UNIVERSIDADE FEDERAL DO CEARÁ

***CAMPUS* SOBRAL**

CURSO DE GRADUAÇÃO EM ENGENHARIA DA COMPUTAÇÃO

VITOR CESAR OLIVEIRA GOMES ARRUDA

REVISÃO BIBLIOMÉTRICA E SISTEMÁTICA DAS PESQUISAS DE AUTENTICAÇÃO E PROTEÇÃO DE IMAGENS DIGITAIS

SOBRAL

2025

VITOR CESAR OLIVEIRA GOMES ARRUDA

REVISÃO BIBLIOMÉTRICA E SISTEMÁTICA DAS PESQUISAS DE AUTENTICAÇÃO E PROTEÇÃO DE IMAGENS DIGITAIS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia da Computação do *Campus* Sobral da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia da Computação.

Orientador: Prof. Dr. Marcelo Marques Simões de Souza

SOBRAL

2025

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

A819r Arruda, Vitor Cesar Oliveira Gomes.
REVISÃO BIBLIOMÉTRICA E SISTEMÁTICA DAS PESQUISAS DE AUTENTICAÇÃO E PROTEÇÃO DE IMAGENS DIGITAIS / Vitor Cesar Oliveira Gomes Arruda. – 2025.
45 f. : il.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Sobral, Curso de Engenharia da Computação, Sobral, 2025.
Orientação: Prof. Dr. Prof. Dr. Marcelo Marques Simões de Souza.

1. Proteção de Conteúdo. 2. Revisão Sistemática. 3. Revisão Bibliométrica. 4. Técnicas Ativas. 5. Técnicas Passivas. I. Título.

CDD 621.39

VITOR CESAR OLIVEIRA GOMES ARRUDA

REVISÃO BIBLIOMÉTRICA E SISTEMÁTICA DAS PESQUISAS DE AUTENTICAÇÃO E PROTEÇÃO DE IMAGENS DIGITAIS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia da Computação do *Campus* Sobral da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia da Computação.

Aprovada em: 12 de Fevereiro de 2025

BANCA EXAMINADORA

Prof. Dr. Marcelo Marques Simões de Souza
(Orientador)
Universidade Federal do Ceará (UFC)

Prof. Me. David Nascimento Coelho
Universidade Federal do Ceará (UFC)

Me. Alan Marques da Rocha
Universidade Federal do Ceará (UFC)

À minha família, por sua capacidade de acreditar em mim e investir em mim. Mãe, seu cuidado e dedicação foi que deram, em alguns momentos, a esperança para seguir. Pai, sua presença significou segurança e certeza de que não estou sozinho nessa caminhada.

AGRADECIMENTOS

Agradeço primeiramente aos meus pais, Valeria Oliveira e Vicente Cesar, e ao meu irmão, Gabriel, pelo incentivo e apoio constante durante a minha graduação. Ao professor Marcelo pelo tempo dedicado na excelente orientação em todas as etapas da construção deste trabalho e por me dar esperança no momento que mais precisei. À banca examinadora, composta pelo professor David Nascimento Coelho e pelo doutorando Alan Marques da Rocha, expresso minha gratidão pelas preciosas colaborações e sugestões que enriqueceram este trabalho. Aos amigos da graduação, Ailton Guarinho, Ananda Karen, Daniel Araujo, Samuel Gomes, Levi Frota, cujas contribuições, reflexões, críticas e sugestões no âmbito pessoal e profissional foram inestimáveis.

"O sonho é que leva a gente para frente. Se a gente for seguir a razão, fica aquietado, acomodado."

(Ariano Suassuna)

RESUMO

A crescente facilidade de manipulação de mídias digitais traz desafios significativos à autenticidade e proteção de imagens e vídeos. Técnicas ativas, como marcas d'água digitais e assinaturas digitais, são empregadas para garantir a integridade desde a origem até o consumo desse tipo de conteúdo. As abordagens passivas analisam características intrínsecas dos arquivos para detectar adulterações, sem a necessidade de informações previamente incorporadas. Este trabalho apresenta uma revisão bibliométrica e sistemática sobre essas técnicas de autenticação e proteção desses conteúdos, classificadas em abordagens ativas e passivas. Por meio de métodos quantitativos e qualitativos, foram analisadas tendências e padrões da produção científica, evidenciando a evolução das técnicas e suas aplicações práticas. Este estudo busca consolidar conhecimentos na área, oferecendo subsídios para pesquisas futuras e avanços tecnológicos na autenticação e proteção de mídias digitais.

Palavras-chave: Proteção de Conteúdo. Revisão Sistemática. Revisão Bibliométrica. Técnicas Ativas. Técnicas Passivas.

ABSTRACT

The growing ease of digital media manipulation has brought significant challenges related to the authenticity and protection of images and videos. Active techniques, such as digital watermarks and digital signatures, are employed to ensure integrity from origin to consumption. Meanwhile, passive approaches analyze intrinsic characteristics of files to detect alterations without requiring pre-embedded information. This work presents a systematic and bibliometric review of the techniques for authentication and protection of these contents, categorized into active and passive approaches. Through quantitative and qualitative methods, trends and patterns in scientific production were analyzed, highlighting the evolution of techniques and their practical applications. This study aims to consolidate knowledge in the field, providing a foundation for future research and technological advancements in the authentication and protection of digital media.

Keywords: Content Protection. Systematic Review. Bibliometric Review. Active Techniques. Passive Techniques.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

A manipulação de mídias digitais faz parte do cotidiano das pessoas, com implicações nas áreas da justiça, indústria, educação e política. Devido a ascensão das tecnologias de aprendizagem profunda, como as redes generativas recorrentes (CAMACHO; WANG, 2021; WU; SUN, 2021), ferramentas para adulteração e produção de novos conteúdos de mídia tornaram-se populares. Técnicas automáticas para embelezar rostos, alterar expressões faciais, idade e o estilo visual de fotografias, por exemplo, disponíveis para download em diversos aplicativos para download ou inseridas em dispositivos portáteis (KORUS, 2017b). Entretando, esses algoritmos também possibilitam criar mídias replicando características faciais, gestuais e vocais, tornando a autenticação, proteção e identificação de fraudes nesses conteúdos ainda mais desafiadora devido a ploriferação massiva dessas mídias (MARAS; ALEXANDROU, 2019). Neste contexto, a autenticação e proteção das imagens e vídeos surgiram como uma necessidade para garantia da proteção e confiabilidade desses conteúdos.

As técnicas de autenticação e proteção de imagens são classificadas como ativas ou passivas (KORUS, 2017b; SABER *et al.*, 2020). A primeira é utilizada, principalmente para a proteção das imagens desde sua origem até o seu consumo, enquanto a segunda para a detecção de adulterações ou falsificações em situações em que não há informações adicionais suficientes a respeito do conteúdo original. A autenticação ativa apresenta multiplas estratégias, destacando-se como principais as assinaturas digitais e as marcas d'água. Já na abordagem passiva, técnicas de análise do conteúdo são usadas para detectar falsificações em imagens a partir de diversos meios, sendo as principais, Detecções baseadas em geometria, física, pixels, formato e câmera (SABER *et al.*, 2020; LIN *et al.*, 2018).

As pesquisas em autenticação e proteção das imagens e vídeos estão em rápida evolução, trazendo como desafio compreender suas tendências e impactos (FERREIRA; SILVA, 2019). Neste contexto, desenvolve-se uma revisão bibliográfica dessas áreas de pesquisa a partir dos métodos de revisão sistemática e bibliométrica . A revisão bibliométrica fornece dados objetivos sobre a quantidade, qualidade, impacto e tendências através de métodos matemáticos e estatísticos (RIBEIRO, 2022), enquanto a revisão sistemática possiblita uma visão abrangente da área de pesquisa (LAPEI *et al.*, 2022) a partir da leitura e da síntese dos estudos considerados relevantes, mediante critérios de busca pré-estabelecidos.

O objetivo geral deste trabalho é realizar levantamento bibliográfico das pesquisas de autenticação e proteção de imagens e vídeos através de técnicas de bibliometria. Foram

escolhidos como objetivos centrais, a elucidação da evolução e tendências da área de pesquisa de autenticação e proteção de imagens e vídeos e o estabelecimento de uma avaliação quantitativa estatística para a coleta de dados bibliográficos, voltados à pesquisa de autenticação e proteção de imagens e vídeos, possibilitando uma análise estruturada. Buscou-se assim estabelecer uma base sólida para tomada de decisões e planejamento de pesquisas na análise da produção científica.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta uma síntese de artigos selecionados a partir das bases de dados Web of Science[1] e Scopus[2], reconhecidas pela comunidade científica por sua robustez e abrangência. Essa síntese fornecerá a fundamentação necessária para a compreensão dos temas que foram abordados, bem como para as análises subsequentes que foram conduzidas na revisão bibliométrica. Para ambas as abordagens de revisão, sistemática e bibliométrica, palavras-chave foram previamente definidas, orientando assim a seleção dos artigos sintetizados com base nesses termos.

2.1 Revisão Sistemática

A revisão sistemática é uma metodologia de pesquisa que tem ganhado crescente relevância na ciência contemporânea devido à sua capacidade de compilar e analisar grandes volumes de dados de estudos pré-existentes. Diferente das revisões tradicionais, que frequentemente são subjetivas e suscetíveis a vieses, a revisão sistemática utiliza métodos explícitos e rigorosos que minimizam o viés, proporcionando conclusões mais confiáveis e robustas. Este tipo de revisão integra e resume os resultados de múltiplos estudos originais, oferecendo uma visão mais abrangente sobre o tema investigado (DONATO, 2019).

Uma condução de uma revisão sistemática exige um planejamento meticuloso e uma execução rigorosa, respeitando os critérios metodológicos. A clareza e a transparência em cada etapa do processo são fundamentais para que as revisões sistemáticas cumpram seu papel de oferecer o mais alto nível de evidência para a prática baseada em evidências (MARTIMBIANCO, 2021). Entretanto, sua condução não está isenta de desafios. O processo é demorado e complexo, exigindo uma quantidade significativa de tempo, dependendo da disponibilidade e do volume de literatura relevante. Para que essa revisão seja bem-sucedida, é essencial que o estudante ou pesquisador possua habilidades de registro de dados, computacional, competências em busca bibliográfica e capacidade de avaliação crítica. Além disso, o acesso a bases de dados eletrônicas e a colaboração com especialistas, como bibliotecários e revisores independentes, são fatores críticos para o sucesso do processo (HAM-BALOYI, 2016).

A revisão deve ser fundamentada em uma pergunta de pesquisa clara e estruturada,

[1] $https://clarivate.com/academia-government/scientific-and-academic-research/research-discovery-and-referencing/web-of-science/$

[2] https://www.scopus.com/

para guiar seus processos. Estruturas como PICO (População, Intervenção, Comparação, Resultados), PECO (População, Exposição, Comparador, Resultados) ou PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) são frequentemente utilizadas para formular perguntas específicas, especialmente no contexto de ensaios clínicos e estudos observacionais (SCHIAVENATO; CHU, 2021; SINA; NAZEMI, 2022). A clareza na formulação da pergunta é essencial para determinar os critérios de elegibilidade dos estudos primários que serão incluídos na revisão (MARTIMBIANCO, 2021). A conclusão de uma revisão sistemática deve refletir sua capacidade em responder à questão de pesquisa original e discutir a força das evidências encontradas (DONATO, 2019).

A revisão sistemática, quando conduzida com os recursos adequados e orientação competente, pode aprimorar significativamente a qualidade da pesquisa e da educação, gerando impactos positivos diretos no âmbito educacional. Esta fundamentação tem em vista destacar a importância dessa metodologia como uma ferramenta válida e eficaz no campo da educação (HAM-BALOYI, 2016). Assim, ela se apresenta como uma ferramenta útil para a construção de conhecimento científico, permitindo uma análise detalhada e integrada da literatura disponível, e contribuindo de forma significativa para práticas baseadas em evidências (DONATO, 2019).

2.2 Revisão Bibliométrica

Estudos bibliométricos desempenham um papel importante por fornecer uma visão geral detalhada da produção científica em temas específicos. A análise bibliométrica possibilita a identificação de padrões de publicação, autores de destaque, palavras-chave recorrentes e a distribuição de artigos por país e campo do conhecimento. Essas análises são realizadas com base em dados extraídos de bases acadêmicas amplamente reconhecidas pela comunidade científica, como Scopus e Web of Science, geralmente cobrindo publicações em intervalos de tempo que podem ser definidos pela própria base ou pelo usuário. O objetivo dessas pesquisas é identificar aumentos significativos no número de publicações, examinar suas influências e detectar possíveis casos de influência sobre outras pesquisas, facilitando uma maior dedicação dos pesquisadores à produção científica. Destacando também a importância de softwares como VOSviewer[3] e Bibliometrix[4] na criação de mapas, visualização de redes de autores e exploração da fragmentação das linhas de pesquisa, auxiliando no mapeamento científico (COSTA CAMILA

[3] https://www.vosviewer.com/
[4] https://www.bibliometrix.org/home/

GOMES DANTAS, 2022; COSTA ARTHUR PINHEIRO DE ARAúJO COSTA, 2022).

Essa análise permite mapear e avaliar as tendências de pesquisa em relação à aplicação específica de um estudo, identificando os países com maior número de publicações e citações, além de ressaltar os autores mais influentes na área que tiveram contribuições significativas para o desenvolvimento do campo de pesquisa em foco. As palavras-chave utilizadas devem refletir os principais focos das investigações na área. A análise também destaca a relevância da colaboração internacional, identificando os países que lideram parcerias de pesquisa com outros. Além disso, ela revela quais temas, sejam eles consolidados ou recentes, estão ganhando relevância na pesquisa científica, promovendo o desenvolvimento para essas áreas. Assim, a análise bibliométrica constitui uma base para identificar as principais tendências, lacunas e oportunidades de pesquisa na aplicação científica (COSTA CAMILA GOMES DANTAS, 2022).

2.3 Trabalhos Relacionados

A evolução acelerada das tecnologias da informação nas últimas décadas revolucionou a forma como dados e informações são criados, manipulados e compartilhados globalmente. Esta transformação digital, embora tenha trazido inúmeros benefícios, também apresentou desafios significativos em termos de segurança, autenticidade e integridade dos dados. A área forense de proteção e autenticação digital surge como um campo crítico na intersecção da tecnologia da informação, direito e segurança cibernética, dedicado ao desenvolvimento de métodos para a análise, recuperação e autenticação de dados digitais (STAMM *et al.*, 2013; KUMAR; SRIVASTAVA, 2019; SHI *et al.*, 2023a).

Seu principal objetivo é identificar, preservar, recuperar e analisar dados em meios digitais, garantindo que a informação seja mantida em sua forma mais original e que possa ser utilizada como prova legítima em processos judiciais. Este campo não se limita apenas ao recolhimento de provas digitais após incidentes de segurança, mas também à prevenção de crimes e fraudes através de técnicas proativas de monitoramento e análise (WANG *et al.*, 2009a; CHENNAMMA; MADHUSHREE, 2023).

Os profissionais da área enfrentam diversos desafios, incluindo a volatilidade dos dados digitais, a variedade e a complexidade dos dispositivos e sistemas operacionais, além da crescente sofisticação das técnicas utilizadas por indivíduos mal-intencionados para ocultar ou apagar informações. Para superar esses obstáculos, a forense digital emprega uma gama de metodologias, **Análise de Dispositivos**, examinando sistemas de computadores, dispositivos

móveis e redes, os profissionais utilizam softwares especializados para recuperar arquivos deletados, logs de sistema e outras formas de dados residuais, **Criptografia e Análise de Segurança**, ferramentas de descriptografia e técnicas de quebra de segurança são aplicadas para acessar dados protegidos e criptografados, **Recuperação de Dados**, métodos avançados são utilizados para recuperar informações de dispositivos danificados ou formatados (STAMM *et al.*, 2013; RAJ; SHREELEKSHMI, 2021; CHENNAMMA; MADHUSHREE, 2023).

Com o avanço contínuo das tecnologias digitais, a área forense também precisa evoluir. O desenvolvimento de novas ferramentas forenses que podem eficientemente processar grandes volumes de dados e lidar com novos tipos de dispositivos é fundamental. Além disso, a colaboração internacional entre agências de aplicação da lei, o setor privado e acadêmico é vital para o avanço das práticas forenses e para garantir a segurança e a confiança no espaço digital (SHI *et al.*, 2023a; KAUR *et al.*, 2024). A forense de informação digital desempenha um papel indispensável na manutenção da lei e da ordem na sociedade digitalizada de hoje. À medida que enfrentamos desafios crescentes de crimes cibernéticos e questões de privacidade, o campo continuará a ser um ponto de interesse crítico para inovação tecnológica e cooperação global (KUMAR; SRIVASTAVA, 2019; SHI *et al.*, 2023a).

A tabela 1, mostra a variedade de artigos que podem ser encontrados para um estudo amplo de pesquisas na área, seus conteúdos e visões servem de grande compreendimento para manter atualizado a situação que a sociedade se encontra atualmente, os mais antigos se mostrando corretos ao expressar preocupações e análises para estudos futuros e os mais recentes se auto complementam a médida que um tipo de conteúdo é a evolução de um anterior.

Tabela 1 – Artigos para conhecimento de amplo espectro

Artigos	**Palavras-Chave**	**Referência**
Recent Advances in Digital Multimedia Tampering Detection for Forensics Analysis	Investigação digital Manipulação de multimídia Processamento de imagem e vídeo Mineração de dados Reconhecimento de padrões Taxonomia Pesquisa.	(BOUROUIS *et al.*, 2020)
Digital image forgery detection using passive techniques: A survey	Detecção de falsificação de imagem passiva/cega Forense de imagem Detecção de manipulação de imagem Autenticação de imagem Detecção de adulteração de imagem	(BIRAJDAR; MANKAR, 2013)
Image forgery detection: a survey of recent deep-learning approaches	Detecção de falsificação de imagens Forense de imagens Aprendizado profundo Cópia-mover Emendas DeepFake Pesquisa.	(ZANARDELLI *et al.*, 2023)
Review of Image Forensic Techniques Based on Deep Learning	Forense de imagem Detecção de falsificação de imagem Marca d'água robusta em imagem Aprendizado profundo	(SHI *et al.*, 2023a)

Fonte: Feita pelo autor

As proteções e autenticações vão desde análises ativas utilizando métodos que atuam diretamente no arquivo, como técnicas pássivas que possuem uma complexidade muito maior porém com resultados eficientes para os problemas nos quais são encontrados atualmente, tecnicas ativas mesmo estando em decaimento ainda se fazem uteis no cotidiano de muitos profissionais e até mesmo de simples usuários que não necessitam de conhecimentos especificos para proteger suas informações, algoritmos e programas gratuitos para a implementação de uma marca d'água ou de uma assinatura já são ofertados de forma abrangente.

2.3.1 Ativos

A marca d'água digital é uma técnica sofisticada e crucial utilizada em diversas áreas, se adpatando tanto para proteção de direitos autorais, autenticação de conteúdo e verificação de integridade. Essa tecnologia permite a incorporação de informações invisíveis ou perceptíveis em conteúdos de multimídia, como imagens e vídeos digitais, sem alterar significativamente a percepção do conteúdo original para o usuário final. Dessa forma essa técnica desempenha um papel fundamental na investigação forense, se aplicando à informações, segurança digital, forense digital e em campos críticos como medicina, direito, política e jornalismo, nos quais a autenticidade e a integridade desse tipo de conteúdo tem implicações significativas.

Inicialmente, suas técnicas tinham em vista robustez, assim incorporando impressões digitais rastreáveis para identificar a origem e a propriedade do conteúdo digital. Posteriormente, elas evoluíram para diferenciar entre impressões digitais intrínsecas e extrínsecas. As impressões digitais intrínsecas referem-se a características inerentes ao próprio conteúdo multimídia, incorporadas durante o processo de criação, como variações sutis na cor ou brilho, que permitem a identificação do conteúdo original sem a adição de informações externas.

Em contraste, as impressões digitais extrínsecas são informações adicionais inseridas deliberadamente no conteúdo, como códigos ou marcas d'água invisíveis, projetadas para rastreabilidade e verificação de origem. Essa evolução permitiu abordagens mais sofisticadas e específicas para a marcação d'água. Essas impressões digitais se tornaram ferramentas essenciais na análise forense, contribuindo para a identificação do histórico de processamento e a origem dos arquivos multimídia.

Em campos como o médico e o legal, as marcas d'água frágeis são um foco central, pois são altamente sensíveis a qualquer tipo de alteração, permitindo assim a detecção precisa de adulterações. Tais técnicas são fundamentais para garantir que o conteúdo digital seja

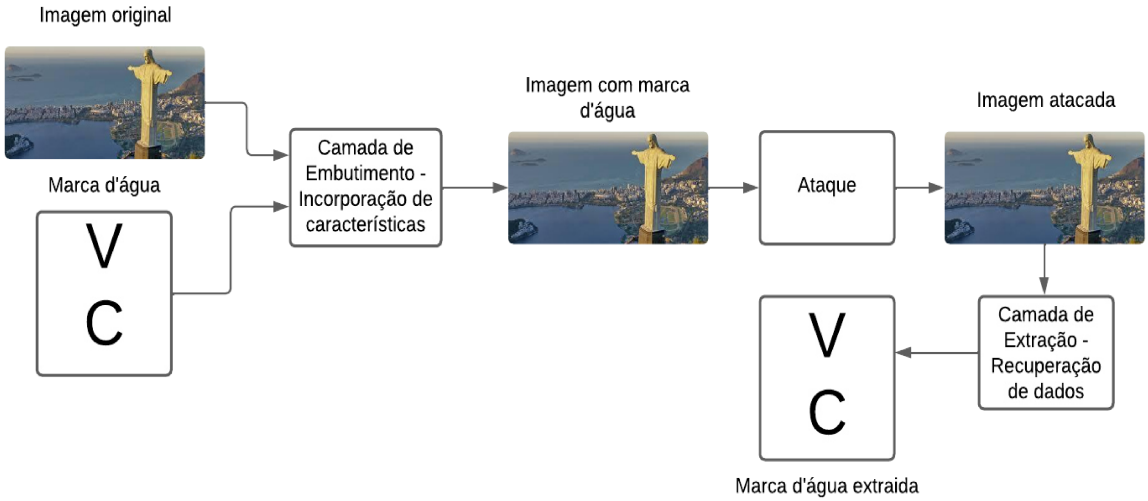
confiável e que sua origem seja verificável, dessa forma auxiliando na prevenção de diagnósticos incorretos, julgamentos equivocados, crises políticas e a disseminação de notícias falsas. Porém o desenvolvimento dessas técnicas enfrentam desafios contínuos, especialmente em relação à imperceptibilidade, robustez e resistência a ataques. Pesquisas estão em constante andamento para explorar novas abordagens, como a incorporação de informações em sinais multimídia e a luta contra ataques de colusão, visando aprimorar a segurança e a confiabilidade da marca d'água (RAJ; SHREELEKSHMI, 2021).

Marcas d'água consistem na variação da incorporação no arquivo multimidia em questão. São adaptadas para serem robustas contra ataques e manipulações, garantindo a integridade e a autenticidade do conteúdo digital (STAMM *et al.*, 2013). A marca d'água digital é, portanto, um dos centros na análise forense digital, proteção de conteúdo e verificação de autenticidade. À medida que a tecnologia e os métodos de ataque se tornam mais sofisticados, a importância de técnicas avançadas e seguras precisam continuar crescendo. O compromisso com a pesquisa e o desenvolvimento nessa área é crucial para assegurar a integridade e a confiabilidade do conteúdo digital em uma variedade de aplicações práticas (EL-SHAFAI *et al.*, 2023).

Os exemplos apresentados a seguir ilustram dois tipos de abordagem de marcas d'água digitais. A Figura 3 representa um framework básico de uma marca d'água robusta do tipo end-to-end (ponta a ponta), que se baseia em três etapas principais: embutimento, ataque e extração. Na etapa de embutimento, características relacionadas à robustez da marca são extraídas e aprimoradas, na etapa de extração, a marca é recuperada e sua integridade e autenticidade são avaliadas após a aplicação do ataque simulado. O ataque, por sua vez, é utilizado para treinar um modelo gerador de marcas d'água, com o objetivo de aumentar sua robustez, comparando a marca inicial com a final.

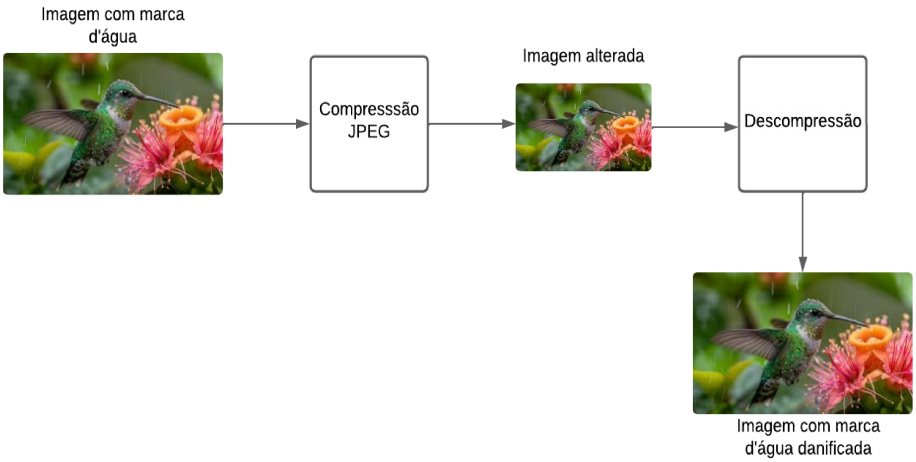
A Figura 2 apresenta uma abordagem tradicional, na qual a marca d'água é embutida na imagem e posteriormente submetida a uma compressão e recuperação. Embora este método seja mais simples, ele pode ser eficaz em situações onde o responsável pela adulteração desconhece a existência da marca. Nesse caso, a análise da marca permite identificar se a imagem foi manipulada ou não.

Figura 1 – Marca d'água robusta ponta a ponta



Fonte: Adaptada de (SHI *et al.*, 2023b)

Figura 2 – Marca d'água tradicional



Fonte: Adaptada de (SHI *et al.*, 2023b)

A tabela 2, mostra outros artigos que serviram como objetos de estudo para o entendimento geral e específico sobre marcas d'água.

Tabela 2 – Artigos utilzados para análise de marca d'água

Artigos	**Palavras-Chave**	**Referência**
A Survey of Passive Image Tampering Detection	Adulteração de imagem Detecção de adulteração de imagem Processo de imagem Modelo de imagem	(WANG *et al.*, 2009b)
Review of image forensic techniques based on deep learning	Forense de imagem Detecção de falsificação de imagem Marca d'água robusta em imagens Aprendizado profundo	(SHI *et al.*, 2023b)

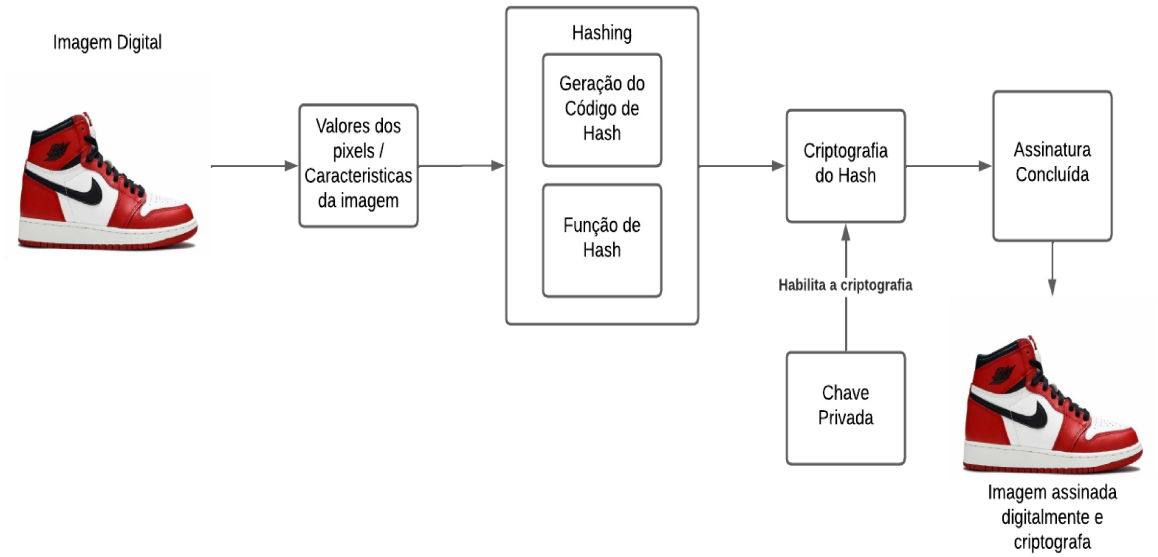
Fonte: Feita pelo autor

Assinatura digitais por sua vez, é uma técnica criptográfica que se utiliza de um conjunto de operações matemáticas para garantir a autenticidade e integridade de dados digitais, como documentos, mensagens e imagens. Esse método é fundamental em sistemas de comunicação e arquivamento, onde a segurança e verificação de dados são cruciais. Uma assinatura é baseada na criptografia de chave pública, que envolve um par de chaves criptográficas, uma privada e uma pública. A chave privada é usada para gerar a assinatura, enquanto a chave pública permite a qualquer pessoa verificar se a assinatura é válida. O processo se divide em duas etapas principais, assinatura e verificação.

A assinatura consiste em dois processos, Hashing e Criptografia do Hash. No Hashing primeiramente, calcula-se o hash sendo um resumo criptográfico dos dados a serem assinados. O hash é uma sequência de bytes com tamanho fixo que parece aleatória sendo praticamente único para cada conjunto de dados. Na Criptografia do Hash ele é então criptografado com a chave privada do signatário. O resultado é a assinatura digital, que é anexada aos dados originais. Diferente do processo de assinatura a Verificação consiste em três processos sendo, Decifrar Assinatura, Hashing dos Dados e Comparação.

Ao decifrar uma assinatura, a assinatura é decifragem usa a chave pública do signatário, em hashing dos dados o hash dos dados originais é recalculado e na Comparação o hash decifrado e o hash recalculado são comparados. Se forem iguais, a assinatura é considerada válida, o que significa que os dados não foram alterados após a assinatura e que a identidade do signatário está confirmada (CHENNAMMA; MADHUSHREE, 2023).

Figura 3 – Procedimento da geração de uma assinatura digital



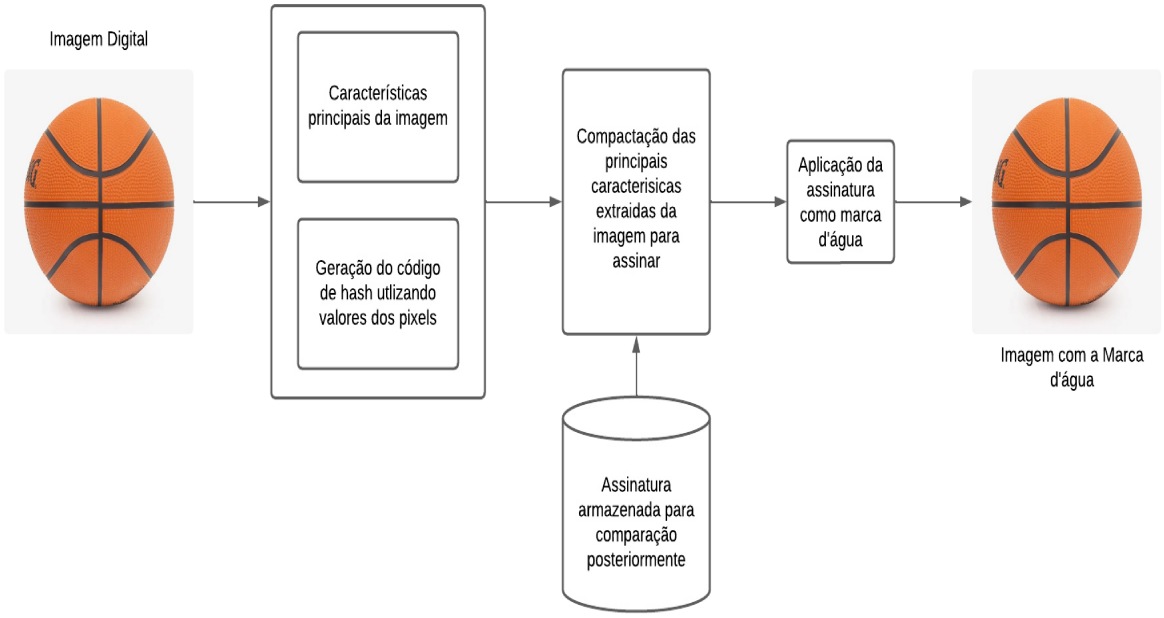
Fonte: Adaptada de (CHENNAMMA; MADHUSHREE, 2023)

As assinaturas digitais são utilizadas em diversos contextos. Documentos eletrônicos que garantem a autenticidade de contratos e documentos legais, em Softwares para confirmar que se a assinatura baixada não seja alterada ou verificar se foi alterada. Utilizada também em Transações Online para a segurança de operações bancárias e compras na internet. Porém sua implementaçã requer alguns requisitos. Uma Infraestrutura de Chave Pública, também sendo denominado por PKI, um Sistema para gerar e gerenciar chaves criptográficas e Certificados Digitais, que são documentos eletrônicos que utilizam a PKI para vincular chaves públicas a entidades, sendo, pessoas, organizações ou dispositivos, sendo assinados por alguma Autoridade Certificadora (CHENNAMMA; MADHUSHREE, 2023).

Assim como em marcas d'água, assinaturas digitais também possuem suas limitações e desafios, a Gestão de Chaves é uma delas, pois a segurança depende das chaves criptográficas utilizadas. A perda ou comprometimento da chave privada pode resultar em uma quebra de segurança. Possuindo uma Complexidade Computacional, devido o processo de criação e verificação de assinaturas digitais sendo computacionalmente intenso, impactando o desempenho de sistemas em tempo real. A Figura 4 demonstra o que pode ser encontrado como técnica híbrida, que consiste em aplicar uma assinatura como marca d'água, uma assinatura é gerada a partir de uma imagem e inserida como marca, evitando o envio separado delas. A interoperabilidade é algo bastante discutido pois por existir diferentes sistemas de assinatura digital e PKI causando problemas de compatibilidade, o que dificulta a interoperabilidade entre sistemas (BIRAJDAR;

MANKAR, 2013).

Figura 4 – Procedimento da geração do método híbrido



Fonte: Adaptada de (CHENNAMMA; MADHUSHREE, 2023)

A assinatura digital é uma tecnologia robusta e útil para a segurança digital moderna, oferecendo proteção contra muitas formas de fraudes e falsificações digitais, dessa forma assinaturas digitais possuem propriedades definidas Autenticação, Integridade e Não repúdio. A autenticação confirma a identidade do signatário, a integridade assegura que os dados não foram alterados desde que foram assinados e o não repúdio impede que o signatário negue a autoria da assinatura (PANDEY *et al.*, 2016). No entanto, desafios como a gestão de chaves e a necessidade de uma infraestrutura complexa e segura precisam ser continuamente adicionados para maximizar sua eficácia e confiabilidade. Em combinação com outras medidas de segurança, como técnicas forenses passivas e ativas. Assinaturas são fundamentais para uma estratégia abrangente de segurança digital. (BIRAJDAR; MANKAR, 2013; CHENNAMMA; MADHUSHREE, 2023).

A tabela 3, mostra outros artigos que serviram como objetos de estudo para o entendimento geral e específico sobre assinaturas digitais.

Tabela 3 – Artigos utilzados para análise de assinaturas digitais

Artigos	**Palavras-Chave**	**Referência**
A Survey on Photo Forgery Detection Methods	Não disponíveis no artigo	(GURUNLU; OZTURK, 2018)
Passive forensics in image and video using noise features: A review	Forense de Imagens Forense de Vídeos Ruído Técnicas de Extração de Ruído Técnicas Forenses Passivas	(PANDEY *et al.*, 2016)

Fonte: Feita pelo autor

2.3.2 Passivos

As técnicas passivas de detecção de falsificações em imagens representam uma área fundamental da perícia digital, sendo vitais para garantir a autenticidade e a integridade das imagens em uma variedade de contextos. Essas abordagens são particularmente úteis em ambientes que carecem de marcas d'água digitais, assinaturas digitais ou outras formas preexistentes de autenticação, tornando-as aplicáveis em uma ampla gama de cenários, desde o cumprimento da lei até a mídia, sendo um elemento chave na segurança digital, na investigação forense e no jornalismo. As técnicas passivas de detecção de falsificações de imagens surgem como uma resposta robusta, operando sem a necessidade de marcas ou dados pré-incorporados nas imagens.

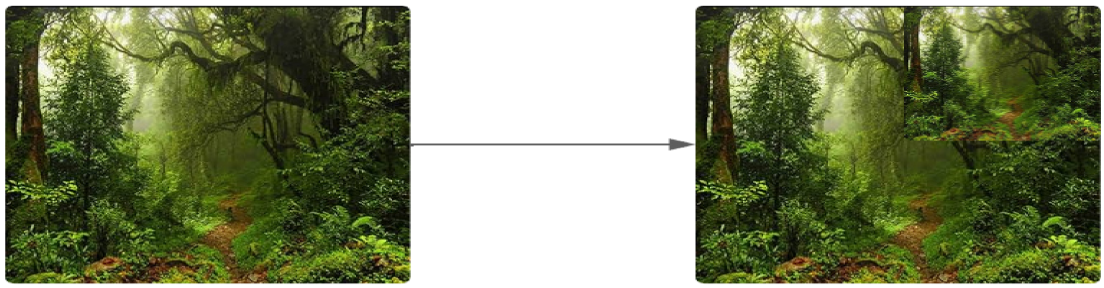
Também referidas como métodos cegos ou não intrusivos, as técnicas passivas independem de qualquer informação anteriormente incorporada à imagem. Esses métodos concentram-se em analisar as características intrínsecas das imagens, identificando sinais de manipulação que podem sugerir uma falsificação. Esta abordagem é particularmente vantajosa em situações onde as imagens provêm de fontes desconhecidas ou inverificável, utilizando assim a análise de inconsistências visuais para detectar adulterações sem a necessidade de acessar informações externas ou marcas pré-estabelecidas (SHARMA *et al.*, 2023; SHI *et al.*, 2023a). Essas técnicas concentram-se em diversos aspectos da imagem para determinar sua autenticidade. Algumas das abordagens mais comuns incluem:

- Detecção Baseada em Geometria: Analisa irregularidades nos elementos geométricos das imagens, como perspectiva e alinhamento de objetos, que podem sugerir manipulação.
- Detecção Baseada em Física: Concentra-se em inconsistências físicas, como iluminação e sombras incoerentes, que são difíceis de replicar corretamente em falsificações;
- Detecção Baseada em Pixels: Verifica irregularidades nos valores dos pixels, que podem revelar clonagem, movimentação de objetos dentro da imagem, ou alterações feitas por ferramentas de edição;

- Detecção Baseada em Formato: Foca em anomalias introduzidas pelo processo de compressão e edição, especialmente em formatos populares como JPEG, que podem deixar rastros estatisticamente detectáveis após a manipulação;
- Detecção Baseada em Câmera: Utiliza metadados da câmera e características específicas, como padrões de ruído do sensor, para identificar modificações na imagem (GUPTA *et al.*, 2022; SHARMA *et al.*, 2023; KORUS, 2017a).

As figuras apresentadas a seguir ilustram exemplos dos modelos mencionados. As Figuras 5 e 6 destacam exemplos relacionados às técnicas baseadas em pixels. Alterações de formato, frequentemente associadas a deepfakes, tornam-se cada vez mais realistas devido aos avanços nas tecnologias de deep learning e inteligência artificial. A Figura 7, por exemplo, exibe a transformação de um homem comum em uma imagem inicial para a mesma pessoa utilizando uma armadura, um exemplo simples, mas que, se utilizado de maneira inadequada, pode gerar sérios problemas. Além disso, variações físicas nem sempre são perceptíveis, especialmente quando as alterações são sutis e passam despercebidas por aqueles que desconhecem o conteúdo original. Na Figura 8, observa-se uma pintura de uma mulher segurando um animal. Na versão original, o animal apresenta uma determinada cor, enquanto na versão adulterada sua cor foi alterada, ilustrando a sutileza dessas manipulações.

Figura 5 – Exemplo copiar mover (*copy-move*)

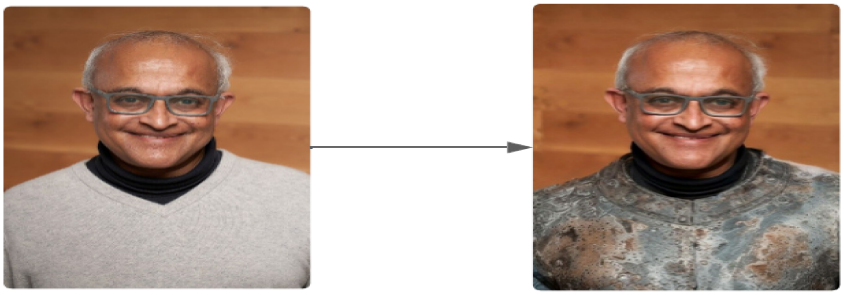


Fonte: Feita pelo autor

Figura 6 – Exemplo emenda (*splicing*)

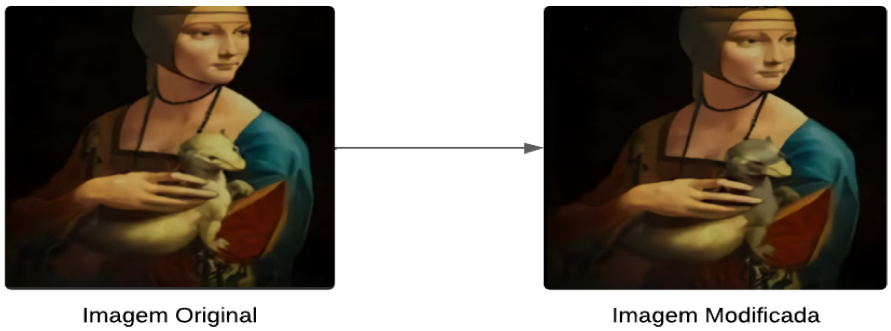
Fonte: Feita pelo autor

Figura 7 – Exemplo formato com *deepfake*



Fonte: Feita pelo autor

Figura 8 – Exemplo físico com variação de cor



Fonte: Feita pelo autor

A maior vantagem das técnicas passivas é sua aplicabilidade universal, podendo ser utilizadas em qualquer imagem independentemente de sua origem ou preparação prévia.

Isso é particularmente útil em cenários legais e jornalísticos onde a proveniência da imagem pode ser desconhecida ou não verificável (GUPTA *et al.*, 2022). Apesar de sua eficácia, as técnicas passivas enfrentam vários desafios. A complexidade e a qualidade das ferramentas de manipulação de imagens estão evoluindo rapidamente, o que exige constantes atualizações e melhorias nos métodos de detecção. Além disso, as altas taxas de falsos positivos e a necessidade de processamento computacional intensivo para analisar grandes volumes de dados são obstáculos significativos.

Pesquisadores estão focados em desenvolver algoritmos mais robustos e eficientes que possam se adaptar a novos tipos de falsificações e integrar técnicas avançadas de aprendizado de máquina para automatizar e aprimorar os processos de detecção (BIRAJDAR; MANKAR, 2013). A evolução contínua das técnicas de edição de imagens também introduz novos desafios, exigindo atualizações constantes dos métodos de detecção para manter sua eficácia. As técnicas passivas são essenciais em diversas áreas, incluindo segurança digital, forense, jornalismo e direito. Elas ajudam a assegurar a integridade da informação visual, protegendo indivíduos e organizações contra as consequências de imagens falsificadas (GUPTA *et al.*, 2022).

O futuro das técnicas passivas de detecção de falsificação de imagens incluirá a integração com tecnologias emergentes como inteligência artificial e aprendizado de máquina. Essas tecnologias prometem melhorar a capacidade de detectar manipulações sofisticadas, aumentando a confiabilidade e a eficiência dos processos de detecção (GUPTA *et al.*, 2022; KORUS, 2017a). As técnicas passivas de detecção de falsificações em imagens digitais são fundamentais para manter a credibilidade e a autenticidade do conteúdo visual em uma era digitalmente saturada. A contínua pesquisa e desenvolvimento nessa área é vital para acompanhar as rápidas mudanças nas tecnologias de manipulação de imagens, garantindo a segurança e a veracidade das informações visuais em diversos contextos (FARHAN *et al.*, 2024; GUPTA *et al.*, 2022; SHI *et al.*, 2023a).

A tabela 4, mostra outros artigos que serviram como objetos de estudo para o entendimento geral e específico sobre as técnicas passivas para proteção e autenticação de imagens e vídeos.

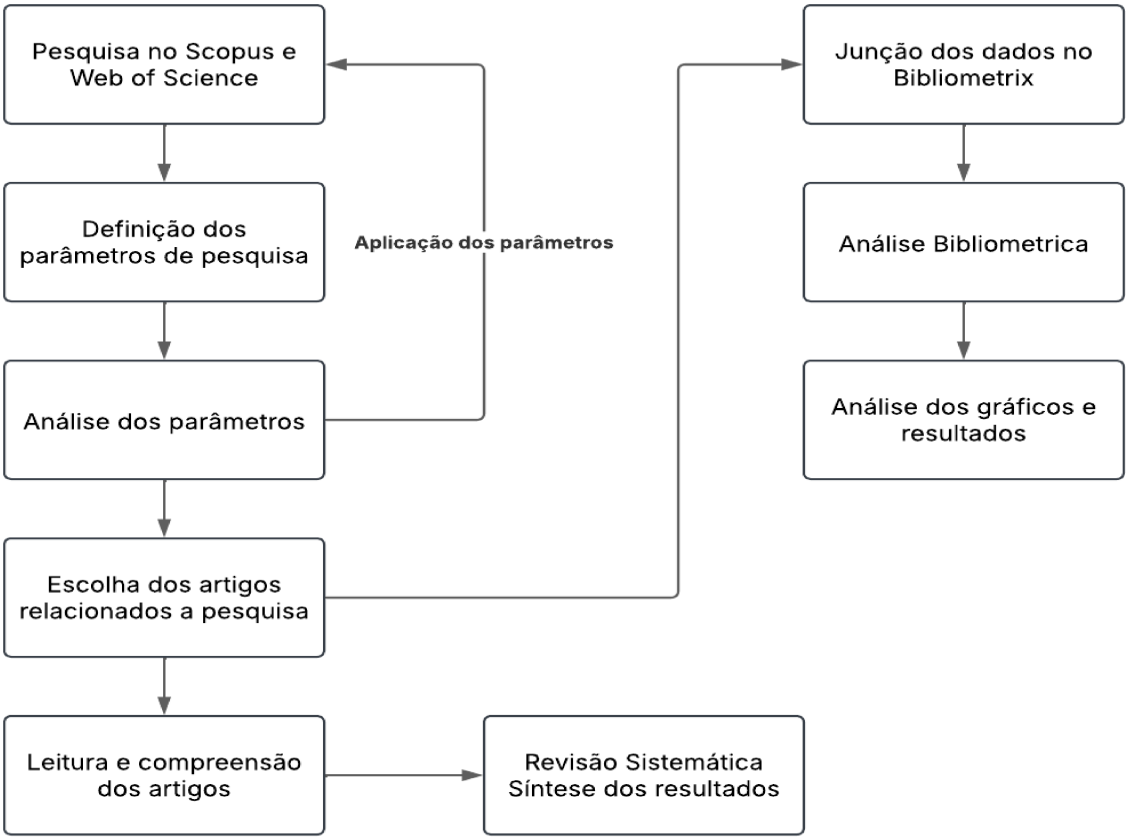
Tabela 4 – Artigos utilzados para análise de técnicas passivas

Artigos	**Palavras-Chave**	**Referência**
Passive Image Forgery Detection Techniques: A Review, Challenges and Future Directions	Imagem Digital Copiar-Mover Detecção Passiva de Falsificaçao de Imagens Emenda de Imagem	(KAUR *et al.*, 2024)
Image forgery detection based on physics and pixels: a study	Perícia de Imagens Digitais Manipulação de Imagens Falsificação Baseada em Física	(KUMAR; SRIVASTAVA, 2019)

Fonte: Feita pelo autor

3 METODOLOGIA

Figura 9 – Passos da metodologia



Fonte: Feita pelo autor

A revisão sistemática iniciou-se através das coletas de trabalhos nas bases científicas Web of Science e Scopus. Foram estabelecidos critérios para realização dessas coletas, em termos de materiais, como artigos, pesquisas e palavras-chave. As análises foram feitas a partir de métricas, como número de referências, palavras-chave, autores, coautores, ano de publicação, instituição, país e citações. Os trabalhos coletados foram selecionados com base nos critérios já estabelecidos anteriormente, seguidos por uma análise mais aprofundada dos textos completos, análise essa feita com base na leitura de artigos, escolhidos ao decorrer da execução do trabalho, que serviu para avaliar sua qualidade e relevância para a pesquisa.

A condução da revisão bibliométrica abrangeu uma série de etapas metodológicas, I. Encontrar um método de busca efetivo e conciso, II. Estabelecimento da string de busca nas bases e III. Encontrar o método mais eficiente para a análise dos dados. O tópico III sendo mais

específico para a Revisão Bibliométrica. Ao se estabelecer critérios de inclusão e exclusão dos estudos, determinando quais elementos se alinham diretamente aos objetivos da pesquisa. A extração dos dados pertinentes foi realizada numa análise para identificação de padrões, lacunas ou tendências que possam contribuir para a compreensão do tema. A análise de dados foram feitas através da linguagem R[1] e utilizando uma biblioteca disponível Bibliometrix.

3.1 Condução da Revisão Sistemática e Bibliométrica

3.1.1 I. Método de busca efetivo e conciso

Ao definir o foco principal do trabalho, tornou-se necessário coletar uma variedade de dados, incluindo artigos, revistas, trabalhos acadêmicos e outras pesquisas relevantes. As bases de dados utilizadas permitem consultas por meio de strings de busca que empregam lógica algébrica, como 'AND' e 'OR', ou símbolos matemáticos, como '+' e '-'. Essas strings facilitam a adição ou remoção de palavras-chave específicas, otimizando a inclusão ou exclusão de termos na busca.

3.1.2 II. Definição das strings de busca nas bases

O tema em questão abrange uma área ampla, o que torna o tempo necessário para a análise dos artigos impraticável, influenciando diretamente a eficácia da revisão sistemática. Para este trabalho, foram selecionadas três palavras-chave principais: 1. Tema amplo, 2. Tipo de pesquisa e 3. Palavra-chave específica. Um exemplo dessas categorizações seria: 1. Imagem Forense, 2. Pesquisa e 3. Marca d'água, que juntas direcionam o foco da investigação para áreas específicas dentro do campo mais amplo.

O tema amplo trabalha em torno do tema principal do tipo de trabalho, por exemplo, quando trata-se de sistemas de proteções e validações, uma área com afinidade a esse tema é a forense, dessa forma para este trabalho foi escolhido como tema amplo forense digital, devido a seguir um conceito de constante uso de ferramentas para análises de proteção e uso de técnicas para proteção. O tipo de pesquisa é adaptado para abranger não apenas um espectro amplo, por exemplo, ao inserir nas bases científicas forense digital, os resultados seriam bastante abrangentes.

Para focar especificamente nas pesquisas de proteção e autenticação foram seleci-

[1] https://www.r-project.org/

onadas palavras-chave pertinentes como 'Overview', 'Review', 'Survey', e 'Researches' para direcionar a busca de literatura relevante. Uma 'Review' analisa e sintetiza criticamente a literatura existente sobre um tema, identificando padrões e lacunas, com foco na qualidade e relevância das fontes, podendo ser narrativa, sistemática ou crítica. Já um 'Survey' coleta e apresenta dados de forma descritiva e quantitativa, abrangendo um número maior de estudos, mas com menos profundidade. A escolha das palavras-chave 'Marca d'água', 'Assinatura Digital', e 'Técnicas Passivas', objetiva enfatizar pontos específicos a serem discutidos no trabalho ou conceitos frequentemente mencionados em outras pesquisas, destacando-os como fundamentais para um estudo em questão.

3.1.3 III. Busca do método eficiente para a análise dos dados

Para a análise dos dados, foi necessário gerar gráficos a partir dos arquivos resultantes da pesquisa. Esses gráficos permitiram a identificação de padrões, lacunas e tendências, contribuindo significativamente para a compreensão do tema abordado. Para realizar tal análise, era imprescindível o uso de uma linguagem de programação capaz de produzir gráficos e compatível com arquivos de extensão .xlsx, além de ser de fácil compreensão para os analistas. As linguagens Java[2], Python[3] e R foram avaliadas, pois todas atendiam ao requisito de geração de gráficos. No entanto, a linguagem R foi escolhida por oferecer a melhor facilidade de compreensão para a execução deste trabalho específico.

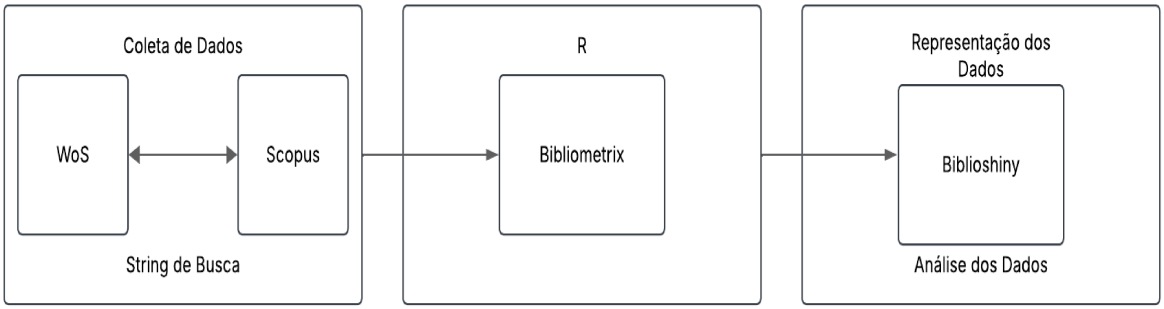
Essa possui uma biblioteca/pacote denominada Bibliometrix, que possibilita compreender as dinâmicas e estruturas dentro de campos científicos específicos e identificar as tendências emergentes e as influências predominantes na pesquisa acadêmica. Como pacote estatístico R, a Bibliometrix é voltada especificamente para a análise quantitativa de dados bibliográficos, sendo sua principal utilidade a capacidade de processar e analisar grandes volumes de dados bibliométricos, como aqueles derivados de bases de dados acadêmicas e científicas.

Além disso, o pacote Bibliometrix é acompanhado de uma interface gráfica de usuário, chamada Biblioshiny, que proporciona uma experiência mais acessível e menos técnica para os usuários que preferem uma interação mais visual com o software, desta forma ao exportar os dados exportados, que são padronizados pelas bases e em formato BibTex, das duas bases de dados com um conjunto de dados único, sendo cada conjunto uma junção das duas bases

[2] https://dev.java/
[3] https://www.python.org/

utilizando a mesma string de busca. Pode-se assim realizar análises, como, mapeamento de citações, análise de co-citação, análise de rede de colaboração entre autores, análise de tendências de publicação, e análise de palavras-chave.

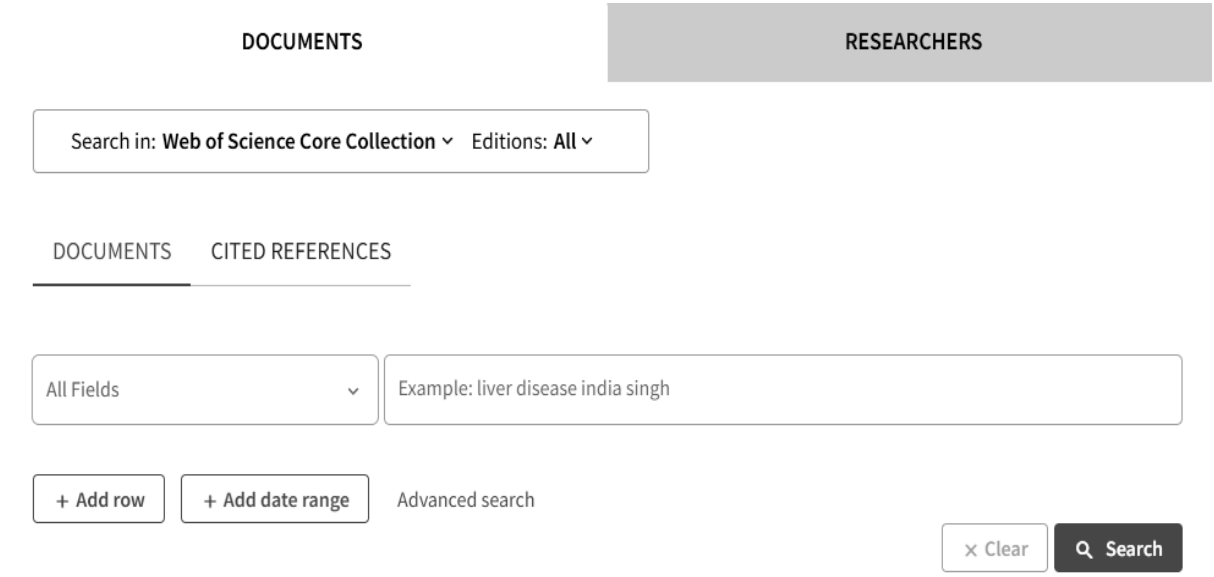
Figura 10 – Atribuição do conjunto de dados ao bibliometrix.



Fonte: Feita pelo autor

Os dados a serem inseridos e analisados no DataSet principal se deram de dois das quatro palavras-chave definidas anteriormente, sendo elas *Review* e *Survey*. Devido aos seus conceitos complementarem um ao outro, foram considerados necessários apenas esses duas para uma produção de resultados eficiente para este trabalho. Enquanto a 'Review' aprofunda-se na análise crítica, o 'Survey' prioriza a amplitude dos dados coletados. Ambos são importantes e complementares, dependendo dos objetivos da pesquisa. Outro detalhe foi a escolha dos textos analisados. Após a aplicação dos passos da metodologia foram escolhidos cerca de 30 artigos para o estudo da Revisão Sistemática, esses artigos contudo como a Bibliométrica abrangeu a área da pesquisa como um todo, dessa forma foram selecionados todos os arquivos disponiveis das bases com a aplicação das palavras-chaves. A Figura 9 demonstra os passos simplificados aplicados na metodologia e a Figura 11 mostra o local onde pode ser inserido a string nas bases.

Figura 11 – Local de inserção das strings no web of science



Fonte: Feita pelo autor

4 RESULTADOS

4.1 Busca nas bases

No decorrer da execução dos tipos de pesquisa, observou-se que a inclusão de palavras-chave específicas resultava em uma diminuição no volume de resultados. Essa redução foi crucial, pois permitiu um foco mais aguçado e um uso mais eficiente do tempo, garantindo que os resultados obtidos estejam estritamente relacionados ao objeto de estudo em vez de abrangerem um espectro mais amplo. As tabelas 5 e 6 a seguir mostram os resultados encontrados de acordo a string utilizada.

Tabela 5 – Strings de busca e resultados no web of science

Strings	**Resultados**	**Strings**	**Resultados**
Imagem Forense	11.642	Image Forensics	11.642
Imagem Forense + Pesquisa	306	Image Forensics + Survey	306
Imagem Forense + Pesquisa + Marca d'água	15	Image Forensics + Survey + Watermark	15

Fonte: Feita pelo autor

Tabela 6 – Strings de busca e resultados no scopus

Strings	**Resultados**	**Strings**	**Resultados**
(TITLE-ABS-KEY("imagem forense"))	2.355	(TITLE-ABS-KEY("image forensics"))	2.355
(TITLE-ABS-KEY("imagem forense") AND TITLE-ABS-KEY("marca d'agua"))	35	(TITLE-ABS-KEY("image forensics") AND TITLE-ABS-KEY("watermark"))	35
(TITLE-ABS-KEY("imagem forense") AND TITLE-ABS-KEY("marca d'água") AND TITLE-ABS-KEY("pesquisa"))	5	(TITLE-ABS-KEY("image forensics") AND TITLE-ABS-KEY("watermark") AND TITLE-ABS-KEY("survey"))	5

Fonte: Feita pelo autor

4.2 Revisão Sistemática

Com base nos estudos realizados a partir das sínteses dos artigos analisados, as abordagens de proteção e autenticação de imagens podem ser classificadas em duas categorias: ativas e passivas. As abordagens ativas requerem a inserção prévia de informações no arquivo desde sua criação, enquanto as passivas não possuem essa exigência. No contexto das abordagens ativas, destacam-se as marcas d'água e as assinaturas digitais, enquanto as abordagens passivas são classificadas principalmente com base em técnicas de detecção, devido à sua maior abrangência. No que se refere às técnicas ativas, observou-se que, embora sua aplicação tenha diminuído ao longo do tempo, estudos sobre o tema continuam sendo desenvolvidos, dada a relevância da integridade que essas técnicas proporcionam.

Dessa forma, observou-se que as marcas d'água são utilizadas para a proteção de direitos autorais e a autenticação de arquivos. Sua evolução ocorreu por meio de dois métodos principais: intrínsecos e extrínsecos. As marcas d'água intrínsecas são visíveis no arquivo, manifestando-se por meio de alterações de cor, brilho ou pela inserção de uma marca autenticada em determinada região da imagem. Já as marcas extrínsecas são imperceptíveis a olho nu, porém mais robustas, sendo aplicadas por meio de sistemas especializados. A aplicação das marcas d'água se estende a diversas áreas, como a medicina, o setor jurídico e o jornalismo.

No contexto médico, elas são essenciais para a verificação e proteção de laudos, prevenindo possíveis fraudes que poderiam acarretar consequências graves. Da mesma forma, são utilizadas na autenticação de petições legais e notícias, garantindo a veracidade das informações divulgadas. No entanto, as marcas d'água enfrentam desafios, sendo a imperceptibilidade um dos principais requisitos. Idealmente, mesmo que um arquivo seja editado, a marca d'água deve permanecer imperceptível, possibilitando sua autenticação. Além disso, é fundamental que seja resistente a ataques, de modo que não possa ser facilmente removida ou comprometida.

As assinaturas digitais são implementadas de forma distinta das marcas d'água, sendo baseadas no uso de um par de chaves criptográficas: uma chave privada e uma chave pública. O processo de assinatura ocorre por meio da chave privada, enquanto a verificação é realizada utilizando a chave pública. Esse mecanismo garante a autenticidade e a integridade do arquivo, impedindo alterações não autorizadas. A implementação das assinaturas digitais ocorre em três etapas principais: hashing, criptografia do hash e verificação. O hash pode ser gerado a partir de um conjunto de valores aleatórios convertidos em um único valor ou, pode representar características específicas da imagem transformadas em um identificador único. Esse valor resultante é então criptografado, e o arquivo recebe a assinatura digital. Para a verificação, a chave pública compara o hash gerado com o valor armazenado na assinatura. Caso os valores coincidam, o acesso ao arquivo é autorizado, caso contrário, o acesso é negado.

As assinaturas digitais são amplamente empregadas na proteção de softwares e na validação de documentos eletrônicos, garantindo sua autenticidade. No entanto, assim como as marcas d'água, enfrentam desafios. Um dos principais desafios é a gestão de chaves, pois a perda da chave privada pode resultar na impossibilidade de recuperar o arquivo assinado. Outro ponto crítico é a interoperabilidade, uma vez que diferentes sistemas podem utilizar métodos distintos de criptografia e descriptografia, o que pode causar incompatibilidades na verificação da assinatura.

As técnicas passivas, por não exigirem a inserção prévia de informações nas imagens, possuem um escopo mais amplo e abrangente, sendo amplamente utilizadas para a detecção de manipulações e fraudes. Essas técnicas podem ser classificadas em diferentes categorias de detecção, incluindo geometria, física, pixels, formato e câmera. Essas abordagens tornam as técnicas passivas altamente eficazes na detecção de edições e falsificações, sendo amplamente utilizadas em áreas como segurança digital, perícia forense e verificação de autenticidade de imagens.

Na geometria é analisado inconsistências em perspectivas e desalinhamento de objetos dentro da imagem, permitindo identificar alterações estruturais que possam indicar manipulação. A física examina aspectos como iluminação e sombras, verificando possíveis incoerências que possam sugerir modificações artificiais na imagem. Pixels identifica irregularidades como clonagem de partes da imagem ou remoção de elementos. Essa abordagem geralmente abrange uma grande parte das demais detecções, pois analisa diretamente a distribuição e a estrutura dos pixels. O formato foca nos padrões introduzidos por processos de compressão ou edição, permitindo detectar indícios de alterações feitas por softwares de edição e em câmera é avaliado as características do sensor da câmera, verificando se a imagem apresenta vestígios de manipulação que possam comprometer sua autenticidade.

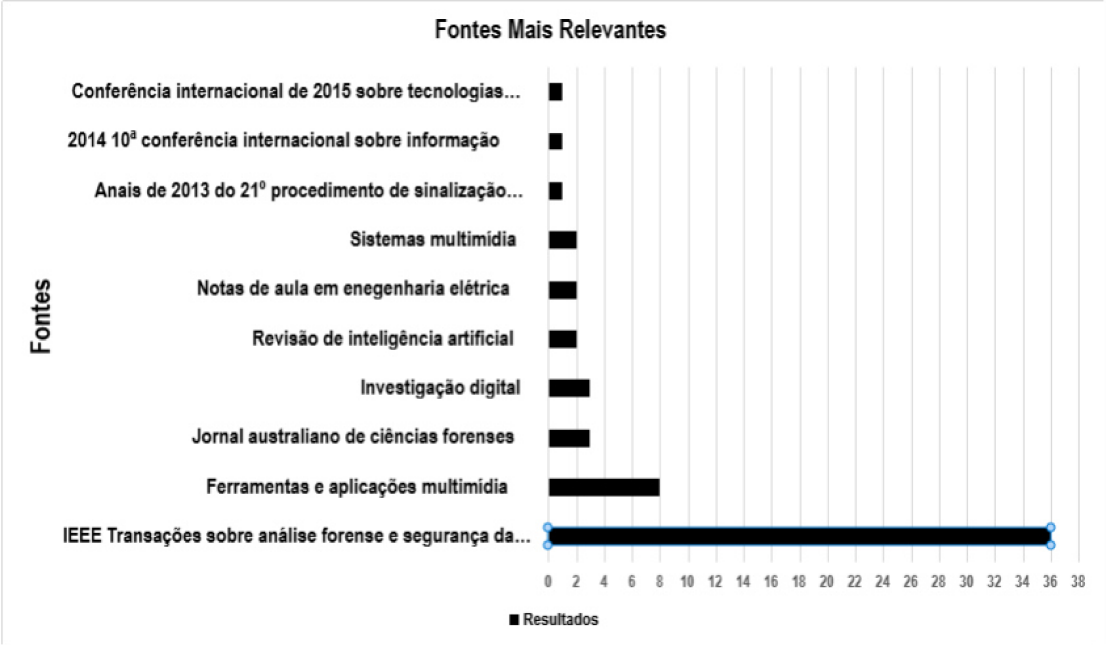
A abordagem passiva enfrenta desafios comparáveis às abordagens ativas, especialmente devido ao avanço contínuo das ferramentas de edição, que tornam as falsificações cada vez mais sofisticadas e difíceis de detectar. Embora as técnicas de análise tenham evoluído significativamente, ainda há um alto índice de falsos positivos, o que pode comprometer a confiabilidade dos resultados. Além disso, o custo operacional representa outro obstáculo relevante. Para garantir uma análise precisa e confiável, é necessário processar um grande volume de arquivos, o que exige alto poder de processamento e algoritmos otimizados. Esse fator pode impactar tanto o desempenho quanto o tempo necessário para a verificação, tornando essencial o desenvolvimento de métodos mais eficientes e automatizados para aprimorar a detecção de manipulações.

4.3 Revisão Bibliométrica

Os resultados apresentados a seguir foram gerados e extraídos diretamente do Biblioshiny, utilizando as bases de dados previamente explicadas. Conforme detalhado na seção de metodologia, a coleta de dados foi realizada por meio de quatro palavras-chave. No entanto, para a análise, optou-se por utilizar apenas duas dessas palavras-chave, 'Review' e 'Survey',

pois elas forneceram resultados pertinentes e concisos sobre o tema abordado. Assim como suas análises serão em torno de pesquisas como um todo, dentro da área de proteção e autenticação em imagens e vídeos.

Figura 12 – Fontes relevantes na área de autenticação e proteção de imagens



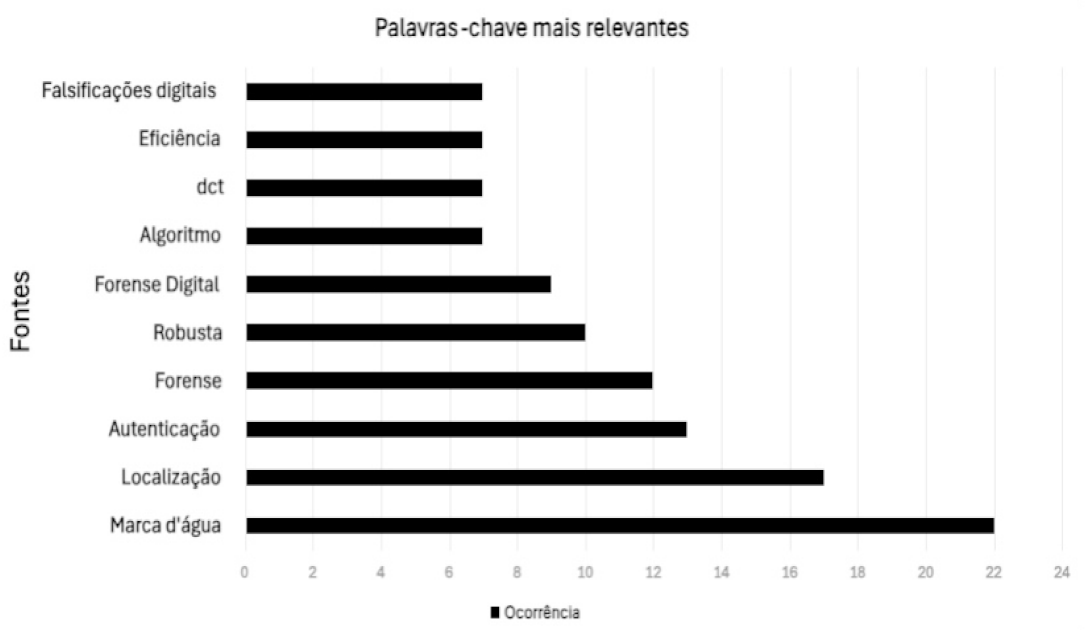
Fonte: Feita pelo autor

Na Figura 12 mostra a análise das fontes mais relevantes mostra que a distribuição dos documentos começou com contribuições isoladas em conferências de 2013, 2014 e 2015, cada uma com apenas um artigo publicado. A IEEE Transações sobre Análise Forense e Segurança da Informação emergiu como a principal fonte, acumulando 36 documentos ao longo do período analisado. Outras fontes, como Ferramentas e Aplicações Multimídia e o Jornal Australiano de Ciências Forense, também mostraram uma relevância, sendo um com 8 e 3 artigos respecitivamente. Embora não haja um padrão rígido, a um aumento na concentração de publicações em revistas especializadas, refletindo a importância crescente dessas fontes na disseminação de pesquisas sobre autenticação e proteção de imagens e vídeos.

Analisar as palavras-chave pode fornecer informações valiosas sobre as áreas de maior interesse e foco em uma determinada pesquisa. A Figuras 13 mostra que a palavra-chave marca d'água teve o maior número de ocorrências com 22 resultados, seguida por localização

com 17 e autenticação com 13 resultados, indicando que esses são os temas mais discutidos na literatura sobre autenticação e proteção de imagens e vídeos.

Figura 13 – Número de ocorrência de determinados palavras-chave



Fonte: Feita pelo autor

Outros termos relevantes incluem Forense com 12 resultados, Robusta com 10 e Forense Digital tendo 9. Esses termos sugerem que a robustez e a aplicação forense digital também são áreas de interesse significativo. Termos como Algoritmo, dct, Eficiência e Falsificações Digitais aparecem todos com 7 ocorrências cada, refletindo uma provável ênfase na eficiência e na detecção de falsificações digitais. Esses resultados destacam as áreas centrais de pesquisa e desenvolvimento na proteção e autenticação de conteúdo digital, com um foco particular em técnicas robustas e forenses que garantem a integridade e a autenticidade de imagens e vídeos.

A Tabela 7 mostra 10 autores presentes na literatura disponível a partir das métricas utilizadas, assim como o número de artigo ou trabalhos publicados, alguns dos trabalhos desses autores estao presentes neste trabalho, partindo para um mapa de relacionamento que destaca as diferentes áreas de foco e colaboração dos autores dentro do campo, refletindo a diversidade de abordagens e especializações entre os principais pesquisadores da área.

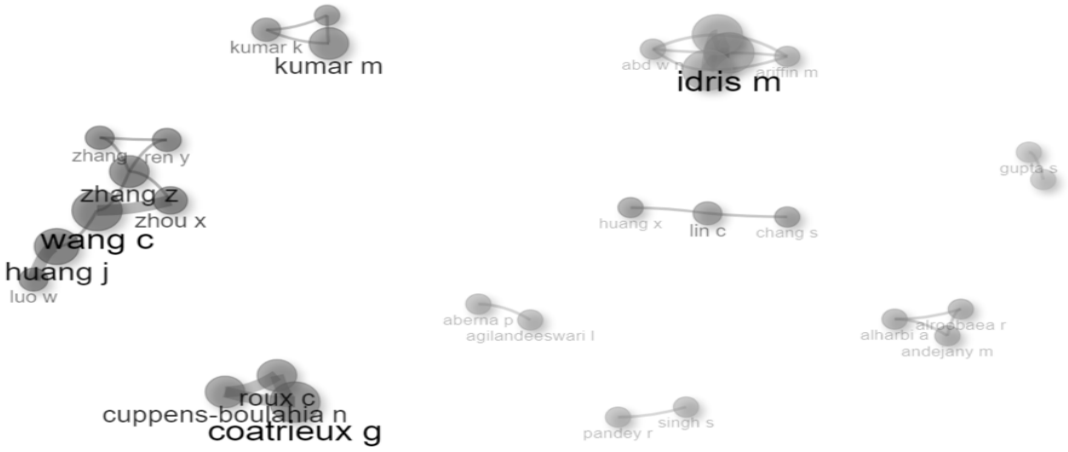
Tabela 7 – Autores relevantes na literatura

Autores	Nº Artigos
Coatrieux G	3
Huang J	3
Korus P	3
Kumar M	3
Wang C	3
Chang S	2
Cheng L	2
Cuppens-Boulahia N	2
Gupta S	2
Huang X	2

Fonte: Feita pelo autor

A Figura 14 mostra a análise da rede de relacionamento entre os autores foi realizada utilizando um software o Bibliometrix. A figura apresenta uma rede de autores distribuída em diferentes clusters. Um dos maiores grupos de autores conectados é composto por Zhang Z., Wang C., Huang J., entre outros, formando um cluster de grande relevância. Outro cluster significativo é liderado por Idris M., que se conecta com outros autores como Arifin M. e Abd W.. Esses cluteres maiores podem não conter autores com maior número de publicações, contudo isso não significa que ele é um autor de menos importância, apenas que ele está ligado na produção de determinados trabalhos, tendo sua relevância própia.

Figura 14 – Relacionamento entre autores no campo



Fonte: Feita pelo autor

A análise revela que há múltiplos clusters independentes, como o de Coatrieux G. e Cuppens-Boulahia N., e o de Kumar M., cada um operando em nichos específicos dentro da área

de pesquisa. Não há conexões diretas entre a maioria dos clusters, indicando que as colaborações entre esses grupos de autores são relativamente segmentadas, cada qual explorando aspectos específicos do campo de autenticação e proteção de imagens e vídeos.

A Tabela 8 apresenta a distribuição de documentos dos 5 principais países ou territórios em um intervalo de tempo entre os anos de 2005 a 2024. A China ocupa o primeiro lugar, com 759 documentos, seguida pela India, com 424 e os Estados Unidos, com 366 artigos publicados. Esses três países representam aproximadamente 84,55% de todos os documentos publicados sobre as pesquisas e produções científicas de análise em imagens digitais. Esse resultado provavelmente se justifica devido ao fato deles serem reconhecidos como as maiores potências do mundo, com mais investimentos em pesquisa. Além disso, destaca-se que foram considerados todos os tipos de documentos, não apenas artigos de periódicos.

Tabela 8 – Distribuição das produções por países

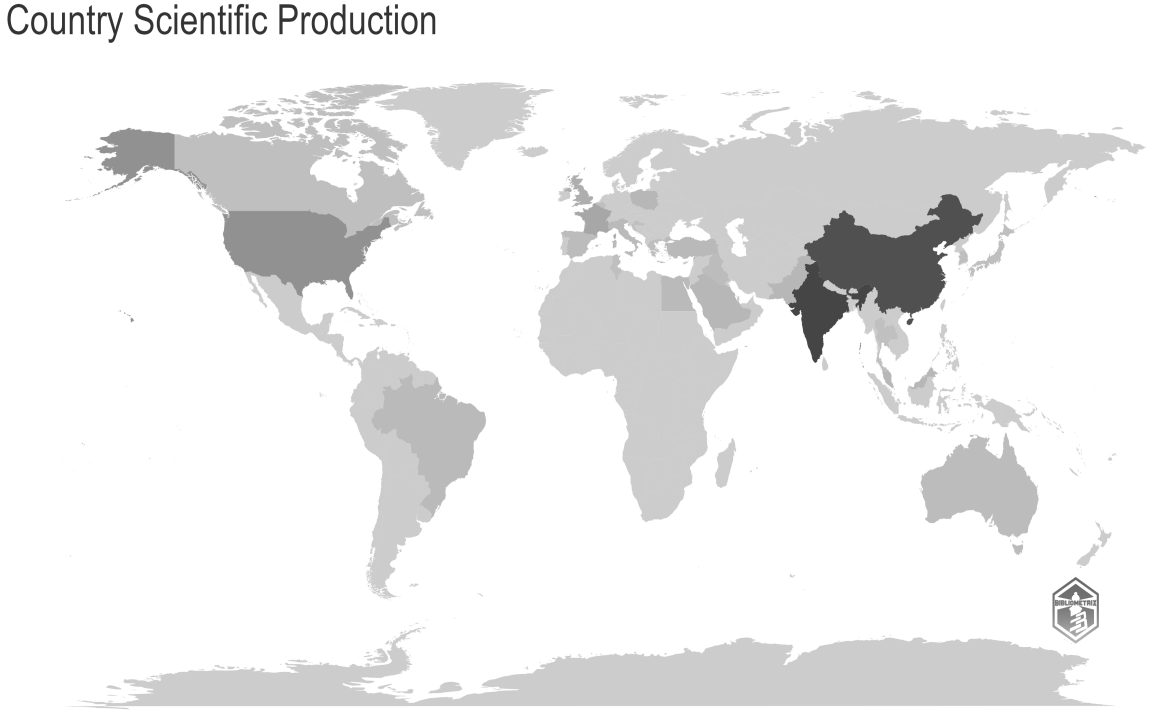
Países	**Nº Artigos**
China	759
França	177
India	424
Reino Unido	106
USA	366

Fonte: Feita pelo autor

A Figura 15 mostra a produção científica por país na área de autenticação e proteção de imagens e vídeos (destacados em escala de cinza). Observa-se que a maioria dos países com alta produção científica se encontra na América do Norte, Europa e Ásia. Como mencionado anteriormente, China e Índia destacam-se como os principais contribuidores, isso se da devido ao crescente investimento em pesquisa e tecnologia digital nesses países. América do Sul e África possuem poucos países com publicações na área, o que pode estar relacionado ao menor investimento em pesquisa e desenvolvimento tecnológico em comparação com nações mais desenvolvidas.

A disparidade dos resultados reflete uma desigualdade na produção científica global, indicando que o avanço na pesquisa de autenticação e proteção digital ainda é concentrado em regiões com maior capacidade econômica e tecnológica. Esse cenário demonstra a importância de promover a cooperação internacional e aumentar o suporte a pesquisadores em países em desenvolvimento, tendo em vista a redução de lacunas existentes e a ampliação do acesso a tecnologias avançadas de proteção digital.

Figura 15 – Produção científica por país



Fonte: Feita pelo autor

5 CONCLUSÕES

Este trabalho realizou um levantamento bibliográfico das pesquisas de autenticação e proteção de imagens através de técnicas de bibliometria. Dessa forma, foram estabelecidos objetivos específicos de elucidar a evolução e as tendências da área de pesquisa de autenticação e proteção de imagens e vídeos, estabelecendo sua importância, desafios e implicações e estabelecer uma análise quantitativa estatística para a coleta de dados bibliográficos, voltados à pesquisa de autenticação e proteção de imagens e vídeos, que possibilite sua análise estruturada. Evidenciou-se a relevância crescente das pesquisas em autenticação e proteção de imagens e vídeos em função da quantidade e relevância dos trabalhos apresentados. As revisões bibliométrica e sistemática apresentaram um panorama abrangente sobre as técnicas ativas e passivas, evidenciando suas aplicações práticas, desafios e tendências.

O escopo da pesquisa estava direcionado para autenticação e proteção de imagens e vídeos, dessa forma o volume de resultados potenciais era consideravelmente alto. A pesquisa de elementos individuais poderia gerar centenas ou mesmo milhares de resultados. Assim, o número de resultados obtidos estava dentro do previsto, o que exigiu a implementação de uma metodologia mais refinada para a pesquisa. Tratando-se das técnicas ativas, como marcas d'água digitais e assinaturas digitais, destacou-se a sua eficácia em garantir a integridade de conteúdos desde a sua criação até o consumo final do produto. Apesar disso, essas abordagens enfrentam limitações em cenários onde a manipulação é mais sofisticada, o que ressalta a importância das técnicas passivas. Estas últimas, demonstram um grande potencial na detecção de adulterações com base nas características intrínsecas das mídias digitais, sendo especialmente úteis em contextos onde não há informações pré-incorporadas.

Os resultados da revisão bibliométrica revelaram tendências importantes na produção científica, baseada em aprendizado profundo e inteligência artificial. Além disso, identificou-se a predominância de países como China, Índia e Estados Unidos em publicações na área. Este estudo também apontou a necessidade de abordagens mais integradas e colaborativas, tanto no desenvolvimento de novas ferramentas quanto na formulação de estratégias globais para combater os desafios impostos pela manipulação digital. Assim, reforça-se a importância de pesquisas contínuas que explorem a convergência entre técnicas ativas e passivas, para melhorar a robustez, eficiência e acessibilidade das soluções.

REFERÊNCIAS

BIRAJDAR, G. K.; MANKAR, V. H. Digital image forgery detection using passive techniques: A survey. **DIGITAL INVESTIGATION**, v. 10, n. 3, p. 226–245, OCT 2013. ISSN 1742-2876.

BOUROUIS, S.; ALROOBAEA, R.; ALHARBI, A. M.; ANDEJANY, M.; RUBAIEE, S. Recent advances in digital multimedia tampering detection for forensics analysis. **SYMMETRY-BASEL**, v. 12, n. 11, NOV 2020.

CAMACHO, I. C.; WANG, K. A comprehensive review of deep-learning-based methods for image forensics. **Journal of imaging**, MDPI, v. 7, n. 4, p. 69, 2021.

CHENNAMMA, H. R.; MADHUSHREE, B. A comprehensive survey on image authentication for tamper detection with localization. **MULTIMEDIA TOOLS AND APPLICATIONS**, v. 82, n. 2, p. 1873–1904, JAN 2023. ISSN 1380-7501.

COSTA ARTHUR PINHEIRO DE ARAúJO COSTA, A. M. S. C. F. S. G. M. d. S. Igor Pınheıro de A. **BIBLIOMETRIC STUDIES ON MULTI-CRITERIA DECISION ANALYSIS (MCDA) METHODS APPLIED IN MILITARY PROBLEMS**. 2022.

COSTA CAMILA GOMES DANTAS, B. M. D. L. O. M. d. O. K. A. M. G. G. A. B. C. L. T. Bruna da. **USO DA ANÁLISE BIBLIOMÉTRICA COMO FERRAMENTA PARA O LEVANTAMENTO DE ESTUDOS SOBRE A METABOLÔMICA APLICADA NA BIORREMEDIAÇÃO DE ÁREAS IMPACTADAS POR HIDROCARBONETOS**. 2022.

DONATO, M. D. H. **Etapas na Condução de uma Revisão Sistemática**. 2019. 227 p.

EL-SHAFAI, W.; FOUDA, M. A.; EL-RABAIE, E.-S. M.; EL-SALAM, N. A. A comprehensive taxonomy on multimedia video forgery detection techniques: challenges and novel trends. **MULTIMEDIA TOOLS AND APPLICATIONS**, 2023 MAY 24 2023. ISSN 1380-7501.

FARHAN, M. H.; SHAKER, K.; AL-JANABI, S. Copy-move forgery detection in digital image forensics: A survey. **MULTIMEDIA TOOLS AND APPLICATIONS**, 2024 FEB 7 2024. ISSN 1380-7501.

FERREIRA, J. B.; SILVA, L. d. A. M. O uso da bibliometria e sociometria como diferencial em pesquisas de revisão. **Revista Brasileira de Biblioteconomia e Documentação**, v. 15, n. 2, p. 448–464, 2019.

GUPTA, S.; MOHAN, N.; KAUSHAL, P. Passive image forensics using universal techniques: a review. **ARTIFICIAL INTELLIGENCE REVIEW**, v. 55, n. 3, p. 1629–1679, MAR 2022. ISSN 0269-2821.

GURUNLU, B.; OZTURK, S. A survey on photo forgery detection methods. In: CATTANI, C.; ATANGANA, A.; BULUT, H.; HAMMOUCH, Z.; BASKONUS, H.; MEKKAOUI, T.; AGOUJIL, S. (Ed.). **THIRD INTERNATIONAL CONFERENCE ON COMPUTATIONAL MATHEMATICS AND ENGINEERING SCIENCES (CMES2018)**. [S.l.], 2018. (ITM Web of Conferences, v. 22). ISSN 2271-2097. 3rd International Conference on Computational Mathematics and Engineering Sciences (CMES), Final Int Univ, Girne, CYPRUS, MAY 04-06, 2018.

HAM-BALOYI, P. J. Wilma ten. **Systematic review as a research method in post-graduate nursing education**. 2016. 120 p.

KAUR, N.; JINDAL, N.; SINGH, K. Passive image forgery detection techniques: A review, challenges, and future directions. **WIRELESS PERSONAL COMMUNICATIONS**, v. 134, n. 3, p. 1491–1529, FEB 2024. ISSN 0929-6212.

KORUS, P. Digital image integrity - a survey of protection and verification techniques. **DIGITAL SIGNAL PROCESSING**, v. 71, p. 1–26, DEC 2017. ISSN 1051-2004.

KORUS, P. Digital image integrity–a survey of protection and verification techniques. **Digital Signal Processing**, Elsevier, v. 71, p. 1–26, 2017.

KUMAR, M.; SRIVASTAVA, S. Image forgery detection based on physics and pixels: a study. **AUSTRALIAN JOURNAL OF FORENSIC SCIENCES**, v. 51, n. 2, p. 119–134, MAR 4 2019. ISSN 0045-0618.

LAPEI; FACE; UFG. **Um pouco sobre Revisão Bibliométrica e Revisão Sistemática**. LAPEI, 2022. Disponível em: <https://lapei.face.ufg.br/p/42358-um-pouco-sobre-revisao-bibliometrica-e-revisao-sistematica>. Acesso em: 06 nov. 2023.

LIN, X.; LI, J.-H.; WANG, S.-L.; CHENG, F.; HUANG, X.-S. *et al.* Recent advances in passive digital image security forensics: A brief review. **Engineering**, Elsevier, v. 4, n. 1, p. 29–39, 2018.

MARAS, M.-H.; ALEXANDROU, A. Determining authenticity of video evidence in the age of artificial intelligence and in the wake of deepfake videos. **The International Journal of Evidence & Proof**, SAGE Publications Sage UK: London, England, v. 23, n. 3, p. 255–262, 2019.

MARTIMBIANCO, A. L. C. **How to prepare a systematic review and meta-analysis: the methodological approach**. 2021.

PANDEY, R. C.; SINGH, S. K.; SHUKLA, K. K. Passive forensics in image and video using noise features: A review. **DIGITAL INVESTIGATION**, v. 19, p. 1–28, DEC 2016. ISSN 1742-2876.

RAJ, N. R. N.; SHREELEKSHMI, R. A survey on fragile watermarking based image authentication schemes. **MULTIMEDIA TOOLS AND APPLICATIONS**, v. 80, n. 13, p. 19307–19333, MAY 2021. ISSN 1380-7501.

RIBEIRO, C. A. Análise bibliométrica da produção científica mundial sobre apicultura de precisão nas bases de dados scopus e web of science. 2022.

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 Journal**, v. 5, n. 3, p. 361–370, 2020.

SCHIAVENATO, M.; CHU, F. Pico: What it is and what it is not. **NURSE EDUCATION IN PRACTICE**, v. 56, OCT 2021. ISSN 1471-5953.

SHARMA, P.; KUMAR, M.; SHARMA, H. Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: an evaluation. **MULTIMEDIA TOOLS AND APPLICATIONS**, v. 82, n. 12, p. 18117–18150, MAY 2023. ISSN 1380-7501.

SHI, C.; CHEN, L.; WANG, C.; ZHOU, X.; QIN, Z. Review of image forensic techniques based on deep learning. **MATHEMATICS**, v. 11, n. 14, JUL 2023.

SHI, C.; CHEN, L.; WANG, C.; ZHOU, X.; QIN, Z. Review of image forensic techniques based on deep learning. **Mathematics**, MDPI, v. 11, n. 14, p. 3134, 2023.

SINA, L. B.; NAZEMI, K. Visual analytics for systematic reviews according to prisma. In: BANISSI, E.; URSYN, A.; BANNATYNE, M.; PIRES, J.; DATIA, N.; NAZEMI, K.; KOVALERCHUK, B.; ANDONIE, R.; NAKAYAMA, M.; SCIARRONE, F.; HUANG, W.; NGUYEN, Q.; MABAKANE, M.; RUSU, A.; TEMPERINI, M.; CVEK, U.; TRUTSCHL, M.; MUELLER, H.; SIIRTOLA, H.; WOO, W.; FRANCESE, R.; ROSSANO, V.; DIMASCIO, T.; BOUALI, F.; VENTURINI, G.; KERNBACH, S.; MALANDRINO, D.; ZACCAGNIN, R.; ZHANG, J.; YANG, X.; GEROIMENKO, V. (Ed.). **2022 26TH INTERNATIONAL CONFERENCE INFORMATION VISUALISATION (IV)**. [S.l.: s.n.], 2022. (IEEE International Conference on Information Visualization), p. 307–313. ISBN 978-1-6654-9007-8. ISSN 1550-6037. 26th International Conference Information Visualisation (IV), Vienna, AUSTRIA, JUL 19-22, 2022.

STAMM, M. C.; WU, M.; LIU, K. J. R. Information forensics: An overview of the first decade. **IEEE ACCESS**, v. 1, p. 167–200, 2013. ISSN 2169-3536.

WANG, W.; DONG, J.; TAN, T. A survey of passive image tampering detection. In: HO, A.; SHI, Y.; KIM, H.; BARNI, M. (Ed.). **DIGITAL WATERMARKING**. [S.l.], 2009. (Lecture Notes in Computer Science, v. 5703), p. 308–322. ISBN 978-3-642-03687-3. ISSN 0302-9743. 8th International Workshop on Digital Watermarking, Univ Surrey, Guildford, ENGLAND, AUG 24-26, 2009.

WANG, W.; DONG, J.; TAN, T. A survey of passive image tampering detection. In: SPRINGER. **Digital Watermarking: 8th International Workshop, IWDW 2009, Guildford, UK, August 24-26, 2009. Proceedings 8**. [S.l.], 2009. p. 308–322.

WU, J.; SUN, W. Towards multi-operation image anti-forensics with generative adversarial networks. **Computers & Security**, Elsevier, v. 100, p. 102083, 2021.

ZANARDELLI, M.; GUERRINI, F.; LEONARDI, R.; ADAMI, N. Image forgery detection: a survey of recent deep-learning approaches. **MULTIMEDIA TOOLS AND APPLICATIONS**, v. 82, n. 12, p. 17521–17566, MAY 2023. ISSN 1380-7501.