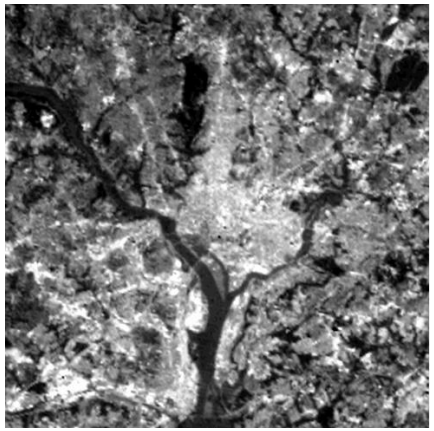


Band_3



Band_4

Band_5



Band_6

Band_7

APÊNDICE D – PALACE DATABASE

Neste apêndice, ilustra-se as trinta e uma imagens que compõem a base de imagens *Palace Database.*


Original


Alternative (1)


Alternative (2)


Alternative (3)


Alternative (4)


Alternative (5)


Alternative (6)


Alternative (7)


Alternative (8)


Alternative (9)


Alternative (10)


Alternative (11)


Alternative (12)


Alternative (13)


Alternative (14)


Alternative (15)


Alternative (16)


Alternative (17)


Alternative (18)


Alternative (19)


Alternative (20)


Alternative (21)


Alternative (22)


Alternative (23)


Alternative (24)


Alternative (25)


Alternative (26)


Alternative (27)

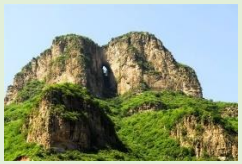

Alternative (28)


Alternative (29)


Alternative (30)

APÊNDICE E – MOUNTAIN DATABASE

Neste apêndice, ilustra-se as trinta imagens que compõem a base de imagens *Mountain Database*.


Original


Alternative (1)


Alternative (2)


Alternative (3)


Alternative (4)


Alternative (5)


Alternative (6)


Alternative (7)

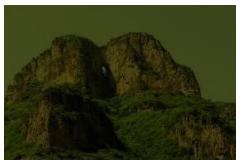

Alternative (8)


Alternative (9)


Alternative (10)


Alternative (11)

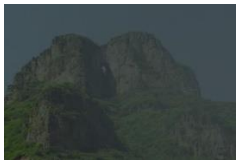

Alternative (12)


Alternative (13)


Alternative (14)


Alternative (15)


Alternative (16)

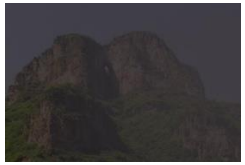

Alternative (17)


Alternative (18)


Alternative (19)


Alternative (20)


Alternative (21)


Alternative (22)


Alternative (23)


Alternative (24)


Alternative (25)


Alternative (26)


Alternative (27)


Alternative (28)


Alternative (29)

APÊNDICE F – PARK DATABASE

Neste apêndice, ilustra-se as onze imagens que compõem a base de imagens *Park Database.*

Original

Alternative (1)

Alternative (2)

Alternative (3)

Alternative (4)

Alternative (5)

Alternative (6)

Alternative (7)

Alternative (8)

Alternative (9)

Alternative (10)

APÊNDICE G – NATURAL IMAGES

Neste apêndice, é ilustrado uma amostra das imagens que compõe a base *Natural Images*. Essa amostra é composta por 20 imagens.

Img(1)

Img(2)

Img(3)

Img(4)

Img(5)

Img(6)

Img(7)

Img(8)

Img(9)

Img(10)

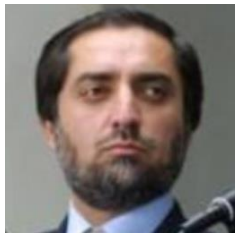
Img(11)

Img(12)

Img(13)

Img(14)

Img(15)



Img(16)

Img(17)

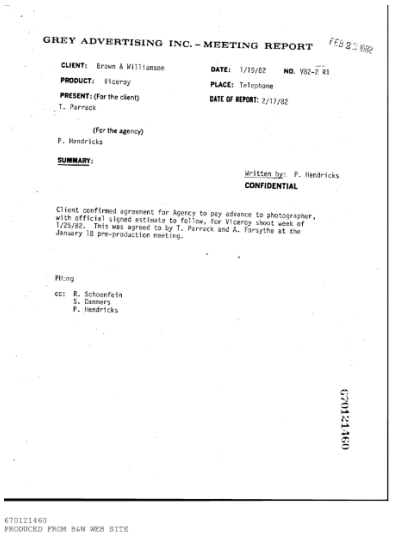
Img(18)

Img(19)

Img(20)

APÊNDICE H – FUNSD

Neste apêndice, é ilustrado uma amostra das imagens que compõe a base FUNSD (*Form Understanding in Noisy Scanned Documents*). Essa amostra é composta por 6 imagens.



GREY ADVERTISING INC. – MEETING REPORT

CLIENT: Brown & Williamson
PRODUCT: Vicerey
PRESENT: (For the client) T. Parrack
(For the agency) P. Hendricks
DATE: 1/19/82 NO. V82-2 R1
PLACE: Telephone
DATE OF REPORT: 2/17/82

SUMMARY:

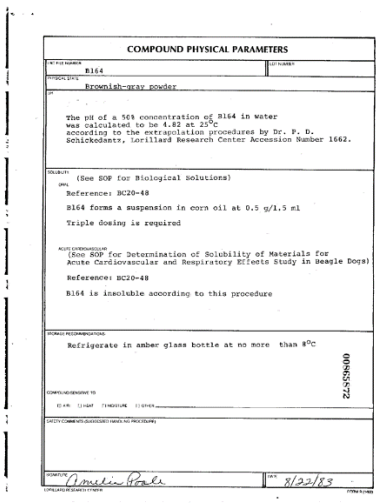
Written by: P. Hendricks
CONFIDENTIAL

Client confirmed agreement for Agency to pay advance to photographer, with official signed estimate to follow, for Vicerey shoot week of 1/25/82. This was agreed to by T. Parrack and A. Forsythe at the January 18 pre-production meeting.

Filing
cc: R. Schoenfein
S. Dannars
P. Hendricks

670121460
PRODUCED FROM B&W WEB SITE

660978



COMPOUND PHYSICAL PARAMETERS

B164

Brownish-gray powder

The pH of a 56% concentration of B164 in water was calculated to be 4.82 at 25°C according to the extrapolation procedures by Dr. F. D. Schickedantz, Lorillard Research Center Accession Number 1662.

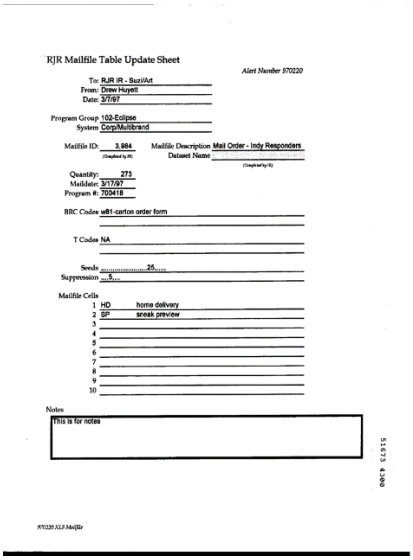
(See SOP for Biological Solutions)
Reference: BC20-48
B164 forms a suspension in corn oil at 0.5 g/1.5 ml
Triple dosing is required

(See SOP for Determination of Solubility of Materials for Acute Cardiovascular and Respiratory Effects Study in Beagle Dogs)
Reference: BC20-48
B164 is insoluble according to this procedure

Refrigerate in amber glass bottle at no more than 8°C

00865872

00865872



RJR Mailfile Table Update Sheet

Alert Number 970220

To: RJR IR - Suzi/Art
From: Drew Huyett
Date: 3/7/97

Program Group 102-Eclipse
System Corp/Multibrand

Mailfile ID: 3.984 Mailfile Description: Mail Order - Indy Responders
Dataset Name:

Quantity: 273
Maildate: 3/17/97
Program #: 700418

BRC Codes w61-carton order form

T Codes NA

Seeds 25
Suppression 5

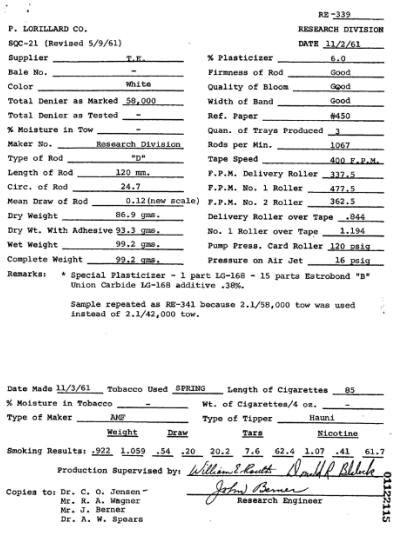
Mailfile Cells
1 HD home delivery
2 SP sneak preview
3
4
5
6
7
8
9
10

Notes
This is for notes

970220.XLS Mailfile

51673 4/98

00920294



RE-339

P. LORILLARD CO. RESEARCH DIVISION
SQC-21 (Revised 5/9/61) DATE 11/2/61

Supplier	T.E.	% Plasticizer	6.0
Bale No.	-	Firmness of Rod	Good
Color	White	Quality of Bloom	Good
Total Denier as Marked	58,000	Width of Band	Good
Total Denier as Tested	-	Ref. Paper	#450
% Moisture in Tow	-	Quan. of Trays Produced	3
Maker No.	Research Division	Rods per Min.	1067
Type of Rod	"B"	Tape Speed	400 F.P.M.
Length of Rod	120 mm.	F.P.M. Delivery Roller	337.5
Circ. of Rod	24.7	F.P.M. No. 1 Roller	477.5
Mean Draw of Rod	0.12(new scale)	F.P.M. No. 2 Roller	362.5
Dry Weight	86.9 gms.	Delivery Roller over Tape	.044
Dry Wt. With Adhesive	93.3 gms.	No. 1 Roller over Tape	1.194
Wet Weight	99.2 gms.	Pump Press. Card Roller	120 psig
Complete Weight	99.2 gms.	Pressure on Air Jet	16 psig

Remarks: * Special Plasticizer - 1 part LG-168 - 15 parts Estrobond "B" Union Carbide LG-168 additive .38%.

Sample repeated as RE-341 because 2.1/58,000 tow was used instead of 2.1/42,000 tow.

Date Made 11/3/61 Tobacco Used SPRING Length of Cigarettes 85
% Moisture in Tobacco - Wt. of Cigarettes/4 oz. -
Type of Maker AMF Type of Tipper Hauni

	Weight	Draw	Tars	Nicotine
Smoking Results:	.922	1.059	.54	.20
	20.2	7.6	62.4	1.07
	.41	61.7		

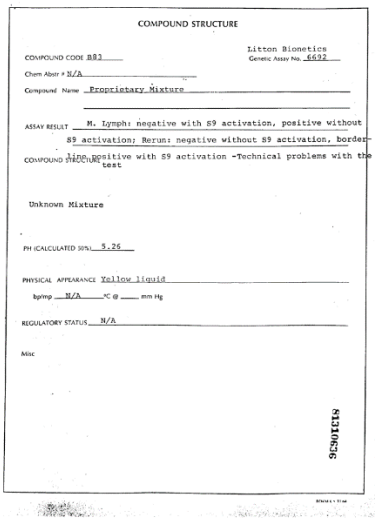
Production Supervised by: William E. Ruth, Donald P. Blevins

Copies to: Dr. C. O. Jensen
Mr. R. A. Wagner
Mr. J. Berner
Dr. A. W. Spears

John Berner
Research Engineer

01122115

01122115



COMPOUND STRUCTURE

Litton Bionetics
Generic Assay No. 6692

COMPOUND CODE B83
Chem Abstr # N/A
Compound Name Proprietary Mixture

ASSAY RESULT M. Lymph: negative with S9 activation, positive without S9 activation; Rerun: negative without S9 activation, borderline positive with S9 activation -Technical problems with the test

COMPOUND STRUCTURE

Unknown Mixture

PH (CALCULATED 50%) 5.26

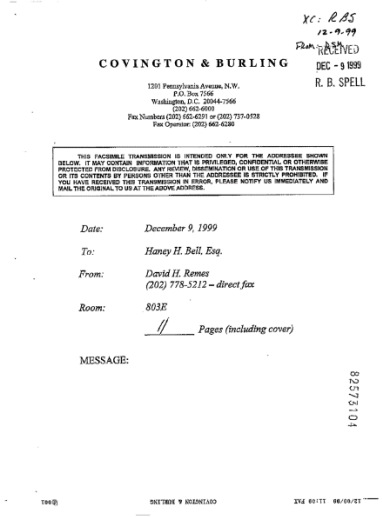
PHYSICAL APPEARANCE Yellow liquid
bp/mp N/A °C @ ___ mm Hg

REGULATORY STATUS N/A

Misc

81310636

81310636



COVINGTON & BURLING

1201 Pennsylvania Avenue, N.W.
P.O. Box 7566
Washington, D.C. 20044-7566
(202) 662-6000
Fax Numbers (202) 662-6291 or (202) 737-5928
Fax Operator: (202) 662-6280

THIS FACSIMILE TRANSMISSION IS INTENDED ONLY FOR THE ADDRESSEE SHOWN BELOW. IT MAY CONTAIN INFORMATION THAT IS PRIVILEGED, CONFIDENTIAL OR OTHERWISE PROTECTED FROM DISCLOSURE. ANY REVIEW, DISSEMINATION OR USE OF THIS TRANSMISSION OR ITS CONTENTS BY PERSONS OTHER THAN THE ADDRESSEE IS STRICTLY PROHIBITED. IF YOU HAVE RECEIVED THIS TRANSMISSION IN ERROR, PLEASE NOTIFY US IMMEDIATELY AND MAIL THE ORIGINAL TO US AT THE ABOVE ADDRESS.

Date: December 9, 1999
To: Haney H. Bell, Esq.
From: David H. Remes
(202) 778-3212 – direct fax
Room: 803E
11 Pages (including cover)

MESSAGE:

RECEIVED
DEC - 9 1999
R. B. SPELL

cc: RAS 12-9-99

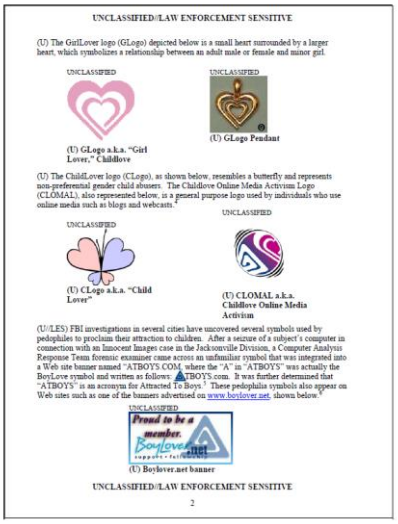
82573101

82573104

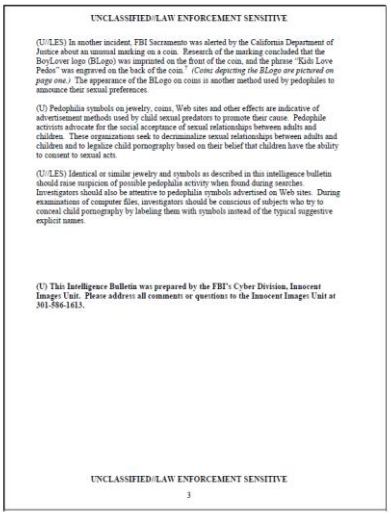
APÊNDICE I – FBI SYMBOLS DOCUMENT

Neste apêndice, é ilustrado o documento com as imagens que compõe a base FBI Symbols Document. No total, o documento é composto por 6 páginas e 13 Símbolos relacionados a crimes contra o público infantojuvenil.

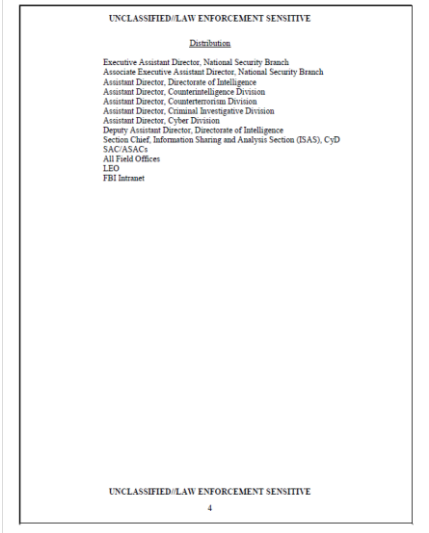
Página 1



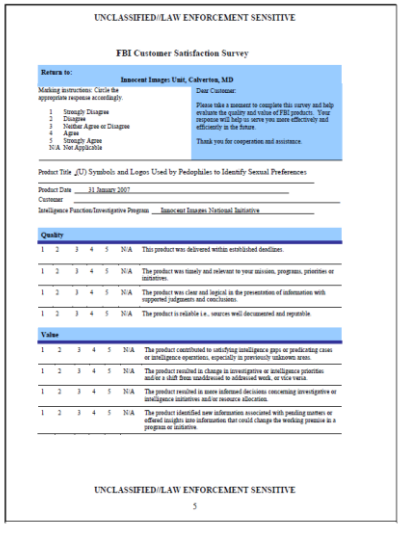
Página 2



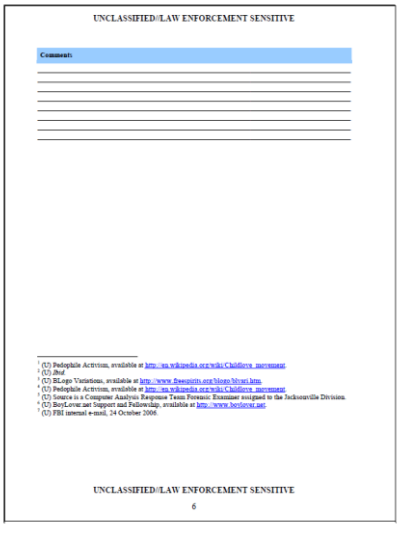
Página 3



Página 4



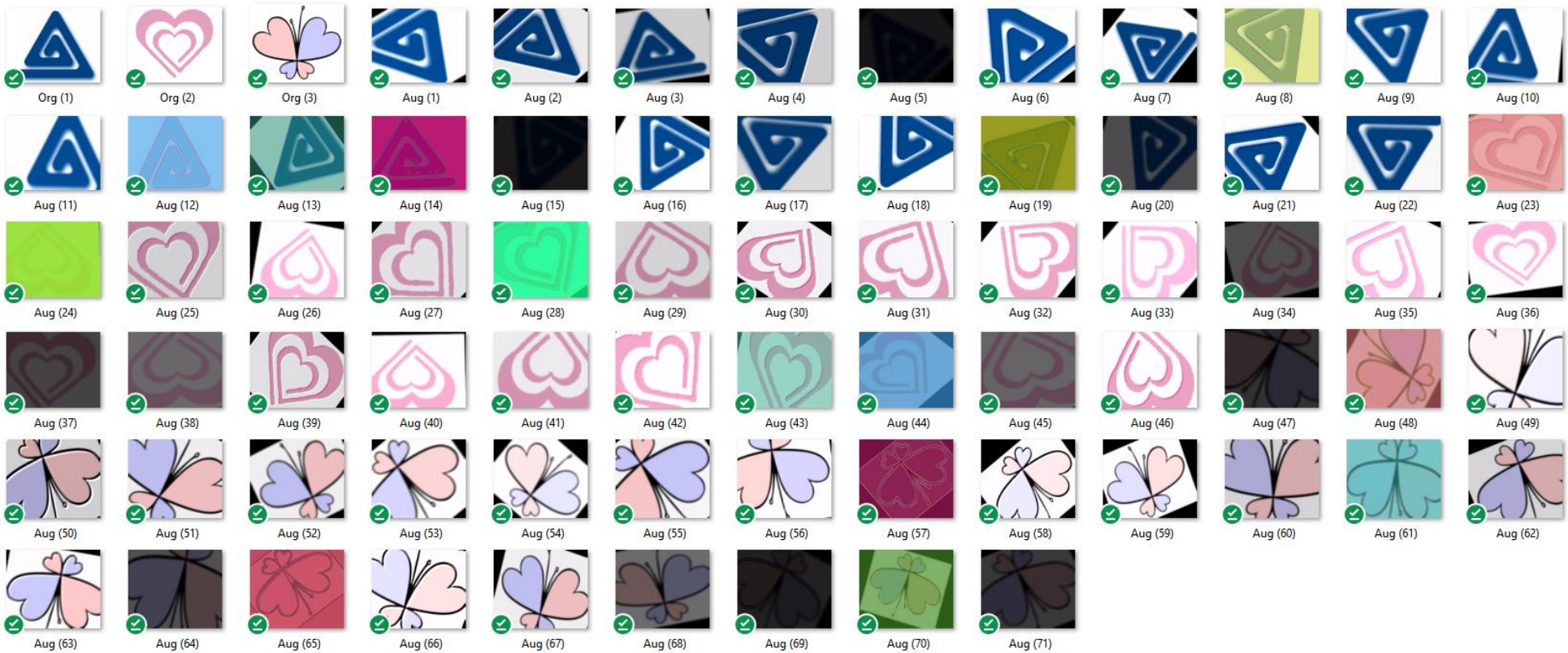
Página 5



Página 6

APÊNDICE J – FBI SYMBOLS DOCUMENT ENRIQUECIDA

Neste apêndice, é ilustrado as imagens produzidas pelo enriquecimento gerado pela aplicação de Aumento de Dados com as Redes Adversárias Generativas (RAGs).



APÊNDICE K – FBI SYMBOLS DOCUMENT VALIDAÇÃO

Neste apêndice, é ilustrado as imagens que serão utilizadas para validação da Estratégia D.


SymbolA_01


SymbolA_02


SymbolA_03


SymbolA_04


SymbolA_05


SymbolA_06

SymbolA_07


SymbolA_08


SymbolAB_01


SymbolB_01

APÊNDICE L – DISTÂNCIA DE HAMMING ENTRE OS VALORES HASH PERCEPTIVOS

Neste apêndice, são descritas as distâncias de Hamming entre os valores Hash Perceptivos gerados pelos algoritmos de Hash Perceptivo aplicado nas bases: *Lenna Database, Washington Database, Palace Database, Mountain Database e Park Database,* na fase A4 da Estratégia A.

- *Lenna Database*

Nome	Original _Array	A-Hash	P-Hash	D-Hash	W-Hash	CPR-Hash
Original	0	0	0	0	0	0
Imagem em Bmp	0	0	0	0	0	0,50
Imagem em Png	0	0	0	0	0	0,50
Imagem em Tiff	0	0	0	0	0	0,50
Gaussiana 3x3	0	0	0	0	0	0,88
Gaussiana 7x7	0	0	0	0	0	1,13
Mediana 7x7	0	0	0	0	0	1,25
Mediana 3x3	0	0	0	0	0	1,50
Média 3x3	0	0	0	0	0	2,88
Média 7x7	0	0	0	0	0	2,88
Pouca alteração	0	1	0	0	0	0,88
Adição de Texto	0	3	2	0	0	0,63
Escala de Cinza	0	0	0	0	0	0,50
Ruído Sal e Pimenta	0	0	0	1	2	13,63
Bordas Enfatizadas	0	0	0	2	0	12,00
Muita alteração	0	10	8	2	6	12,88
Binarização com OTSU	0	7	10	5	5	13,13
Metade Alterada	0	14	10	8	14	14,50
Efeito Espelho	0	14	16	14	14	14,75
Adição de Objetos	0	7	6	5	6	15

- *Washington Database*

Nome	Original _Array	A-Hash	P-Hash	D-Hash	W-Hash	CPR-Hash
Fig01_WashingtonDC_Band1	0	0	0	0	0	0
Fig02_WashingtonDC_Band2	0	4	2	7	2	15,1
Fig03_WashingtonDC_Band3	0	2	2	7	2	14,4
Fig04_WashingtonDC_Band4	0	16	16	16	16	15,9
Fig05_WashingtonDC_Band5	0	9	13	12	11	15,9
Fig06_WashingtonDC_Band6	0	5	7	5	6	16
Fig07_WashingtonDC_Band7	0	6	11	3	7	15,6

- *Palace Database*

Nome	Original _Array	A-Hash	P-Hash	D-Hash	W-Hash	CPR-Hash
Imagem Original	0	0	0	0	0	0
Alternative (1)	0	0	0	2	0	15,40
Alternative (2)	0	0	0	2	0	15,40
Alternative (3)	0	0	0	1	0	15,20
Alternative (4)	0	0	0	0	0	15,40
Alternative (5)	0	0	0	0	0	15,00
Alternative (6)	0	0	0	2	0	15,20
Alternative (7)	0	0	0	1	0	15,40
Alternative (8)	0	0	0	1	0	15,00
Alternative (9)	0	0	0	0	0	15,00
Alternative (10)	0	0	0	2	0	15,00
Alternative (11)	0	0	0	2	0	15,00
Alternative (12)	0	0	0	2	0	15,00
Alternative (13)	0	0	0	0	0	15,00
Alternative (14)	0	0	2	2	0	15,20
Alternative (15)	0	0	0	1	0	15,20
Alternative (16)	0	0	0	1	0	15,20
Alternative (17)	0	10	10	10	11	15,40
Alternative (18)	0	10	11	9	11	15,40
Alternative (19)	0	10	10	10	11	14,00
Alternative (20)	0	11	11	8	9	14,80
Alternative (21)	0	10	10	9	11	15,20
Alternative (22)	0	10	10	9	11	15,00
Alternative (23)	0	10	10	9	11	15,20
Alternative (24)	0	0	0	1	0	15,00
Alternative (25)	0	0	0	1	0	15,00
Alternative (26)	0	0	0	1	0	15,00
Alternative (27)	0	0	0	0	0	15,00
Alternative (28)	0	0	0	1	0	15,20
Alternative (29)	0	0	0	2	0	15,00
Alternative (30)	0	0	0	1	0	15,00

- *Mountain Database*

Nome	Original _Array	A-Hash	P-Hash	D-Hash	W-Hash	CPR-Hash
Imagem Original	0	0	0	0	0	0
Alternative (1)	0	0	2	2	2	14,16
Alternative (2)	0	0	2	1	2	15,16
Alternative (3)	0	0	2	1	2	14,66
Alternative (4)	0	0	2	2	2	15,16
Alternative (5)	0	0	2	1	2	15,16
Alternative (6)	0	0	2	1	2	14,66

Nome	Original _Array	A-Hash	P-Hash	D-Hash	W-Hash	CPR-Hash
Alternative (7)	0	0	2	2	2	15,16
Alternative (8)	0	0	2	2	4	15,16
Alternative (9)	0	0	2	1	4	15,16
Alternative (10)	0	0	2	1	2	15,16
Alternative (11)	0	0	2	1	2	15,16
Alternative (12)	0	0	2	1	2	15,16
Alternative (13)	0	0	0	1	4	15,16
Alternative (14)	0	0	2	0	2	15,16
Alternative (15)	0	0	2	2	4	15,16
Alternative (16)	0	4	6	3	6	15,50
Alternative (17)	0	4	8	4	6	15,16
Alternative (18)	0	2	8	4	6	14,66
Alternative (19)	0	2	6	5	6	15,16
Alternative (20)	0	1	8	4	6	15,33
Alternative (21)	0	3	8	2	6	15,33
Alternative (22)	0	1	6	5	6	15,16
Alternative (23)	0	0	2	2	2	15,16
Alternative (24)	0	0	2	1	2	15,16
Alternative (25)	0	0	2	1	2	15,16
Alternative (26)	0	0	2	1	0	15,66
Alternative (27)	0	0	2	1	2	15,16
Alternative (28)	0	0	2	1	2	15,16
Alternative (29)	0	0	2	1	2	15,16

- *Park Database*

Nome	Original _Array	A-Hash	P-Hash	D-Hash	W-Hash	CPR-Hash
Imagem Original	0	0	0	0	0	0
Alternative (1)	0	0	0	0	0	13,77
Alternative (2)	0	0	0	0	0	9,44
Alternative (3)	0	0	0	0	0	6,66
Alternative (4)	0	0	0	1	0	10,00
Alternative (5)	0	0	0	1	0	31,11
Alternative (6)	0	6	6	3	4	14,40
Alternative (7)	0	6	6	3	4	11,33
Alternative (8)	0	6	7	3	4	26,66
Alternative (9)	0	6	6	3	4	28,88
Alternative (10)	0	6	7	4	4	50,00

APÊNDICE M – HISTOGRAMAS DE DISTRIBUIÇÃO DOS VALORES DOS PIXELS DAS BANDAS R, G E B NA BASE SKIN SEGMENTATION

Neste apêndice, são ilustrados os histogramas de distribuições dos valores dos pixels das bandas R, G e B na base *Skin Segmentation*.