UNIVERSIDADE CESUMAR - UNICESUMAR
CENTRO DE CIÊNCIAS EXATAS TECNOLÓGICAS E AGRÁRIAS
CURSO DE GRADUAÇÃO EM ENGENHARIA DE SOFTWARE

COMPUTAÇÃO FORENSE E A TÉCNICA DE ESTEGANOGRAFIA APLICADA EM IMAGENS DIGITAIS: UM MAPEAMENTO SISTEMÁTICO

JÉSSICA SANTIAGO FERREIRA

MARINGÁ – PR
2020

Jéssica Santiago Ferreira

COMPUTAÇÃO FORENSE E A TÉCNICA DE ESTEGANOGRAFIA APLICADA EM IMAGENS DIGITAIS: UM MAPEAMENTO SISTEMÁTICO

Artigo apresentado ao Curso de Graduação em Engenharia de Software da Universidade Cesumar – UNICESUMAR como requisito parcial para a obtenção do título de Bacharel(a) em Engenharia de Software, sob a orientação do Prof. Esp. Maurílio Martins Campano Junior.

MARINGÁ – PR

2020

FOLHA DE APROVAÇÃO

JÉSSICA SANTIAGO FERREIRA

COMPUTAÇÃO FORENSE E A TÉCNICA DE ESTEGANOGRAFIA APLICADA EM IMAGENS DIGITAIS: UM MAPEAMENTO SISTEMÁTICO

Artigo apresentado ao Curso de Graduação em Engenharia de Software da Universidade Cesumar –UNICESUMAR como requisito parcial para a obtenção do título de Bacharel(a) em Engenharia de Software, sob a orientação do Prof. Esp. Maurílio Martins Campano Junior.

Aprovado em: ____ de _____ de _____.

BANCA EXAMINADORA

_____

Prof. Esp. Maurílio Martins Campano Junior - UNICESUMAR

_____

Prof. M.e Arthur. Cattaneo Zavadski - UNICESUMAR

COMPUTAÇÃO FORENSE E A TÉCNICA DE ESTEGANOGRAFIA APLICADA EM IMAGENS DIGITAIS: UM MAPEAMENTO SISTEMÁTICO

Jéssica Santiago Ferreira

RESUMO

Junto a evolução da tecnologia, a criminalidade avança em formas digitais, atacando softwares de empresas, instituições e indivíduos. Novas formas de ataque, técnicas e ferramentas surgem para aumentar o trabalho da computação forense que, por meio de métodos técnico-científicos, busca por evidências tecnológicas que elucidem os fatos em investigações de atos ilícitos no ambiente digital. Este estudo apresenta, portanto, os resultados de um mapeamento sistemático da literatura sobre as metodologias, ferramentas e softwares ligados a computação forense, com o objetivo de sintetizar os estudos disponíveis, aferindo o estado da arte acerca do tema. Uma das técnicas utilizadas em crimes computacionais que vem ganhando força é a esteganografia, que pode ser aplicada em arquivos como imagens, vídeos e áudios. Nesse sentido, essas técnicas de identificação de esteganografia em imagens digitais também são evidenciadas neste trabalho.

Palavras-chave: Ocultação de informações. Perícia. Segurança.

COMPUTER FORENSICS AND THE STEGANOGRAPHY TECHNIQUE APPLIED IN DIGITAL IMAGES: A SYSTEMATIC MAPPING

ABSTRACT

Along with the evolution of technology, crime advances in digital forms, attacking software of companies, institutions, and individuals. New forms of attack, techniques, and tools arise to increase the work of computer forensics, which seeks technological evidence that elucidates the facts in investigations of illicit acts in the digital environment through technical-scientific methods. Therefore, this study presents the results of a systematic mapping of the literature on the methodologies, tools, and software related to computer forensics, in order to synthesize the available studies and to assess the state-of-the-art on the subject. The steganography is one of the arising techniques used in computational crimes, and it can be applied to files such as images, videos, and audios. Due to its current relevance, the identification technique of steganography in digital images is also pointed out in this paper.

Keywords: Information concealment. Investigation. Security.

1 INTRODUÇÃO

A Ciência Forense é uma área interdisciplinar que, de acordo com Vallim (2019), reúne estudos de conhecimentos técnicos e científicos de diversas áreas como criminologia, computação, psicologia, medicina legal entre outras áreas, que apoiam na busca pela verdade em investigações relativas à justiça civil e criminal. O profissional qualificado em qualquer dos campos de atuação da Ciência Forense é responsável por examinar o local do crime em busca de evidências que comprovem o que de fato ocorreu e quem são os indivíduos envolvidos no caso.

Dentre os ramos da Ciência Forense se encontra a Perícia Forense Computacional que conforme Eleutério (2019) tem como objetivo principal determinar a dinâmica, a materialidade e autoria de ilícitos ligados à área de informática, identificando e processando evidências digitais por meio de métodos técnico-científicos, conferindo-lhes validade probatória em juízo. Também pode ser conhecida como Computação Forense ou Perícia Digital, que através do profissional perito forense utiliza de técnicas investigativas para encontrar e analisar evidências tecnológicas, extraídas desde equipamentos computacionais até dados provenientes do tráfico de rede, a fim de solucionar ou esclarecer o crime cometido.

Cada vez mais a computação forense se faz presente nos ambientes profissionais e pessoais. O rápido avanço tecnológico e o uso em massa da rede mundial de computadores proporciona, consequentemente, o aumento dos ataques cibernéticos contra às instituições, empresas e indivíduos. A facilidade com que se é possível trocar informações e manter-se conectados mundialmente através do serviço de *World Wide Web* (WWW) chama a atenção dos indivíduos mal intencionados, que usufruem da alta disseminação de informação na internet para obter conhecimento necessário do funcionamento dos sistemas para, então, explorar as vulnerabilidades dos mesmos. A empresa russa Kaspersky, produtora de softwares de segurança para internet, em um de seus artigos sobre como se proteger contra crimes cibernéticos, aponta diversos tipos de crimes dos quais podemos citar como exemplo a fraude por e-mail, roubo de dados financeiros, espionagem, extorsão, dentre outros, dos quais o criminoso na maioria das vezes visa provocar danos a fim de se beneficiar (KASPERSKY, 2020).

Boas práticas, técnicas bem como serviços podem e devem ser adotados para fortalecer a proteção das informações pertinentes no ambiente virtual. Tanto para o usuário comum quanto para as empresas e organizações, conhecer as possíveis ameaças digitais colabora para prevenção dos ataques. Os crimes podem ser dos mais diversos tipos e a cada

ano surgem novas modalidades. Basicamente, eles podem ser distinguidos em dois grupos, os crimes em que o computador é o alvo dos criminosos e os crimes em que o computador é tido como ferramenta para efetuar os delitos (Eleutério, 2019).

Numa tentativa de combater a ampla variedade de crimes, a computação forense trabalha investigando e analisando evidências digitais, a fim de desvendar as causas do ataque e comprovar através de técnicas e metodologias a validade das provas. Além disso, ferramentas de investigação forense computacional podem ser utilizadas no processo de análise dos dispositivos possivelmente infectados ou maliciosos, com a intenção de auxiliar a identificação de possíveis evidências. Da mesma forma que técnicas e ferramentas são utilizadas para colaborar na busca dessas informações, Barreto (2019) conceitua que técnicas denominadas anti-forense podem ser utilizadas pelos criminosos para ocultar e até remover dados que possam servir como evidência do crime. Tudo isso, destaca como o trabalho da perícia forense computacional é minucioso e extremamente necessário nos dias atuais.

Uma das técnicas utilizadas por criminosos no mundo digital é a esteganografia, sendo um ramo da criptologia, envolve estudos e técnicas que camuflam informações para que não sejam percebidas. Eleutério (2019, p. 80) define a esteganografia como “uma técnica que consiste basicamente em ocultar uma mensagem dentro de outra”. Quando utilizada pelos criminosos no meio virtual podem ter a finalidade de ocultar os rastros da prática criminosa bem como encobrir mensagens maliciosas. As informações podem ser inseridas em diferentes tipos de arquivos como arquivo de texto, imagem, vídeo ou áudio, sendo que para sua detecção são utilizados de métodos e ferramentas onde nem sempre é possível extrair a informação, mas apenas identificar a presença da mesma.

No contexto deste trabalho, serão abordados estudos em que a esteganografia é aplicada em imagens digitais, bem como estudos que apresentam as ferramentas que são comumente utilizadas para a extração e/ou identificação de informações ocultadas neste tipo de arquivo. Em relação ao processo investigativo no ambiente virtual, busca-se ressaltar os processos da perícia digital indicados nos estudos disponíveis, assim como, os softwares e ferramentas utilizadas na solução dos crimes envolvendo mídias de armazenamento na área de informática.

2 FUNDAMENTAÇÃO TEÓRICA

Nesta seção serão abordados os conceitos da segurança no ambiente computacional, como também a definição do método de pesquisa utilizado para a construção deste trabalho.

2.1 SEGURANÇA COMPUTACIONAL NA REDE DE COMPUTADORES

Uma rede pode ser definida como um conjunto de dispositivos conectados por links de comunicação, duas ou mais redes que se comunicam entre si são consideradas uma internet. Forouzan (2008). Dado esses conceitos, destaca-se que a internet mais conhecida atualmente é a Internet (note com I maiúsculo), ela garante a conexão de milhares de dispositivos computacionais no mundo todo. Até a década de 1960 de acordo com Kurose (2010) a rede telefônica era a rede de comunicação dominante no mundo inteiro, mas com o surgimento da World Wide Web em 1990, a Internet foi levada para os lares e empresas de milhões de pessoas revolucionando a forma de se comunicar garantindo rapidez e facilidade na troca de informações.

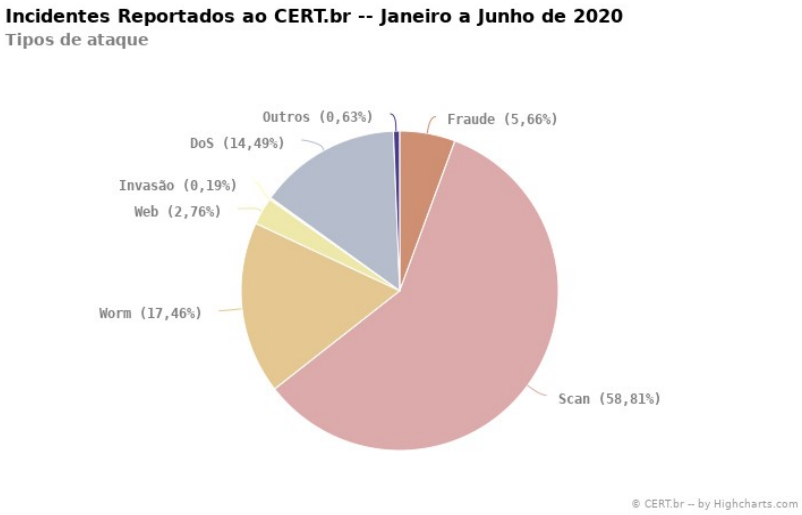
A Internet que utilizamos hoje evoluiu muito desde o seu surgimento, em consequência do avanço da tecnologia além dos computadores de mesa, outros diversos dispositivos como notebooks, celulares, *tablets*, televisores, câmeras e, até equipamentos domésticos como geladeiras, cafeteiras e lavadoras passaram a utilizar da Internet para as mais diversas funcionalidades. Cada vez mais o cotidiano das pessoas é tomado por atividades que envolvem o uso dos dispositivos computacionais, um estudo da agência de notícias brasileiras - Agência Brasil - referente a quantidade de usuários que atualmente acessam a internet, publicado em maio de 2020, mostra que três a cada quatro brasileiros acessam a Internet (Valente, 2020).

Em paralelo a essa evolução, os crimes na área da informática ganham proporções maiores, o que implica, cada vez mais, na importância dos cuidados a serem tomados ao utilizar-se dos serviços tecnológicos. Os criminosos exploram as vulnerabilidades dos sistemas para concretizarem os ataques em busca de informações valiosas, em Stallings (2014) os ataques à segurança são classificados como ataques passivos e ataques ativos, onde os passivos têm a característica de descobrir ou utilizar informações do sistema sem que os recursos computacionais sejam afetados, já os ativos tentam alterar recursos do sistema ou afetar sua operação.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) disponibiliza relatórios indicando o total de incidentes reportados por ano no

Brasil. No primeiro semestre de 2020, o total de notificações recebidas foi de 318.697. No gráfico a seguir, retirado do site oficial do CERT.br é possível visualizar a porcentagem das notificações classificadas por tipos de ataques.

Figura 1 – Incidentes reportados no primeiro semestre de 2020



Fonte: CERT.br (2020).

Para contornar a ocorrência desses incidentes Stallings (2014) aponta que a área de segurança de rede e de Internet visa desviar, prevenir, detectar e corrigir violações de segurança que envolvam a transmissão de informações e ainda diz que a segurança computacional baseia-se em três pilares, sendo eles a confidencialidade, integridade e disponibilidade. Conhecidos como a tríade CIA (do inglês *Confidentiality, Integrity and Availability*), esses pilares apresentam os objetivos fundamentais da segurança tanto para dados, quanto para serviços de informação e computação. A confidencialidade está relacionada a privacidade dos dados, que busca garantir que as informações sejam compartilhadas apenas com os que tiverem autorização de acesso, aqui, muitas vezes, envolve que os dados sejam cifrados, a fim de impedir que uma mensagem que caia em mãos erradas seja entendida. Já a integridade condiz com garantir que uma mensagem enviada pelo transmissor chegue ao receptor sem que dados tenham sido alterados, perdidos ou roubados. Por sua vez, a disponibilidade consiste em dispor de acesso aos dados de forma rápida e confiável.

A implementação efetiva das metas de segurança envolve a utilização de duas técnicas predominantes atualmente, a criptografia e a esteganografia. A criptografia além de confidencialidade provê autenticação, integridade de mensagem, não repudiação e controle de

acesso. De origem grega, a palavra significa “escrita secreta” sendo definida como a ciência que utiliza algoritmos matemáticos para codificar e decodificar dados, a fim de impedir que pessoas não autorizadas tenham entendimento da mensagem transmitida em um meio de comunicação. Já a esteganografia significa “escrita oculta” que diferentemente da criptografia que esconde o conteúdo de uma mensagem por meio de cifração, oculta a mensagem em si, encobrindo-a com alguma outra coisa, Forouzan (2013). Neste trabalho, dar-se-á ênfase na técnica de esteganografia aplicada em imagens digitais.

2.2 MAPEAMENTO SISTEMÁTICO

A revisão sistemática da literatura é um método de pesquisa científica que surgiu na área medicinal, mas que a partir de seu sucesso fez com que outras áreas começassem a produzir artigos como tal. Pode-se citar como exemplos de revisões de literatura, tanto a revisão sistemática quanto o mapeamento sistemático que foi o tipo utilizado neste trabalho. Sendo considerado um estudo secundário, o mapeamento sistemático tem por objetivo identificar e classificar os estudos primários relacionados com um tópico de pesquisa, sendo, então, uma revisão mais ampla das evidências disponíveis de um dado tópico (SCANNAVINO, 2017). Com ele é possível reunir a literatura disponível em um certo campo de pesquisa, de modo que possa identificar lacunas em que mais estudos primários se fazem necessários, dessa forma, apresentando o estado atual de conhecimento sobre o determinado tópico.

Kitchenhan (2004) organiza o mapeamento em três fases, sendo elas: Planejamento, Condução e Análise de Resultados. Para a condução seguiu-se o protocolo elaborado na fase de planejamento que formaliza a execução do mapeamento sistemático com a definição dos objetivos, das questões de pesquisa, como também das estratégias para busca e seleção dos estudos. Tendo identificado e selecionados os estudos foram analisados e extraídos os resultados para assim responder as questões elaboradas e apresentar um posicionamento quanto ao tema definido.

3 METODOLOGIA

Seguindo a estrutura apresentada por Kitchenhan (2004), nesse tópico serão apresentados a definição dos objetivos, as questões de pesquisa, bem como as estratégias de

busca e seleção e os critérios de inclusão e exclusão, representando, assim, a fase de planejamento do mapeamento sistemático.

3.1 OBJETIVOS E QUESTÕES DE PESQUISA

A condução do mapeamento sistemático neste artigo tem como objetivo sintetizar estudos primários relacionados a computação forense e a técnica de esteganografia, com propósito de identificar os processos da investigação criminal assim como os métodos, ferramentas e softwares envolvidos no exame de mídias de armazenamento e na detecção de informações ocultas em imagens digitais, com intuito de fornecer uma visão geral dos estudos que vêm sendo disponibilizados neste campo de pesquisa. Para alcançar os objetivos propostos restringiu-se o escopo da pesquisa de acordo com as seguintes questões:

Questão 01: Quais os processos e metodologias da perícia forense em crimes computacionais?

Questão 02: Quais softwares ou ferramentas vêm sendo utilizados em exames periciais de mídias de armazenamento?

Questão 03: Quais técnicas, métodos ou ferramentas vêm sendo utilizados para a identificação da técnica de esteganografia em imagens digitais?

Questão 04: Quais crimes são cometidos utilizando a esteganografia em imagens digitais?

3.2 ESTRATÉGIAS DE BUSCA: FONTES DE PESQUISA

Na coleta dos estudos utilizou-se da busca avançada aplicando-se duas strings definidas por meio do agrupamento de palavras chaves relacionadas ao tópico de pesquisa concatenadas por meio dos operadores lógicos E (AND em inglês) e OU (OR em inglês). As strings são apresentadas a seguir:

String 1: (“pericia digital” OR "computação forense" OR "forense computacional" OR "pericia forense computacional") AND (ferramenta OR software OR técnica);

String 2: (esteganálise OR esteganografia) AND (ocultar OR ocultação OR segurança OR "imagem digital" OR "imagens digitais");

Além da busca avançada, também se adotou a busca manual e snowballing. Perante os resultados da busca automática, a busca manual só foi considerada nos casos em que o

documento esteve indisponível de forma completa nas fontes de pesquisa, dessa forma, o título juntamente com o nome dos autores foi utilizado como uma string de busca. Nos casos em que o estudo não fora encontrado na íntegra, o mesmo não fora incluído. A estratégia *snowballing* colaborou no alcance de estudos relevantes, a partir de estudos já selecionados anteriormente e foi utilizada durante a Seleção Final que será detalhada mais a frente neste trabalho.

Referente aos estudos retornados nas fontes de pesquisa foram considerados apenas os que foram publicados nos últimos 3 anos (2017 – 2020), trabalhos que estejam em português e sejam artigos científicos, teses ou dissertações de mestrado e teses de doutorado. As fontes de busca selecionadas estão elencadas no Quadro 1 apresentado a seguir:

Quadro 1 – Fontes de busca

FONTE	URL
Biblioteca Unicesumar	https://www.unicesumar.edu.br/biblioteca/
BASE	https://www.base-search.net/
Google acadêmico	https://scholar.google.com.br/

3.3 CRITÉRIOS DE INCLUSÃO E EXCLUSÃO

Para a seleção dos estudos foi elaborado os critérios de inclusão e exclusão conforme apresentados nas tabelas 2 e 3.

Tabela 1 – Critérios de Inclusão

Sigla	Critério
CI1	O estudo que satisfaz a string de busca no título ou resumo.
CI2	O estudo que foque no contexto da pesquisa.
CI3	O estudo que possui versão completa disponível.

Tabela 2 – Critérios de Exclusão

Sigla	Critério
CE1	O estudo que seja repetido.
CE2	O estudo que não seja um estudo primário.
CE3	O estudo que não satisfaz o tema da pesquisa.
CE4	O estudo em que o resumo não satisfaz o tema da pesquisa.

4 EXECUÇÃO DO MAPEAMENTO: BUSCA E SELEÇÃO

Seguindo as estratégias definidas no tópico anterior, executou-se a busca sobre as fontes de pesquisa consideras e obteve-se um total de 387 resultados, dos quais 275 resultam da primeira *string* de busca, assim como 112 resultam da segunda *string*. Nessa seleção preliminar foram identificados e descartados 49 estudos duplicados, com isso, considerou-se apenas 338 como relevantes. A tabela a seguir indica a quantidade de estudos de acordo com cada fonte de pesquisa.

Tabela 3 – Seleção preliminar

Fonte	Qtd.	Descartados (duplicados)	Seleção preliminar
Biblioteca Unicesumar	37	23	14
BASE	52	1	51
Google Acadêmico	298	25	273
Total:	387	49	338

A partir disso, novas seleções foram realizadas e classificadas em duas etapas que serão detalhadas logo abaixo.

4.1 SELEÇÃO INICIAL

Nesta etapa, analisou-se o título e o resumo de cada trabalho levando em consideração os critérios de inclusão e exclusão e selecionou-se 45. Com base nisso, pode-se separar os estudos que tratam sobre computação forense dos que tratam sobre esteganografia. Os que abordavam assuntos pertinentes ao tema da pesquisa foram incluídos para, posteriormente, serem analisados em detalhes, os demais foram descartados. A relação dos estudos pode ser consultada na Tabela 4.

4.21 SELEÇÃO FINAL

Dos 45 trabalhos selecionados na análise da etapa anterior foram considerados 25 com base na leitura completa e avaliação detalhada. Para que mais estudos fossem recuperados, a técnica de *snowballing* foi aplicada o que acrescentou 3 estudos relacionados a computação forense e 7 relacionados a esteganografia, totalizando assim 35 estudos para serem extraídas as informações.

Tabela 4 – Seleção Inicial e Final

Fonte	Descartados (Seleção Inicial)	Seleção Inicial	Descartados (Seleção Final)	Seleção Final
Esteganografia	4	9	2	7
Computação Forense	2	36	18	18
Total:	6	45	20	25

5 RESULTADOS E DISCUSSÕES

Nesta seção serão apresentados os resultados extraídos dos estudos selecionados, a fim de responder as questões de pesquisas definidas anteriormente.

Questão 01: Quais os processos e metodologias da computação forense em crimes computacionais?

No que concerne aos processos que constituem a investigação forense no âmbito computacional, observou-se, através da análise dos estudos classificados, uma variação na determinação de quais processos se fazem necessários. Dos 35 estudos foram encontrados 18 que apontam ou um determinado modelo dos processos essenciais para a investigação ou métodos e técnicas que podem ser adotados na busca e elucidação das evidências. Segue uma discussão sobre como cada estudo apresentam os processos e metodologias.

Em Ubaldo (2017) não houve uma determinação exata dos processos, mas basicamente, destacou-se que os dispositivos apreendidos são examinados por especialista forenses os quais buscam por evidências que podem ou não necessitarem de recuperação baseada em hardware ou software. Enfatizou-se o uso do método de criar cópia digital do estado inicial do dispositivo, a fim de garantir autenticidade da cadeia de custódia, como também a utilização da técnica de soma de verificação através dos algoritmos de *hash* para garantir a integridade das evidências.

Já em Júnior (2019), faz-se um estudo de diversos modelos já existentes de investigação forense e defini os seguintes processos: Ações Preliminares, Colheita, Exame, Análise e Apresentação, onde Ações Preliminares se subdivide em Autorização e em Busca e Identificação, bem como Colheita se subdivide em Preservação e Colheita. Cita a cadeia de custódia como um conjunto de procedimentos essenciais, mas não obrigatórios, que permitem aos operadores do Direito determinar se as evidências apresentadas foram tratadas com o devido rigor, como também cita o método de duplicação dos dados no processo de Colheita,

cálculo de *hashes* no processo de Exame e elaboração do laudo pericial no processo de Apresentação. Para a análise dos dados discorre sobre três diferentes técnicas, sendo elas *Live Analysis, Post Mortem* e Reprodução do Ambiente.

Em Hoelz (2009) referenciam-se os processos como sendo Planejamento, Atuação no Local, Coleta de Vestígios, Exame Pericial, Laudo Pericial e, por fim, Revisão. Foi possível observar que a concretização do laudo pericial é tida como uma das etapas do processo maior que é a investigação. Além disso, infere que a iniciação da cadeia de custódia é no processo de Coleta de Vestígios.

Os estudos de Souza (2016), Silva (2018b) e Borges (2017) baseiam-se no modelo de Kent (2006) para definir como Coleta, Exame, Análise e Resultados Obtidos os processos da computação forense, no entanto, apenas Souza (2016) e Borges (2017) citam os métodos de imagem e espelhamento bem como a utilização do algoritmo de *hash*, e apenas Silva (2018b) incrementa o estudo apresentando a *Live analysis*, *Network Analysis* e *Post Mortem Analysis* como técnicas para análises dos dispositivos.

Os trabalhos de Silva (2017), Nunes (2018), Mesquita (2018) e Rodrigues (2019) também definem as etapas como Coleta, Exame, Análise e Resultados Obtidos, mas o trabalho de Silva (2017), difere-se dos demais ao citar a importância da cadeia de custódia e da cópia dos dados e geração do *hash* e, juntamente com ele, o estudo de Mesquita (2018) ressalta a elaboração do laudo pericial.

O estudo de Filho (2018) cita cinco processos, Identificação, Coleta, Preservação, Análise e Apresentação. No processo de preservação, apresenta ser comum realizar a cópia dos dados e utilizar do cálculo de *hash* para garantir a integridade dos dados. Referente aos tipos de análises possíveis identificou apenas a descrição da análise do tipo *Post Mortem*.

Em Dias (2019), o trabalho é voltado para a computação forense aplicada no meio IoT, porém aponta os processos como Preservar, Analisar e Apresentar as Evidências. Já no trabalho Araújo (2019) não se define diretamente os processos a serem desempenhados, mas destaca-se a criação da cadeia de custódia e criação da cópia digital do dispositivo na investigação forense.

O estudo de Tolentino (2018) aponta que toda evidência deve ser identificada, preservada, analisada, apresentada e, assim, define os processos básicos. Comenta sobre a análise ao vivo que em outros estudos é denominada como *Live Analysis* e, também, apresenta a cadeia de custódia como forma de garantir a inalterabilidade das provas. Destaca que a análise é feita sobre a cópia realizada dos dados e que o laudo pericial descreve os passos do perito durante a investigação.

A ideia do trabalho Pereira (2016) apresenta os quatro processos: Coleta de Dados, Exame dos dados, Análise das Informações e, por fim, Interpretação dos resultados. Cita apenas duas formas de analisar o dispositivo sendo elas *Live Forensics* e *Post Mortem Forensics*. Especifica que a construção da cadeia de custódia se faz no processo de coleta dos dados do mesmo modo que o laudo é gerado no processo de interpretação dos resultados.

O trabalho de Silva (2018a) define os seguintes processos: Aquisição, Identificação, Avaliação e Apresentação e destaca a criação da cadeia de custódia como forma de documentar o tratamento dos dados e a utilização do cálculo de *hash* para comprovação de autenticidade.

Por fim, dois dos trabalhos voltados para a técnica de esteganografia discorrem sobre os processos e metodologias. O estudo Martins (2017) classifica os processos da computação forense como sendo Coletar, Examinar, Identificar, Preservar e Documentar e cita a construção da cadeia de custódia. Já o estudo de Freitas (2014) aponta os processos como Coleta, Exame, Análise e Resultados Obtidos além de comentar sobre a elaboração do laudo e a realização da cópia das informações dos dispositivos de armazenamento.

Além dos 18 estudos apresentados anteriormente, dois outros foram classificados como relevantes. O trabalho de Rocha (2018), apesar de não comentar diretamente dos processos e metodologias, descreve as competências necessárias do perito na área da computação forense, destacando a importância do cuidado para com os dispositivos computacionais para a preservação das possíveis evidências que poderão ser identificadas durante o processo de investigação. Já o estudo de Campos (2019) apresenta uma metodologia diferenciada, pois elucida a utilização do *malware*, que muitas vezes é tido como o alvo da investigação, como um método eficaz na obtenção de evidências no processo penal.

Com a leitura completa dos artigos, percebe-se que os processos são empregados como etapas a serem desenvolvidas pelo perito forense onde a quantidade e definição dessas etapas podem variar dentre as investigações, sendo possível incluir ou excluir algumas delas de acordo com a necessidade. No entanto, de modo geral, os trabalhos apontam ao menos três etapas essenciais, sendo elas a coleta, o exame e a apresentação dos resultados, que podem receber denominações diferentes entre os estudos analisados, mas que possuem o mesmo objetivo. Compreende-se também que não há uma definição padronizada dos processos a serem seguidos, mas que a organização dos mesmos é indispensável. Em relação as metodologias que podem ser adotadas no decorrer dos processos foram identificadas a utilização do algoritmo de *hash*, a duplicação dos discos para a cópia dos dados, alguns tipos

de análises específicas como a *Live Analysis, Post Mortem* e *Network Analysis* e, por fim, a elaboração da cadeia de custódia e do laudo pericial.

Questão 02: Quais softwares ou ferramentas vêm sendo utilizadas em exames periciais de dispositivo de armazenamento?

Observou-se que a utilização dos softwares e ferramentas no processo investigativo pode variar de acordo com o tipo do dispositivo em análise, assim como, seu estado atual. Os equipamentos que vão de unidades de estado sólido, discos rígidos, pendrives e até dispositivos móveis como os celulares podem sofrer perda dos dados de forma intencional ou não, o que implica no processo de recuperação das informações antes mesmos de iniciar o processo de exame.

Na cópia dos dados do dispositivo, os estudos de Ubaldo (2017), Júnior (2019), Souza (2016), Borges (2017), Araújo (2019), Pereira (2016), Freitas (2014) citam a utilização de ferramentas como os bloqueadores de escrita ou duplicadores, a fim de que possam garantir a cópia fiel dos dados, evitando que os mesmos sofram alterações. Em relação aos softwares, alguns trabalhos apresentaram estudos de casos e experimentos com a utilização de alguns dos softwares disponíveis atualmente, e a seguir são referenciados cada estudo.

Carvalho (2005) utilizou-se o software FDTK para a recuperação de arquivos de um *pendrive.* Júnior (2019) realiza três experimentos sobre SSD com a utilização dos softwares FTK Imager, Foremost, Scalpel, Magic Rescue, Photorec e Recoverjpeg e NTFS Unselete.

Borges (2017) utiliza dos softwares FTK Imager, Data Recovery Toolkit, FTK, Autopsy, RainbowCrack na identificação e recuperação das possíveis evidências do dispositivo de armazenamento removível.

Silva (2017) demonstra a utilização dos softwares ERDNT, Windows Registry Recovery, RegRipper na tentativa de identificar se houve vazamento de informação confidencial por meio da análise de um HD.

Nunes (2018) realiza a captura de dados de um aparelho celular com o uso das ferramentas AFLogical e Santoku.

O estudo de Pereira (2019) não utiliza um software diretamente, mas foi levado em consideração, pois apresenta um estudo de caso em que busca informações relevantes através da análise das mensagens geradas pela syslog, a fim de identificar a possível conexão de um pendrive no servidor. Já Filho (2018), em especial, apresenta os resultados da utilização dos softwares FTK Imager, RegRipper, Kali Linux e Nessus um caso real de sistema invadido vítima de ransomware.

Rodrigues (2019) utilizou das ferramentas FTK Imager, Autopsy e, especificamente, para a busca de rootkits os softwares Chkrootkit, Rkhunter e Diamorphine LKM, mas ressaltou a utilização dos softwares IPED, EnCase e Celebrite.

Pereira (2016) aponta o uso dos softwares Encase, FTK, Helix, FTDK, PerBR, mas em seu estudo de caso sobre roubo de dados através de malwares, utilizou- se apenas Encase e Helix para a análise e extração dos dados do disco rígido e da memória RAM.

O trabalho de Silva (2018a), na análise de um sistema comprometido utilizou dos softwares Autopsy, Chkrootkit e Rkhunter.

Outros estudos como os de Ubaldo (2017), Souza (2016), Araújo (2019) apesar de não apresentarem um estudo de caso, mencionam a utilização dos seguintes softwares: EnCase, FTK, X-Ways, Sleuth Kit, Authopsy, Recuva e PCI File Inspector.

Com isso, nota-se que a escolha das ferramentas e softwares no decorrer do processo ocorre de acordo com as necessidades e características específicas de cada investigação, pois em especial, um mesmo software pode ser utilizado em situações diferentes no momento em que possuem diversas funcionalidades.

Questão 03: Quais técnicas, métodos ou ferramentas vêm sendo utilizados para a identificação da técnica de esteganografia em imagens digitais?

A análise dos 15 estudos referente a esteganografia resultou nas observações a seguir: O estudo de Possatti (2019) apresenta a utilização do software StegExpose composto pela implementação de quatro diferentes métodos de esteganálise sendo eles *Primary Sets, Chi Square, Sample Pair,* e *RS Steganalysis* para analisar uma seleção de imagens em que a maioria continha informações ocultas por meio do método esteganográfico LSB. Além disso, citou as técnicas de ataques visuais e ataques estatísticas como principais, onde menciona os métodos *Chi Square, RS Analysis, Primary Sets* e *Sample Pair* no âmbito de esteganálise por ataques estatísticos. Os trabalhos de Coelho (2004) e Martins (2017) também indicam as técnicas de ataques visuais e estatísticas, no entanto, Martins (2017) acrescenta o ataque estrutural.

Destaca-se no trabalho de Geoflly (2017), a avaliação objetiva da modificação de imagens realizadas com o uso das métricas PSNR, *Structural Similarity Index* (SSIM) e *Structural Similarity Index with Perceptual Weighting* (PW-SSIM) que permitem a verificação da degradação do arquivo. Com isso, é possível identificação da presença da técnica esteganográfica por meio da observação do SI do arquivo, parâmetro que indica o nível de detalhes espaciais percebido por um observador humano em uma imagem.

No estudo de Estevan (2017) desenvolveu uma ferramenta embasada nos conceitos de ocultação de imagem através da esteganografia e apesar de não especificar o método utilizado para análise, descreveu que o sistema desenvolvido é capaz de inserir informações bem como identificar a presença da mesma. Santos (2017), também cita as técnicas de ataques visuais, ataques estruturais e ataques estatísticos, mas as classificam em 5 subtipos: *stego-only atack* (apenas esteganografia), *known cover* (mensagem de cobertura conhecida), *known message atack* (mensagem conhecida), *stego-attack* (ataque de esteganografia) e *cover-emb-stego* ou *known-cover-message* (dado embutido e mensagem de cobertura conhecidos). Além disso, observou-se a utilização das ferramentas StegDetect que faz parte do utilitário StegBreak como também da ferramenta StegExpose que é especializada na detecção de esteganografia LSB, ambas com intuito de identificar a presença de informações em imagens.

O estudo de Floret (2018) utilizou-se das ferramentas Binwalk do Backtrack ou Kali Linux, Okteta do Caine, Outguess e Hexdump do FDTK, e Bless Hex Editor do Helix3 na busca por dados ocultados nas imagens em análise. Já Freitas (2014) realiza experimentos envolvendo tanto o processo de ocultação quanto da análise dos arquivos alterados. Observou-se a utilização das ferramentas Outguess, Stegcompare e Xsteg nativas do FDTK, bem como a wbStego e Spammimic.

Almeida (2017) apesar de apresentar os conceitos da técnica de esteganografia, não menciona diretamente as técnicas e ferramentas utilizadas no processo de análise de imagens, no entanto, foi levado em consideração por destacar que cálculos estatísticos como o da média e variância permitem avaliar os dados ocultos antes e depois da passagem pelo processamento das imagens, resultando em informações relevantes referentes ao comportamento dos pixels. Dessa forma, colabora no processo de esteganálise. Farias (2017) utiliza a técnica *Structural Similarity* (SSIM), a fim de constatar o percentual de sucesso do processo de esteganografia, possibilitando a análise do grau de semelhança entre as imagens originais e suas respectivas cópias.

Os trabalhos de Julio (2007) e Rocha (2006) se assemelham ao citar os ataques aurais, estruturais e estatísticos para a identificação de dados ocultos e também ao referenciar as técnicas de análises *Chi-Square Test Approach*, Análise RS, métricas de qualidade de imagens (*Image Quality Metrics*) e métricas de tons contínuos e análise de pares de amostragem. No entanto, se distinguem por Rocha (2006) acrescentar a técnica de Taxa de inversão da energia do gradiente (*Gradient Energy Flipping Rate*) e Análise de estatísticas de alta ordem. Ainda sobre Julio (2007), observou-se o destaque para utilização das ferramentas StegSpy, StegDetect.

Julio (2007) citou apenas a ferramenta OutGuess para a identificação da esteganografia. Já Rocha (2003) apresentou a criação de uma ferramenta para comunicação segura através dos métodos da esteganografia e realizou a análise das mesmas através da técnica do tipo ataque estatístico.

Eduardo (2019) propõe a identificação de informações embutidas em imagens por meio da análise da vizinhança, ou seja, uma análise pixel a pixel de uma determinada região da imagem em busca de diferenças entre elementos vizinhos que tendem a ter o mesmo valor de cor. Notou-se a utilização das ferramentas Notepad++ e Matlab que não são consideradas ferramentas específicas para análise da técnica de esteganografia, mas que colaboraram no estudo em questão.

Questão 04: Quais crimes são cometidos utilizando a esteganografia em imagens digitais?

Dos 35 estudo selecionados, 8 mencionaram algum tipo de prática criminosa em que o uso da esteganografia pode ou foi identificada. Segue a descrição de cada um dos estudos.

Possatti (2019) aponta que a esteganografia pode ser utilizada para transmitir imagem de pornografia e pedofilia, como também já fora utilizada na comunicação secreta entre espiões criminosos.

Coelho (2004) ressalta a utilização da esteganografia por razões ilegítimas, alegando que pode ser utilizada em práticas como roubo de dados, geração de arquivos pornográficos e comunicação secreta entre terroristas. Martins (2017) comenta que a esteganografia incentiva dentre outros crimes, a fraude, pedofilia e o terrorismo.

Santos (2017) cita mensagens com *spam*, imagens com conteúdo de pedofilia e mensagens com informações de atentados como exemplos dos crimes envolvendo o uso de tal técnica.

Freitas (2014) comenta sobre casos reais de crimes cometidos com uso da técnica de esteganografia em que mensagens e até mesmo instruções de vírus são embutidas em imagens.

Julio (2007) cita que a esteganografia é indiciada em crimes como a divulgação de imagens de pornografia infantil na Internet e, da mesma forma que Carvalho (2018), cita a transmissão de mensagens de redes terroristas como a Al-Qaeda.

6 CONCLUSÃO

Diante do importante papel da computação forense em função do avanço tecnológico, o presente artigo apresentou os principais resultados de um mapeamento sistemático sobre os processos, softwares e ferramentas referentes às investigações no âmbito informático, bem como sobre as técnicas e ferramentas utilizadas no combate aos crimes envolvendo a técnica de esteganografia. De modo geral, a execução do mapeamento contribui para a identificação dos trabalhos relevantes que são disponibilizados relativo a um tema específico. Nesse sentido, buscou-se coletar estudos que contribuíssem para apresentar maior entendimento do atual estado da arte relacionado a computação forense e a esteganografia.

Os resultados apresentaram um grande número de obras que discutem os processos da perícia forense investigativa e pôde-se concluir que não há um padrão estabelecido para a realização dos trabalhos do perito forense, nem ferramentas e softwares especificamente determinados para o desvendamento do crime. O profissional age conforme suas necessidades diante dos fatos do caso em questão que está sendo investigado. Apesar disso, foi possível identificar que a coleta e análise dos equipamentos, bem como a apresentação dos resultados são etapas significativas na elucidação das evidências de um crime. Com a leitura dos estudos percebe-se a existência de uma vasta quantidade de ferramentas e softwares disponíveis para a realização dos exames periciais. No entanto, a computação forense necessita estar sempre pareada ao surgimento das novas técnicas, metodologias e ferramentas, pois o desenvolvimento tecnológico traz consigo novas formas de cometer práticas criminosas.

Na busca por estudos na área de esteganografia, uma das dificuldades encontradas é o fato de ser notável que estudos referentes as técnicas e softwares de identificação da técnica esteganográfica em imagens digitais são carentes. Ainda assim, foi possível detectar trabalhos que discutem os crimes que envolvem a aplicação da técnica, como também os métodos e sistemas utilizados para a constatação de informações ocultas.

A revisão de literatura desenvolvida neste artigo não abrangeu todos os trabalhos disponíveis atualmente, mas pode sintetizar os principais trabalhos condizentes com os objetivos, agregando assim uma nova fonte de conhecimento aos profissionais e estudiosos da área. Propõe-se como trabalhos futuros, ampliar o mapeamento em busca de outros trabalhos relevantes ao tema, como também aprofundar-se nos conceitos discutidos neste estudo.

REFERÊNCIAS

ALMEIDA, W. D.; NETO, P. S.; AQUINO, F. JA. Estudo Comparativo e Implementação de Técnicas Esteganográficas para Ocultamento de Informações. **Revista de tecnologia da informação e comunicação**. v. 7, n. 2, 2017.

ARAÚJO, A. S. de. Dificuldades de análise Forense em Mídias SSD. **Revista on-line IPOG.** 2019.

BORGES, J. A. D.; PRADO, N. Computação forense: Procedimentos técnicos e operacionais. 2017.

CAMPOS, J. F. **O malware como meio de obtenção da prova em processo penal.** 2019**.**

CARVALHO, D. F. de C. Exploração Tecnológica para Esteganografia em Vídeos Digitais. 2005;

CARVALHO, F. A. B.; EDUARDO, B. de S.; RODRIGUES, A. R. P. Computação forense: Uma aplicação de softwares livres para recuperação de dados digitais. **Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação**, [s. l.], v. 1, n. 9, nov. 2018.

COELHO, L. C. M.; BENTO, R. J. Ferramentas de esteganografia e seu uso na infowar. **I Conferência Internacional de Perícias em Crimes Cibernéticos.** 2004**.**

DIAS, M. A. A. Internet das Coisas: novos desafios na análise forense. Parc. Estrat.. Brasília-DF. v. 24 .n. 48. p. 33-54. jan-jun 2019.

EDUARDO, W. F. E.; IMAMURA, C. Y. M. Desafios da detecção de esteganografia em imagens digitais através de análise de vizinhança. **10° Congresso de Inovação, Ciência e Tecnologia do IFSP.** 2019.

ELEUTÉRIO, P. M. da S.; MACHADO, M. P. Desvendando a computação forense. São Paulo: Novatec, 2019.

ESTEVAN, E. C. Segurança de dados com esteganografia e criptografia. v. 1, n. 1 .2017.

FARIAS, E. da S.; ADONIAS, G. de L.;REGIS, C. D. M. Análise de Similaridade Estrutural de Imagens Esteganografadas com Python.2017.

FILHO, W. L.da S. Uma Proposta de Abordagem para Análise Forense de Sistemas Invadidos por Ransomware. 2018.

FOROUZAN, Behrouz A. Comunicação de Dados e Redes de Computadores. 3a edição. Porto Alegre: Bookman, 2008.

FLORET, C. P.; MARTINS, H. P.; MUSSIO, S. C.; VALIDÓRIO, V. C. Crimes cibernéticos: um comparativo de técnicas de esteganografia. v. 5 n. 09 (2018): **Revista FATEC Sebrae em debate: gestão, tecnologias e negócios**. 2018.

FREITAS, M. P.; JACOBSEN, W.; ROTONDO, G.; ALMEIDA, D.; PINHO, L.;AMARAL, É. Da Computação Forense a Técnica de Esteganografia. Um ensaio sobre a ocultação de informações em sistemas computacionais. v. 7 .2014.

GEOFLLY, L. A.; EWERTON, S. F.; WESLLEY C. S..; CARLOS, D. M. R. Análise Objetiva do Número de Bits Menos Significativos em Esteganografia de Imagens Digitais. **iSys - Revista Brasileira de Sistemas de Informação.** v. 10, n. 3. 2017.

HOELZ, B. W. P. **Uma abordagem Multiagente para o Exame Pericial de Sistemas Computacionais.** 2009. 137f. Dissertação de Mestrado. Universidade de Brasília, Brasília,2009

JULIO, E. P.; BRAZIL, W. G.; ALBUQUERQUE, C. V. N. Esteganografia e suas Aplicações. VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. Rio de Janeiro, RJ, Brasil, 2007.

JÚNIOR, M. A. C. C. **Solid State como fonte de prova no Processo Penal do Brasil.** 2019. 149f. Tese de Doutorado.(Ciência da Computação) - Universidade Federal de Pernambuco, Recife,PE,2019.

KASPERSKY. **Dicas de como se proteger contra crimes cibernéticos**. Disponível: <https:// www.kaspersky.com.br/resource-center/threats/what-is-cybercrime/>. Acesso em: 30 set. 2020.

KITCHENHAN, B. (2004). Procedures for performing systematic reviews. Technical report, Keele University and NICTA.

KUROSE, J. F.; ROSS, K. W. Redes de computadores e a internet. Uma abordagem top-down. São Paulo: Pearson. 2010.

MARTINS, H. P.; VICENTINI, F. R. de S.; OLIVEIRA, H. C. de; GODOY, M. A. de. Técnicas de Segurança Aplicação de Esteganografia em Imagens. v. 5, n. 1 2017.

MESQUITA, P. L. Desafios da forense em dispositivos móveis. **UNISUL.** 2018.

NUNES, M. G.; CARDOSO, F. E. Perícia digital em dispositivos móveis. 2018.

PEREIRA, E. D. V. Investigação Digital: conceitos, ferramentas e estudos de caso. Instituto - Geral de Perícias/RS – **Seção de Informática Forense Universidade do Vale dos Sinos (UNISINOS)** Faculdade de Tecnologia. 2016.

PERERIA, M. L.; JOSÉ, D. A. M. O impacto da Anti Forense na Investigação Digital, um Estudo de caso. 2019.

POSSATTI, L. C.; FILHO, G. N. S.; RESENDO, L. C.; ANDRADE, J. O.; KOMATI, K. S. Um Estudo de Técnicas de Esteganálise em Estego-Imagens com Texto Embutido com LSB. **Braz. J. of Develop**., Curitiba, v. 5, n. 10. 2019.

ROCHA, A. de R. Camaleão. Um Software para Segurança Digital Utilizando Esteganografia. Minas Gerais, 2003.

ROCHA, A. de R. **Randomização Progressiva para Esteganálise**. Dissertação de Mestrado. Universidade Estadual de Campinas. 2006.

ROCHA, M. F. Atuação do perito forense computacional no brasil. **UNISUL.** 2018.

RODRIGUES, A. P. S.; COSTA, E. R.; SOUZA, J. F. de.; TURIBUS, S. N. Análise forense: Técnicas e ferramentas aplicadas em reconstituições de ataques cibernéticos em ambientes corporativos. **Revista Científica Faculdade de Balsas.** 2019. v. 10, n. 2 p. 46-58, 2019.

SANTOS, A. J. dos. Detectando informações ocultas com esteganálise. 2017.

SCANNAVINO, K. R. F.; NAKAGAWA, E. Y.; FABBRI, S. C. P. F.; FERRARI, F. C. **Revisão sistemática da literatura em engenharia de software.** Elsevier. 2017.

SILVA, T. B. F. da. Pericia digital: Estratégias para analisar e manter evidências íntegras em forense computacional. **RIUNI.** 2017.

STALLINGS, W. Criptografia e segurança de redes: Princípios e práticas. Prentice Hall, 8th edition, 2010.

SILVA, T. G. Análise Forense: Técnicas e Reconstituição de Ataques. **Revista on-line IPOG.** 2018.

SILVA, Y. E. da. Computação Forense e Perícia Digital. **Instituto de Pós-Graduação – IPOG.** 2018.

SOUZA, A. G. Etapas do processo de computação forense: uma revisão. **Acta de Ciências e Saúde.** v. 1. n. 5. 2016

TOLENTINO, L. C.; SILVA, W. da; MELLO, P. A. **Perícia Forense Computacional**. 2011. 6 p. Artigo (Graduação em Sistemas de Informação)- Faculdade Projeção, Revista Tecnologias Em Projeção, 2011.

UBALDO, P. F. As dificuldades da forense computacional em discos de estado solido, seus desafios e perspectivas. **RIUNI**, [s. l.], 2017.

VALENTE. J. **Brasil tem 134 milhões de usuários de internet, aponta pesquisa.** Agência Brasil. Disponível: https://agenciabrasil.ebc.com.br/geral/noticia/2020-05/brasil-tem-134-milhoes-de-usuarios-de-internet-aponta-pesquisa. Acesso em: 05 set. 2020

VALLIM, A. P. de A. Forense Computacional e criptografia. São Paulo: Senac, 2019.