Estabraq Hussein Jasim Halboosa, Abbas M. Albakrya

Informatics Institute for Postgraduate Studies Iraq Commission for Computer *and Informatics*
ORCID: 1. 0000-0002-8117-6686, 2. 0000-0001-9518-1024

doi:10.15199/48.2023.05.45

A systematic review: security information for agent approaches in networks - models and methods

***Abstract**. The proliferation of dangers to transmitting vital information across a communication channel has resulted from the advancement of communication systems. One of the security information is hiding secret information using agent approaches for clandestine transmission, protecting against data theft across increasing networks. Hence, it is often employed to address data security concerns. It's difficult to choose the right cover image to hide vital information; therefore, researchers used AI and agent-based algorithms to help secure information hiding. This investigation looked at Web of Science, PubMed, Science Direct, IEEE Xplore, and Scopus. A collection of 658 articles from 2018 to 2022 is gathered to give a better picture and deeper knowledge of academic publications through a final selection of 66 papers based on our exclusion and inclusion criteria. The selected articles were organized by resemblance, objectivity, and goal. First, "cover multimedia selection based on agent approaches" (n = 49). This category contains two subparts: (a) Selection based on agent techniques towards steganography system and (b) Selection based on agent techniques towards steganalysis system" (n = 17). This systematic study highlighted the motives, taxonomy, difficulties and recommendations of cover image selection study employing agent methodologies that require synergistic consideration. In order to execute the recommended research solution for an integrated agent-steganography system, this systematic study emphasizes the unmet obstacles and provides a thorough scientific analysis. Finally, the current study critically reviews the literature, addresses the research gaps, and highlights the available datasets for steganography systems, AI algorithms and agent techniques, and the evaluation matrices collected from the closing papers.*

Streszczenie. Rozprzestrzenianie się zagrożeń związanych z przesyłaniem ważnych informacji przez kanał komunikacyjny wynika z rozwoju systemów *komunikacyjnych. Jedną z informacji o bezpieczeństwie jest ukrywanie tajnych informacji za pomocą agentów do tajnej transmisji, chroniąc przed kradzieżą danych w rozrastających się sieciach. Dlatego jest często używany do rozwiązywania problemów związanych z bezpieczeństwem danych. Trudno jest wybrać odpowiedni obraz na okładkę, aby ukryć ważne informacje; dlatego badacze wykorzystali sztuczną inteligencję i algorytmy oparte na agentach, aby pomóc w zabezpieczeniu ukrywania informacji. Dochodzenie to dotyczyło Web of Science, PubMed, Science Direct, IEEE Xplore i Scopus. Zebrano zbiór 658 artykułów z lat 2018-2022, aby dać lepszy obraz i głębszą wiedzę na temat publikacji akademickich poprzez ostateczny wybór 66 artykułów w oparciu o nasze kryteria wykluczenia i włączenia. Wybrane artykuły zostały uporządkowane według podobieństwa, obiektywności i celu. Po pierwsze, „obejmij wybór multimediów w oparciu o podejście agenta" (n = 49). Ta kategoria zawiera dwie podczęści: (a) Selekcja oparta na technikach agentowych w kierunku systemu steganografii oraz (b) Selekcja oparta na technikach agentowych w kierunku systemu steganalizy" (n = 17). To systematyczne badanie podkreśliło motywy, taksonomię, trudności i zalecenia dotyczące pokrycia badanie selekcji obrazów wykorzystujące metodologie agentów, które wymagają rozważenia synergii. W celu wykonania zalecanego rozwiązania badawczego dla zintegrowanego systemu agent-steganografia, to systematyczne badanie podkreśla niespełnione przeszkody i zapewnia dogłębną analizę naukową. Wreszcie, obecne badanie dokonuje krytycznego przeglądu literatury , odnosi się do luk badawczych i podkreśla dostępne zestawy danych dla systemów steganografii, algorytmów sztucznej inteligencji i technik agentów oraz macierze oceny zebrane z dokumentów końcowych.* (***Przegląd systematyczny: informacje o bezpieczeństwie dla podejść agentowych w sieciach - modele i metody***)

Keywords: Agent Technique, Artificial Intelligence, Information Hiding, Security information, systematic review.
Słowa kluczowe: sztuczna inteligencja, bezpieczeństwo sieci, agent

Introduction

Protecting the transmission of sensitive information has drawn a lot of attention in light of the internet's and information technology's fast expansion [1]–[3]. Data hiding has become essential because to the increasing use of digital communication and multimedia data in modern society. Steganography involves concealing sensitive information within a conventional message that cannot be identified easily [4], [5]. Four factors are primarily used to assess an image steganography technique's performance: payload capacity, imperceptibility, security, and robustness [6]– [8]. Obtaining all of these parameters simultaneously is a complex process. Steganography's major goal is to interact securely with a third party such that private information is hidden from view. Steganography is gaining popularity in internet communication [9], [10] due to cryptography common weakness. While cryptography can safeguard an encoded message, the message visibility exposes it to decoding attacks that a message that is invisible to an eavesdropper avoids [11], [12]. The security of the stego-image depends on choosing the right cover image to hide a particular hidden message [13], [14]. In the past decade, a vast amount of research has been conducted on information hiding, but very few studies have investigated the use of agent approaches and AI algorithms to improve steganographic results. This systematic literature review paper presents a detailed review of the text hiding approach using the steganography system and agents technique through the cover image.

security information: An Overview

It is an important issue to ensure the privacy of the communicated information [15], [16]. In this regard, several strategies have been developed to protect the confidentiality of messages. Occasionally, however, it is necessary to conceal the existence of the communication [7], [17], [18]. To protect communication between two parties from attackers is the core idea behind steganography [4], [19]–[21]. As a result, covert communication may be added to unobtrusive media like computer code, video, or audio recordings [9], [22]. To avoid unintended use of the data, both parties should delete the cover message after data transmission [23], [24]. Techniques for embedding and extracting are needed in order to hide data in any media. The embedding algorithm's goal is to encrypt sensitive information and embed it in a cover media [25] through [28]. In this step, a private key is used to secure the embedding procedure, ensuring that only those with the secret keyword may access the secured data [29]–[32]. The extraction algorithm, in contrast, is applied to an elastic medium and retrieves the buried secret data.

Steganography Categories

Steganography may be divided into three fundamental types: pure steganography, steganography using a secret key, and steganography using a public key [33, 34].

- Pure Steganography: This type does not necessitate the exchange of sensitive information [24], [28], [35]. The mapping E: C ×M→C illustrates the embedding procedure. The extraction process is shown by the mapping D: C→M. Here, C defines the list of potential coverings and M indicates the location of likely hidden messages; │C │≥│M│. However, this lack of security results from the parties' reliance on the idea that others do not possess this intimate knowledge [36]–[39].
- Secret Key Steganography: Steganography with a secret key requires a secret key during communication [40], [41]. Therefore, the sender and recipient must possess the secret key to access and read the communication. This results in increased resilience and security [17], [42], [43].
- Public Key Steganography: The idea of public-key cryptography enhances public-key steganography. This kind utilizes a public key and a private key to preserve communication security [33, 44]–46]; the sender uses the public key throughout the encoding phase. The private key is simultaneously used to decrypt the encrypted message. Although steganography with a public key is more secure, it limits the quantity of hidden information [47, 48] since encryption techniques more than double the message size.

Steganography Usage Challenges

As was already indicated, researchers looking to create secure methods for conveying data without exposing it to anybody outside the intended receiver have always placed a high priority on the security of sensitive information [5, [21], [49], [50]. Multimedia information, such as image data, differs from messages text in that it has special qualities including redundancy, high capacity, and strong pixel correlation [51]–[53]. Additionally, there are certain limitations on the ability of hidden information [20], [54], [55]. Another significant issue is that images lose some data and lose quality when they are hidden. Data Capacity: Increasing the capacity of a cover object's concealed information has always been a key worry since doing so decreases the image quality and might tip off an attacker that anything is hidden [28], [54], [56]-[58]. Visibility: The stego-image appearing normal during transmission when neither computers nor humans can detect any distortion in it [59], [60]. Detectability: When a computer can't tell the difference between the cover image and the stego-image, or when an attacker with access to the original image can easily see that something is hidden. [61], [62]. Robustness is the capacity of communication to withstand compression and other alterations [63]–[65].

Systematic Review Protocol

The protocol for the systematic literature review (SLR) was intended to meet the purpose of this review paper by addressing the research issues described in the previous section. The protocol was primarily comprised of the specifications for conducting the SLR. First, Sections A and B focus on identifying prospective bibliographic databases, creating inclusion/exclusion criteria, and selecting research papers. Each article was meticulously scanned in the second stage, and pertinent papers were extracted, as described in Section C.

A. Conducting the SLR Method

This study was based on a systematic literature review, which conducts the "Preferred Reporting Items for Systematic reviews and Meta-Analyses" (PRISMA) guideline. The reason for this kind of evaluation is to gather reliable studies from different databases. Between 2018 and 2022, a comprehensive search for English-language articles was conducted in the five major digital databases WoS, IEEE, PubMed, SD and Scopus. Due to their vast coverage, these indexes were chosen. Given that the agent method trends have been highly active in steganography system applications in recent years, the majority of studies were relevant to our study. This research employed query search using different keywords associated with the steganography system (e.g., "Text Hiding" OR " Steganography" OR "Information Hiding") and keywords that deliberated all these terms established under the concept of agent technique (e.g., "Agent Technique" OR " Artificial Intelligence" OR "AI"). As shown in Table I, the query is used to support the search for diverse studies for designing an integrated steganography system within all these terms supporting agent technique and AI algorithms.

TABLE 1: Literature review query

Query Details Terms	Databases Result	Final Results

("Text Hiding" OR " Steganography" OR "Information Hiding") AND ("Agent Technique" OR " Artificial Intelligence" OR "AI")	IEEE=67
	SD=313
	Scopus=232
	Pubmed=27
	WoS=19
		658 Articles

B. Identifying Potential Research Articles

To find relevant research publications, we established exclusion criteria and inclusion criteria. Criteria for inclusion in SLR existed reviewed publications on the design of integrated steganography systems employing AI authored in English and published in international conference proceedings and journals. The intelligent agent approach architecture is used to construct or support the analysis of the case-control context of these studies. The criteria for exclusion from the SLR were publications related to the philosophy of steganography and papers not published in any conference proceedings or journals. Additionally, studies focusing on the steganography system but unconnected to the agent technique field, and vice versa, are also omitted. Throughout the study selection procedure, inclusion and exclusion criteria were evaluated.

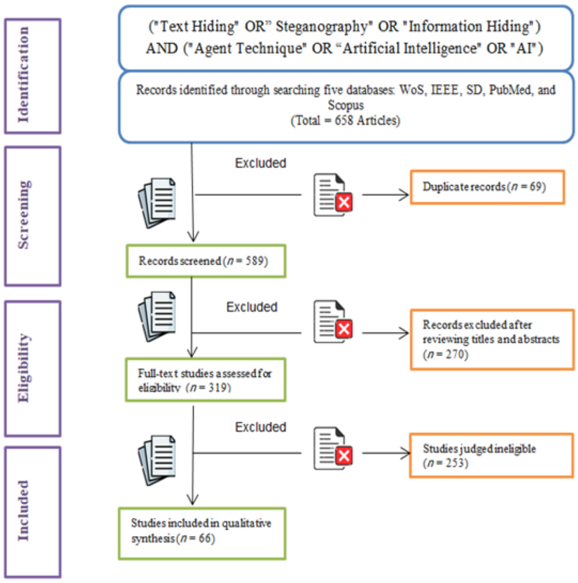
Identification
("Text Hiding" OR" Steganography" OR "Information Hiding")
AND ("Agent Technique" OR "Artificial Intelligence" OR "AI")
Records identified through searching five databases: WoS, IEEE, SD, PubMed, and Scopus
(Total = 658 Articles)
Screening
Excluded
Duplicate records (n = 69)
Records screened (n = 589)
Eligibility
Excluded
Records excluded after reviewing titles and abstracts (n = 270)
Full-text studies assessed for eligibility (n = 319)
Excluded
Studies judged ineligible (n = 253)
Included
Studies included in qualitative synthesis (n = 66)

Fig. 1: Schematic flowchart showing how to find, screen, and include relevant studies.

C. Systematic Review Results

About 658 papers from five databases were included in the first rounds of the research selection procedure. A total of (n = 69) papers were disqualified after the duplicates were eliminated. So the number of items to remember is (n = 589). A total of (n = 319) articles were found after the second screening process, which included scanning the titles and abstracts. Reading the whole text of the articles found in the previous stage's identification was the next step in the screening procedure. 66 publications in all were assessed and determined to be relevant to the review based on our criteria. Fig. 1 depicts the flowchart for the schematic approach phase.

Taxonomy Results

Taxonomy is used in agent-based steganography to determine the analytical dimension of the final collection of articles and to understand their philosophical underpinnings in order to connect them systematically. This makes it simpler for academics to understand agent-based steganography research without the overall complication and overlap of AI ideas. Based on evidence of similarity, objectivity, and purpose across studies, the chosen articles were divided. There are two major categories into which they are separated: the first is "cover multimedia selection based on agent approaches" (n = 49). A subset of this category is made up of the following two categories: (a) Selection based on agent methods towards steganography system, and (b) Selection based on agent techniques towards steganalysis system. "Cover multimedia selection based on features" (n = 17) makes up the second category. According to their overlap and topic content, the publications were classified and arranged using a strong taxonomy, as shown in Fig. 2.

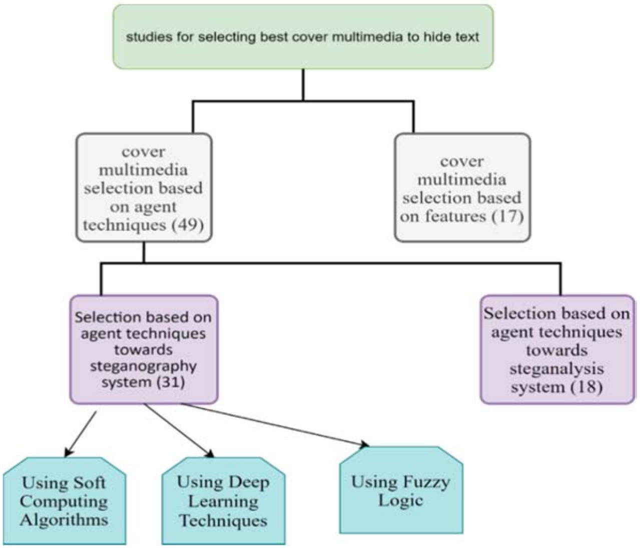
studies for selecting best cover multimedia to hide text
cover multimedia selection based on agent techniques (49)
cover multimedia selection based on features (17)
Selection based on agent techniques towards steganography system (31)
Selection based on agent techniques towards steganalysis system (18)
Using Soft Computing Algorithms
Using Deep Learning Techniques
Using Fuzzy Logic

Fig. 2: Taxonomy of study publications on cover multimedia selection depended on agent techniques.

A. Cover multimedia selection based on agent techniques

This category covers (49/66) studies and includes two main sections: selection based on agent techniques toward steganography system and selection based on agent techniques toward steganalysis system. Previously, steganography has not been combined with agent techniques. The new challenge is effectively connecting them to hide information inside the container image. The cover-image is recognized based on the compatibility between secret text and stego-image. The embedding method may result in little modifications to the stego-image.

B. Selection based on agent techniques toward steganography system

The primary objective of incorporating AI into a steganography system is to choose the right stego-image and embed the payload data at the same time to improve the quality of the stego-image, which is a difficult task. AI methods are used to make the process of choosing cover multimedia from the huge database less complicated. The techniques for steganography systems are soft computing, deep learning techniques, and fuzzy logic.

- Using Soft Computing Algorithms: Most neural network applications focus on invisibility and robustness by exploiting their learning power to provide a superior image. Soft computing algorithms determine the optimal bit positions for information embedding and enhance the payload limit. They are often used to augment the imperceptibility of stego-images by making the blocks of images easier to recognize by comprehending the connection between the cover image and the hidden information. Based on the Bats method, the research of [71] suggested a steganography algorithm for information hiding within the cover image using an LSB approach. In this research, many cover pictures and texts of various sizes were tried. The authors measured the quality of the photos after encryption using a number of accepted standard metrics. These standards' findings show that PSNR is very high and MSE is extremely low, proving that the suggested method is effective at hiding the data within the image. In this work [72], hidden text was generated using the ant colony optimization algorithm. First, a carrier picture for the hidden text is chosen, and then a collection of rows are utilized as input for the ant colony optimization process. The outcomes of the experiment showed that the stego images had a good quality and a low histogram changeability, which provided support for the recommended technique. It's challenging to predict concealing pixels and the sequence of hidden bits.
- The authors of this study [14] devised a novel gravity search technique to discover the most effective and efficient sites in a carrier picture for concealing hidden information. It is challenging to choose a good cover image and hide the secret-data to improve their invisibility. An impossible selection job with trillions and millions of possible permutations may be explored with the help of a genetic algorithm. The researchers in [27] determined that the cover-image is chosen so that LSB of the cover-mage and the payload image have a greater grade of compatibility and that genetic algorithm-based hiding process introduced minor modifications to the resulting stego-image. [73] employs a Bit Mask-Oriented Genetic Algorithm (BMOGA) to decrease the duplication of health test data transmitted between administrations. BMOGA incorporates cryptographic elements for secure data transport. Data that has been encrypted may be included into medical imaging via the use of 1-level and 2-level Discrete Wavelet Transform (DWT). The BMOGA inverse technique is implemented to extract secret messages from encrypted ones. A two-fold methodology was proposed by the paper [74]. First, the Ballot transform (BaT) is applied to each non-corresponding m-pixel group of the stego-image to generate an integer-polynomial series in coefficient form. Second, GA was used to generate a k-digit password using Index Value Mapping (IVM), which found the coefficient positions where bits of sensitive data may be inserted. In lieu of completing an extensive search of all conceivable combinations of k bits, this application of GA aimed to provide the greatest quality stego-image output. The research [75] proved that the correct embedding coefficients are selected using a local neighborhood analysis-derived edge intensity criteria. The suggested technique starts by applying a wavelet transform on each image block. Several coefficients are identified in each high frequency sub band, and then the

coefficients are selected using a genetic algorithm such that the resulting stego image has the highest PSNR value.

- The authors of this study [76] present a GA-based technique for lossless spatial domain image steganography focusing on security. By choosing appropriate locations to cover 2 bits of secret data in each pixel, it is possible to hide a stream of private information in a quarter of an image, which leads to the creation of factors corresponding to the position of the match using a genetic algorithm. The paper [77] presented a new data hiding method integrated to blockchain technique in the geographical realm, described in three steps. To start, the pre-hiding process involves figuring out the maximum number of inserts that may be made into each host image. The second level of data concealment for COVID-19 used the hash functionand Particle Swarm Optimization (PSO) method. Finally, blockchain technology is used in the transmission step to send the stego images to all hospitals in the linked network and to update their information. A multi-agent method for secure data transfer was given in this study [78], which used steganography as its foundation. Agents send/receive messages from a terminal. One terminal's agent encrypts/decrypts messages using steganography and transfers them to another terminal. Whereas the study [43] developed a steganography technique using LSB and the agent technology architecture. Histogram, mean, standard deviation, entropy, variance, and energy were statistically measured. Using ROC, a steganography Ensemble classifier evaluated the given metrics. The results showed the agent-based system could choose the appropriate cover image for the secret message size to avoid visual artefacts. In article [79], researchers trained a model for stego-image selection using an unsupervised Neural Network (NN). The reduction of data loss that occurs as a consequence of using transformation methods and chaotic structures, such as the integer wavelet transform, produces favorable outcomes in a professional setting.
- Using Deep Learning Techniques: The use of deep learning for the purpose of information hiding has progressed considerably over the years. Because a component of deep learning's model, characteristics, and processes correspond to those of information concealing, it is possible to apply deep learning to the area of information concealment.
- According to the study, deep learning models' black-box feature reduces the need for specialized expertise when creating data-hiding strategies and boosts security. To conceal a hidden image behind another cover image, researchers from [80] used deep neural networks (DNN), steganography, and cryptography. The authors used some public steganography methods, and integrating them with NN and cryptography makes breaking them arduously. Automatically creating text covers from a discontinuous input stream is the goal of the Recurrent Neural Networks (RNN-Stega) algorithm that was developed in [81]. For the purpose of researching the conditional distribution of encoding words, both variable and fixed-length coding (VLC and FLC) are used. Experiments demonstrated a strong capacity for embedding and a high level of protection against harmful attempts. In [82], a faster region-based CNN (R-CNN) technique was introduced. The cover image is processed by an R-CNN to expedite the feature extraction selection. These regions are boxed using Softmax loss, and specific steganographic methods are assigned to the boxed parts. The ADV-EMB adversarial embedding steganography technology was developed as a result of the study referenced in [83]. The proposed work was capable of concealing data and tricking a based convolutional neural networks steganalyser. The encoding network includes a distortion mineralization architecture that adjusts and reduces the cost of the image.
- The study [84] offered a DNN method that steganography, integrity protection and integrates encryption to preserve the secret diagnostic systems of a picture. The DNN is used for data preprocessing, hiding images, and showing the stego image, which are each done separately by revealing network, hiding network and preparation network. The research [85] suggested a unique steganography technique based on the translation of two images by adding a steganalysis module and steganography module to Cycle Generative Adversarial Network (CycleGAN) to accommodate the IoT's covert communication and privacy protection.
- Using Fuzzy Logic: Zadeh developed the idea of fuzzy logic (FL) in the 1960s. In computer programming, fuzzy logic aims to mimic human thought [20]. It is possible to figure out an item's membership status using fuzzy logic. As indicated by the literature, the fuzzy logic-based steganography technique will be used due to its capacity to cope with the high level of image uncertainty. Consequently, this method can preserve imperceptibility.
- Adaptive steganography based on innovative fuzzy edge identification was developed in the work [86]. After inserting the secret message, the suggested method effectively conceals the image's specific edge areas and ensures the exact edge location. In contrast, the authors of [87] increased the number of edge pixels and added more secret data to edge pixels than non-edge pixels utilizing the LSB replacement method by employing type-2 fuzzy logic systems and edge detection algorithms. The effectiveness of the suggested approach will be assessed by contrasting the original image with the stego-image using metrics like Histograms, Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). The research [88] also provided an adaptive hybrid approach for image steganography based on bit reduction, pixel correction, fuzzy logic, and integer wavelet transform to conceal data in the stego-image.

C. Selection based on agent techniques toward steganalysis system

Using a wide range of techniques, AI is increasingly frequently employed to find hidden data in images.

AI-based steganalysis techniques have four steps: collecting and processing data, building and training the model, testing the model, and evaluating the model and the AI model. Training data can be put into groups and organized in a certain way to make the procedure more accurate. The best thing about using AI in steganalysis is that it makes it easier to find secret messages. This is because the model is trained on large, normalized data sets.

The people who wrote the paper [89] suggested deep residual learning as a method for picture steganography. The proposed CNN model has more depth than other CNN-based models because it uses residual learning to keep the weak steganographic signal. The model had three parts: the high-pass filtering (HPF) module, which removes noise from the input images; the CNN model, which learns the features and makes the final feature matrix; and the classification module, which gives the final result. CNN can easily pull out the features that define the image's content, but it's hard to pull out the subtle features that indicate the existence of confidential information. Taking this into account, the study's researchers [90] made separate convolution and adversarial algorithms and proposed a new network layout that effectively fixes the problem. Separable convolution optimizes the residual information by using the correlation between the channels. With the adversarial method, the generator pulls out more content features to trick the discriminator and hide more steganographic information.

Quantitative steganalysis tries to figure out how big a hidden message is once it is known that a picture contains sensitive information. Taking into account the recent progress that deep learning has made in binary steganography, the paper [47] proposed a method for quantitative steganography based on deep learning regressors. When the Softmax loss function is replaced with the MSE loss function, a binary classifier becomes a qualitative regressor, and the embedded payloads are used as continuous-valued class labels. At the same time, the researchers in study [91] showed a linguistic steganalysis technique that uses two-level cascaded CNNs to find the hidden texts made by synonym substitution. Sentence-Level CNN is a product for beginning users. It has a layer that combines sentences of different lengths and a layer that is connected to other layers to hide information. The output from the previous level is used by the text-level CNN at the next level of the network to tell the difference between stego and normal text. A text steganography CNN (TS-CNN) algorithm was proposed in [92]. In the work they submitted, the authors used two models: TS-CNN (Single) and TS-CNN (Multi) to get the semantic coherence between sentences and the expression of each sentence's internal semantics, respectively.

In contrast, the research [31] offered a model for highly linked Long short-term memory (LSTM). Feature pyramids were leveraged by the LSTM model to build a large variety of low-level features capable of recognizing generative text steganographic approaches. Multiple bidirectional Long Short-Term Memory (Bi-LSTM) networks were used to achieve a variety of semantic feature levels. The authors of this study [93] present IAS-CNN, a lightweight convolutional neural network designed for image adaptive steganalysis. To overcome the constraint of manually creating residual extraction filters, they employed the network-based self-learning filter approach.

Discussion

After extracting information from the collected articles, this section aims to highlight and discuss three fundamental concepts: (1) the motivations, benefits, and significance of the topics that prompted researchers to highlight and seek solutions to problems; (2) the challenges and what former and current researchers experience in the presented situations and hurdles; and (3) the recommendations made by the authors and the future work to be implemented in the steganography research path based on the agent technique.

A. Motivations

In steganography, a vast quantity of confidential data is concealed in cover media to protect it from eavesdroppers and unauthorized individuals [76]. To ensure the invisibility of secret messages, complex texture objects should be chosen for embedding information [82], [94], [95]. The encrypted data reduce suspicion of illegal attackers. Adaptive steganography is designed to counteract this vulnerability by injecting secret information into a cover medium without drawing the adversary's attention [86]. Simultaneously, the demand for data authentication and robust data integrity management methods has constantly been increasing [96]–[98]. Therefore, selecting an appropriate cover image to conceal a specific secret message is crucial for the security of the stego-image [27]. According to the literature, there is no consensus on using deep learning in reversible steganography. The perception that the perfect reversal of steganographic distortion is unattainable due to the lack of transparency and interpretability of neural networks [99] contributes to the underdevelopment of the field of reversible steganography using deep learning. The collected articles showed a need to integrate neural networks with a steganography system for efficient and accurate training results [79]. Image steganography face very high uncertainty levels [87], [88], [100]. Since the communication route in data transmission is public, the risk of data leakage and extortion in IoT is gradually increasing with its massive deployment. Consequently, IoT security has become a significant issue in information security [83], [85].

B. Challenges

This paper addresses the difficulties researchers face in selecting the optimal cover image for information concealment. Embedding image information into image information without any help from traditional steganography methods to raise image steganography payload capacity and suppress noise pixels generated by generator network are the main challenges [101]–[103]. Although the applied cryptographic method is quite simple, it is effective when combined with DNN. Other steganography techniques efficiently conceal data in a uniform, less certain pattern [73], [80]. The transform-based algorithms [5], [104], [105] partially solve issues like robustness and imperceptibility in image steganography. Updating and transmitting vast quantities of healthcare data securely and effectively is necessary yet difficult [106]. More COVID-19 patients' private health information is gathered and shared between hospitals and clinical laboratories [77]. It is challenging for the monitor to detect abnormalities during stego-transmission so that secret information can be transferred discreetly. To protect communication, researchers are introducing steganographic technologies to the IoT [85], [102], [107]. How to effectively balance the security of image steganography and the amount of confidential information is a challenge in the direction of information-hiding research based on deep learning [107]–[109].

C. Recommendation and Future Work

The purpose of this section is to talk about some suggestions and some guidelines regarding agent-based steganography. According to the literature, many studies recommended designing a multi-processing multi-agent software to handle comparative studies with diverse techniques and produce a particular dataset from all available steganography datasets with unified features and parameters [43], [110]. Others recommended using different algorithms for data embedding, such as frequency domain algorithms [71]. It is also highly advised to look into the possibility of developing cryptographic algorithms that are compatible with neural networks [68], [111], and [113]. Several steganography techniques can be incorporated with neural networks. It is also fascinating to study the idea of combining several pretreatment predictors and post-processing neural network models to increase the accuracy of predictions. Many studies recommended integrating neural nets with audio files [85], [95], [114]. In the field of improving algorithms, the studies of [91] and [92] recommend improving the sentence-level CNN so that it can extract more efficient steganographic characteristics and enhance the performance of both sentence-level and text-level steganalysis techniques. Others concentrated on reducing the timing complexity and explored the option of utilizing multiple sequence generators that offer greater control over sequence formation [27], [76]. New techniques that minimize the noise are suggested to be applied to achieve better information hiding in images using texture segmentation [38], [115]. Whereas the articles [82], [85], and [91] recommended the aspects of hiding a secret message in the foreground completely, switching to different object detection methods and adjusting the steganography algorithm adaptively.

Regarding testing the performance of the proposed system, many studies recommended using the efficiency matrices PSNR, MSE and Histograms [116], [117]. According to [75], [93], [118], and [119], one way to expand the variety of features extracted is to use multiple filters to obtain residuals, and then to generate a minimum residual map and a maximum residual map for use in subsequent feature extraction. This would increase the diversity of feature extraction.

A Critical Analysis of the Literature

In this part, three intricate and important section analyses that are linked with the present subject of this paper are described.

A. Available Datasets Used with AI

The number and type of datasets utilized in previously published studies are variable. In this situation, identifying the most significant dataset that may influence the selection of the cover image is questionable. Many studies used standard images like 'Lena', 'Peppers',' Baboon', 'Mona Lisa' to test their proposed work [71], [72], [76], [87] . According to the literature, the three most used datasets are ImageNet, BOWS2 and BOSSbase, as mentioned in Table II. Regarding the number of datasets that were utilized, the studies of [27], [75],[82], [85], [86], and [101] used only one dataset to train and test the work; others used two or more [73], [83], [94]. Other investigations were conducted without a transparent dataset to show their framework conclusions [77], [88], [120].

B. Utilization of Agent Techniques

Multidisciplinary research is modelling agent techniques and AI algorithms to produce more accurate results. Consequently, various articles on text steganography employing agent strategies are included in Table II. Table II provides information on extracted and established datasets from the research literature, as well as information on algorithmic methodologies. This data can help develop new methodologies and adopt one of the case studies shown in this table. The methods utilized in this research were collected from a literature review and are given in Table II. These data might be used to build new approaches, or they could be used to adopt one of the case studies included in this table. A literature review served as the primary source for the collection of this study's methodologies, which are detailed in Table II. The GA algorithm was used most frequently, followed by the CNN and GAN algorithms. The GA algorithm is efficient when it achieves the best outcomes.

C. Utilization of Evaluation Methods

The algorithms used in this literature were evaluated according to the metrics (Accuracy, MSE, PSNR, SSIM, AD, Correlation, Structural Content (SC), Entropy, Cumulative Frequency, ROC Curve and Total Error Rate) used in each articles [75],[82], [85], and [86]. As demonstrated in Table II, most evaluated research anticipated good accuracy and performance, even though the outcomes of these strategies differed from study to study. In addition, there are a variety of other evaluation methods that vary according to the type of study. Other measures, such as Entropy, Cumulative Frequency, and ROC Curve, have received minimal attention without justification, although accuracy, MSE, PSNR, SSIM, and RMSE have been widely employed [71], [72], [75],[82], [94].

TABLE 2: Description of the dataset utilized and data extraction from the systematic review of the literature.

Ref	Year	Dataset	Agent tech.	Evaluation metrics
[101]	2018	ImageNet	CNN	-
[94]	2018	DTD, COCO2017	GAN and CNN	MSE, PSNR, SSIM
[76]	2018	standard images	GA, LCG	MSE, PSNR
[82]	2018	COCO2014	Faster R-CNN	MSE, PSNR, SSIM
[71]	2018	standard images	Bats Algorithm	MSE, PSNR
[88]	2018	-	hybrid fuzzy logic	MSE, PSNR
[83]	2019	Basic500k, PEG-BOSSBase	ADV-EMB	total error rate
[95]	2019	ImageNet	U-Net CNN	MSE, PSNR, SSIM
[85]	2019	ImageNet	CycleGAN	Freìchet Inception Distance (FID), Inception score (IS)
[86]	2019	BOWS2	FIS	MSE, PSNR, SSIM, AD
[80]	2019	Flickr30k	DNN, ADAM	MSE
[87]	2019	standard images ('Lena', 'Peppers',' Baboon', 'Mona Lisa')	Type-2 Fuzzy Logic	MSE, PSNR
[81]	2019	sentiment140, IMDB	RNN-Stega	Accuracy
[73]	2020	DME Eyes, DICOM	BMOGA	MSE, PSNR, SSIM, correlation, structural content (SC)
[102]	2020	ImageNet	SteganoCNN	MSE, PSNR, SSIM
[99]	2021	BOSSbase	LSTM w/ CNN	Entropy, cumulative frequency, regression analysis
[43]	2021	BOSSbase	LSB and Ensemble classifier	ROC Curve
[120]	2021	-	RNN-Stega, RNN-generated Lyrics	-
[27]	2021	Crowd	GA	RMSE, PSNR, SSIM
[77]	2021	-	PSO, hash function.	MSE, PSNR
[90]	2021	BOSSBase1.01, BOWS2	Separable CNN, GAN	Accuracy
[72]	2021	standard images ('Lena', 'Peppers',' Baboon')	ACO	-
[75]	2022	BOWS2	WCBLG	RMSE, PSNR, SSIM

Conclusion

The goal of this work is to do a full literature review on agent-based steganography systems. This will help a large number of scholars and professionals in this field, especially in figuring out that picking the best cover image is expensive and takes a lot of time. This study offered descriptive information regarding selecting cover images in the context of agent approaches and AI contributions. Evaluating several publications showing the advantages, difficulties, and recommendations associated with agent-based steganography and identified distinct gaps. In this systematic review, the significant findings for designing a superior concealing algorithm in image data hiding that may preserve imperceptibility and boost robustness have been discussed in detail. We have analyzed and compiled the findings from 166 works on steganography and steganalysis and have produced an overview of these papers. The retrieved data demonstrated that the algorithms effectively achieve the three primary aims of information concealment: invisibility, payload capacity, and robustness. It is believed that the system theoretically benefits from extremely exact data extraction and the ability to thwart the identification of image steganalysis techniques, producing payloads of higher quality and more excellent stability. In order to integrate agent techniques with cover image selection and evaluate the methods using efficiency matrices, this study recommended building a new framework that can handle methodology.

Authors: Estabraq Hussein Jasim Halboosa*, Email:* ms202030596@iips.icci.edu.iq*; Abbas M. Albakrya, Email:* abbasm.albakry@uoitc.edu.iq.

REFERENCES

[1] R. F. Mansour and M. R. Girgis, "Steganography-based transmission of medical images over unsecure network for telemedicine applications," *Comput. Mater. Contin.*, vol. 68, no. 3, pp. 4069–4085, 2021.

[2] M. M. Sayah, K. M. Redouane, and K. Amine, "Secure transmission and integrity verification for color medical images in telemedicine applications," *Multimed. Tools Appl.*, 2022.

[3] J. Dey, A. Sarkar, S. Karforma, and B. Chowdhury, "Metaheuristic secured transmission in Telecare Medical Information System (TMIS) in the face of post-COVID-19," *J. Ambient Intell. Humaniz. Comput.*, 2021.

[4] R. Gurunath and D. Samanta, "Advances in text steganography theory and research: A critical review and gaps," in *Multidisciplinary Approach to Modern Digital Steganography*, 2021, pp. 50–74.

[5] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, 2019.

[6] V. H. Iyer, S. Mahesh, R. Malpani, M. Sapre, and A. J. Kulkarni, "Adaptive Range Genetic Algorithm: A hybrid optimization approach and its application in the design and economic optimization of Shell-and-Tube Heat Exchanger," *Eng. Appl. Artif. Intell.*, vol. 85, pp. 444–461, 2019.

[7] S. Liu and D. Xu, "A robust steganography method for HEVC based on secret sharing," *Cogn. Syst. Res.*, vol. 59, pp. 207–220, 2020.

[8] I. Oregi, J. Del Ser, A. Pérez, and J. A. Lozano, "Robust image classification against adversarial attacks using elastic similarity measures between edge count sequences," *Neural Networks*, vol. 128, pp. 61–72, 2020.

[9] H. T. S. Alrikabi and H. T. Hazim, "Enhanced Data Security of Communication System Using Combined Encryption and Steganography," *Int. J. Interact. Mob. Technol.*, vol. 15, no. 16, pp. 144–157, 2021.

[10] N. Uniyal, G. Dobhal, A. Rawat, and A. Sikander, "A Novel Encryption Approach Based on Vigenère Cipher for Secure Data Communication," *Wirel. Pers. Commun.*, vol. 119, no. 2, pp. 1577–1587, 2021.

[11] Halboos, E.H.J. and Albakry, A.M., 2022. Hiding text using the least

significant bit technique to improve cover image in the steganography system. *Bulletin of Electrical Engineering and Informatics*, 11(6), pp.3258-3271.

[12] Alhyani, N.J., Hamid, O.K. and Ibrahim, A.M., 2021. Efficient terrestrial digital video broadcasting receivers based OFDM techniques. *Przegląd Elektrotechniczny*, 97.

[13] P. Bedi and A. Singhal, "Estimating cover image for universal payload region detection in stego images," *J. King Saud Univ. - Comput. Inf. Sci.*, 2022.

[14] O. Younis, "Hiding a Secret Information in Image Using Gravitational Search Algorithm," *Diyala J. Pure Sci.*, vol. 14, no. 1, pp. 44–56, 2018.

[15] R. Bala Krishnan, N. Rajesh Kumar, N. R. Raajan, G. Manikandan, A. Srinivasan, and D. Narasimhan, "An Approach for Attaining Content Confidentiality on Medical Images Through Image Encryption with Steganography," *Wirel. Pers. Commun.*, 2021.

[16] J. Wu *et al.*, "A High-Security mutual authentication system based on structural color-based physical unclonable functions labels," *Chem. Eng. J.*, vol. 439, p. 135601, 2022.

[17] U. Khadam, M. M. Iqbal, S. Saeed, S. H. Dar, A. Ahmad, and M. Ahmad, "Advanced security and privacy technique for digital text in smart grid communications," *Comput. Electr. Eng.*, vol. 93, p. 107205, 2021.

[18] C.-F. Lee, C.-C. Chang, X. Xie, K. Mao, and R.-H. Shi, "An adaptive high-fidelity steganographic scheme using edge detection and hybrid hamming codes," *Displays*, vol. 53, pp. 30–39, 2018.

[19] I. J. Kadhim, P. Premaratne, and P. J. Vial, "Improved image steganography based on super-pixel and coefficient-plane-selection," *Signal Processing*, vol. 171, p. 107481, 2020.

[20] R. Meng, Q. Cui, Z. Zhou, Z. Li, Q. M. Jonathan Wu, and X. Sun, "High-Capacity Steganography Using Object Addition-Based Cover Enhancement for Secure Communication in Networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 2, pp. 848–862, 2022.

[21] A. Ahyuna, S. Syamsuddin, H. Hasriani, A. Ardimansyah, I. Irmawati, and S. Wahyuni, "The Application Of LSB Steganography For Secure Text and Hiding Confidential Information Using AES Cryptography," in *2021 3rd International Conference on Cybernetics and Intelligent System (ICORIS)*, 2021, pp. 1–5.

[22] W. Xiao, M. Li, M. Chen, and A. Barnawi, "Deep interaction: Wearable robot-assisted emotion communication for enhancing perception and expression ability of children with Autism Spectrum Disorders," *Futur. Gener. Comput. Syst.*, vol. 108, pp. 709–716, 2020.

[23] S. A. El_Rahman, "A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information," *Comput. Electr. Eng.*, vol. 70, pp. 380–399, 2018.

[24] J. Li, X. Luo, Y. Zhang, P. Zhang, C. Yang, and F. Liu, "Extracting embedded messages using adaptive steganography based on optimal syndrome-trellis decoding paths," *Digit. Commun. Networks*, 2021.

[25] M. Zheng, J. Jiang, S. Wu, S. Zhong, and Y. Liu, "Content-adaptive selective steganographer detection via embedding probability estimation deep networks," *Neurocomputing*, vol. 365, pp. 336–348, 2019.

[26] J. Lin, Y. Wang, M. Han, Y. Yang, and M. Lei, "A Lightweight Embedding Probability Estimation Algorithm Based on LBP for Adaptive Steganalysis," in *Proceedings of the 2021 IEEE International Conference on Progress in Informatics and Computing, PIC 2021*, 2021, pp. 352–357.

[27] M. K. K. Shyla, K. B. B. S. Kumar, R. Kumar, and R. K. Das, "Image steganography using genetic algorithm for cover image selection and embedding," *Soft Comput. Lett.*, vol. 3, p. 100021, 2021.

[28] I. J. Kadhim, P. Premaratne, and P. J. Vial, "High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform," *Cogn. Syst. Res.*, vol. 60, pp. 20–32, 2020.

[29] S. M. Hashim and D. A. Alzubaydi, "Identify the Presence of Hidden Information Based on Lower Coefficients Value of 2DHWT Sub-bands," in *Proceedings of the 7th International Engineering Conference "Research and Innovation Amid Global Pandemic", IEC 2021*, 2021.

[30] Y. Luo, C. Yao, Y. Mo, B. Xie, G. Yang, and H. Gui, "A creative approach to understanding the hidden information within the business data using Deep Learning," *Inf. Process. Manag.*, vol. 58, no. 5, 2021.

[31] H. Yang, Y. Bao, Z. Yang, S. Liu, Y. Huang, and S. Jiao, "Linguistic Steganalysis via Densely Connected LSTM with Feature Pyramid," in *Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security*, 2020, pp. 5–10.

[32] A. M. Kadan and I. A. Sazanovetz, "Detection of hidden information in graphic files using machine learning," in *CEUR Workshop Proceedings*, 2021, vol. 2834, pp. 185–194, [Online].

Available: https://www.scopus.com/inward/record.uri?eid=2-2.0-103255260&partnerID=40&md5=c63b55781162b0bf787d2abb70cd1ca7.

[33] S. Çalkavur, "Public-Key Cryptosystems and Bounded Distance Decoding of Linear Codes," *Entropy*, vol. 24, no. 4, 2022.

[34] P. Sarosh, S. A. Parah, G. M. Bhat, A. A. Heidari, and K. Muhammad, "Secret Sharing-based Personal Health Records Management for the Internet of Health Things," *Sustain. Cities Soc.*, vol. 74, p. 103129, 2021.

[35] A. Anuradha and H. B. Pandit, "Unique Stego Key Generation from Fingerprint Image in Image Steganography," *Smart Innovation, Systems and Technologies*, vol. 196. pp. 33–42, 2021.

[36] J. J. Ranjani and C. Jeyamala, "Chapter 9 - Machine learning algorithms for medical image security," in *Intelligent Data-Centric Systems*, A. K. Singh and M. B. T.-I. D. S. S. for e-H. A. Elhoseny, Eds. Academic Press, 2020, pp. 169–183.

[37] M. Haghi Kashani, M. Madanipour, M. Nikravan, P. Asghari, and E. Mahdipour, "A systematic review of IoT in healthcare: Applications, techniques, and trends," *J. Netw. Comput. Appl.*, vol. 192, p. 103164, 2021.

[38] A. Iskhakova, A. Iskhakov, R. Meshcheryakov, and E. Jharko, "Method of Verification of Robotic Group Agents in the Conditions of Communication Facility Suppression," *IFAC-PapersOnLine*, vol. 52, no. 13, pp. 1397–1402, 2019.

[39] S. A. Chaudhry, T. Shon, F. Al-Turjman, and M. H. Alsharif, "Correcting design flaws: An improved and cloud assisted key agreement scheme in cyber physical systems," *Comput. Commun.*, vol. 153, pp. 527–537, 2020.

[40] M. Saračević, S. Adamović, V. Miškovic, N. Maček, and M. Šarac, "A novel approach to steganography based on the properties of Catalan numbers and Dyck words," *Futur. Gener. Comput. Syst.*, vol. 100, pp. 186–197, 2019.

[41] H. Kang, H. Wu, and X. Zhang, "Generative text steganography based on LSTM network and attention mechanism with keywords," *IS T Int. Symp. Electron. Imaging Sci. Technol.*, vol. 2020, no. 4, pp. 1–8, 2020.

[42] N. Wu *et al.*, "STBS-Stega: Coverless text steganography based on state transition-binary sequence," *Int. J. Distrib. Sens. Networks*, vol. 16, no. 3, 2020.

[43] F. A. Baothman and B. S. Edhah, "Toward agent - based LSB image steganography system," pp. 903–919, 2021.

[44] P. Wang, B. Chen, T. Xiang, and Z. Wang, "Lattice-based public key searchable encryption with fine-grained access control for edge computing," *Futur. Gener. Comput. Syst.*, vol. 127, pp. 373–383, 2022.

[45] K. Vandana and S. K. Kumari, "Improving Security with Efficient Key Management in Public cloud using Hybrid AES, ECC and LSB Steganography comparing with Novel hybrid Cube Base Obfuscation," in *2022 International Conference on Business Analytics for Technology and Security, ICBATS 2022*, 2022, vol. 2022-Janua.

[46] M. Walshe, G. Epiphaniou, H. Al-Khateeb, M. Hammoudeh, V. Katos, and A. Dehghantanha, "Non-interactive zero knowledge proofs for the authentication of IoT devices in reduced connectivity environments," *Ad Hoc Networks*, vol. 95, p. 101988, 2019.

[47] M. Chen, M. Boroumand, J. Fridrich, and S. Binghamton, "Deep learning regressors for quantitative steganalysis," *Electron. Imaging*, vol. 2018, pp. 1–7, 2018.

[48] Y. Li, J. Zhang, Z. Yang, and R. Zhang, "Topic-aware Neural Linguistic Steganography Based on Knowledge Graphs," *ACM/IMS Trans. Data Sci.*, vol. 2, no. 2, pp. 1–13, 2021.

[49] A. Di Vaio, S. Hasan, R. Palladino, F. Profita, and I. Mejri, "Understanding knowledge hiding in business organizations: A bibliometric analysis of research trends, 1988–2020," *J. Bus. Res.*, vol. 134, pp. 560–573, 2021.

[50] R. Wazirali, R. Ahmad, and A. A.-K. Abu-Ein, "Sustaining accurate detection of phishing URLs using SDN and feature selection approaches," *Comput. Networks*, vol. 201, p. 108591, 2021.

[51] Y. Chen, H. Wang, H. Wu, Y. Zhou, L. Zhou, and Y. Chen, "Exploiting texture characteristics and spatial correlations for robustness metric of data hiding with noisy transmission," *IET Image Process.*, vol. 15, no. 13, pp. 3160–3171, 2021.

[52] S. Jin, F. Liu, C. Yang, Y. Ma, and Y. Liu, "Feature Selection of the Rich Model Based on the Correlation of Feature Components," *Secur. Commun. Networks*, vol. 2021, 2021.

[53] A. Ullah, K. Muhammad, T. Hussain, and S. W. Baik, "Conflux LSTMs Network: A Novel Approach for Multi-View Action Recognition," *Neurocomputing*, vol. 435, pp. 321–329, 2021.

[54] D. Shahi, R. S. V Vinod Kumar, and V. K. Reshma, "High Capacity Reversible Steganography on CMY and HSI Color Images Using Image Interpolation," *Webology*, vol. 18, pp. 133–148, 2021.

[55] N. Mukherjee (Ganguly), G. Paul, and S. K. Saha, "Two-point FFT-based high capacity image steganography using calendar based message encoding," *Inf. Sci. (Ny).*, vol. 552, pp. 278–290, 2021.

[56] L. Mo, L. Zhu, J. Ma, D. Wang, and H. Wang, "MDRSteg: Large-capacity image steganography based on multi-scale dilated ResNet and combined chi-square distance loss," *J. Electron. Imaging*, vol. 30, no. 1, 2021.

[57] M. L. Bensaad and M. B. Yagoubi, "High capacity diacritics-based method for information hiding in Arabic text," in *2011 International Conference on Innovations in Information Technology*, 2011, pp. 433–436.

[58] Y. Liu, G. Feng, C. Qin, H. Lu, and C.-C. Chang, "High-capacity reversible data hiding in encrypted images based on hierarchical quad-tree coding and multi-MSB prediction," *Electron.*, vol. 10, no. 6, pp. 1–23, 2021.

[59] D. Guo, R. Y. Zhong, P. Lin, Z. Lyu, Y. Rong, and G. Q. Huang, "Digital twin-enabled Graduation Intelligent Manufacturing System for fixed-position assembly islands," *Robot. Comput. Integr. Manuf.*, vol. 63, p. 101917, 2020.

[60] F. Meng, Z. Wang, S. Zhang, B. Ju, and B. Tang, "Bioinspired quasi-amorphous structural color materials toward architectural designs," *Cell Reports Phys. Sci.*, vol. 2, no. 7, p. 100499, 2021.

[61] Q. Giboulot, R. Cogranne, and P. Bas, "Detectability-Based JPEG Steganography Modeling the Processing Pipeline: The Noise-Content Trade-off," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 2202–2217, 2021.

[62] T. Sun *et al.*, "Local warning integrated with global feature based on dynamic spectra for FAIMS data analysis in detection of clinical wound infection," *Sensors Actuators B Chem.*, vol. 298, p. 126926, 2019.

[63] S. K. Moon, "Software and hardware-based audio-video crypto steganalysis model for enhancing robustness and imperceptibility of secured data," *Multimed. Tools Appl.*, vol. 81, no. 15, pp. 21047–21081, 2022.

[64] O. Evsutin and K. Dzhanashia, "Watermarking schemes for digital images: Robustness overview," *Signal Process. Image Commun.*, vol. 100, 2022.

[65] M. Huai, T. Zheng, C. Miao, L. Yao, and A. Zhang, "On the Robustness of Metric Learning: An Adversarial Perspective," *ACM Trans. Knowl. Discov. Data*, vol. 16, no. 5, 2022.

[66] R. Tabares-Soto *et al.*, "12 - Digital media steganalysis," M. B. T.-D. M. S. Hassaballah, Ed. Academic Press, 2020, pp. 259–293.

[67] S. Zheng, C. Yin, and B. Wu, "Keys as Secret Messages: Provably Secure and Efficiency-balanced Steganography on Blockchain," in *19th IEEE International Symposium on Parallel and Distributed Processing with Applications, 11th IEEE International Conference on Big Data and Cloud Computing, 14th IEEE International Conference on Social Computing and Networking and 11th IEEE Internation*, 2021, pp. 1269–1278.

[68] N. Mohamed, T. Rabie, I. Kamel, and K. Alnajjar, "Detecting secret messages in images using neural networks," 2021.

[69] J. PejaŚ, Ł. Cierocki, J. PejaS, and L. Cierocki, "Reversible data hiding scheme for images using gray code pixel value optimization," in *Procedia Computer Science*, 2021, vol. 192, pp. 328–337.

[70] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *Int. J. Surg.*, vol. 8, no. 5, pp. 336–341, 2010.

[71] H. N. Abed, A. L. Ahmed, N. H. Hassoon, I. S. Albayaty, A. Lec, and H. Noman, "Hiding Information In An Image Based On Bats Algorithm," *المجلة العراقية لتكنولوجيا المعلومات*, p. 128, 2018.

[72] A. I. Al-hussein, M. S. Alfaras, and T. A. Kadhim, "Text hiding in an image using least significant bit and ant colony optimization," *Mater. Today Proc.*, no. xxxx, 2021.

[73] H. M. Pandey, "Secure medical data transmission using a

fusion of bit mask oriented genetic algorithm, encryption and steganography," *Futur. Gener. Comput. Syst.*, vol. 111, pp. 213–225, 2020.

[74] S. Hossain, S. Mukhopadhyay, B. Ray, S. K. Ghosal, and R. Sarkar, "A secured image steganography method based on ballot transform and genetic algorithm," *Multimed. Tools Appl.*, 2022.

[75] V. Sabeti, M. Sobhani, and S. M. H. Hasheminejad, "An adaptive image steganography method based on integer wavelet transform using genetic algorithm," *Comput. Electr. Eng.*, vol. 99, p. 107809, 2022.

[76] P. D. Shah and R. S. Bichkar, "A secure spatial domain image steganography using genetic algorithm and linear congruential generator," *Adv. Intell. Syst. Comput.*, vol. 632, pp. 119–129, 2018.

[77] A. H. Mohsin *et al.*, "PSO–Blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralized hospitals intelligence architecture," *Multimed. Tools Appl.*, vol. 80, no. 9, pp. 14137–14161, 2021.

[78] V. Gautam, "MASSS—Multi-agent-Based Steganography Security System for VANET BT - Proceedings of 3rd International Conference on Computing Informatics and Networks," 2021, pp. 159–172.

[79] M. Kumar and T. Hussaini, "A Neural Network Based Image Steganography Method using Cyclic Chaos and Integer Wavelet Transform," in *2021 Asian Conference on Innovation in Technology (ASIANCON)*, 2021, pp. 1–6.

[80] K. Sharma, A. Aggarwal, T. Singhania, D. Gupta, and A. Khanna, "Hiding Data in Images Using Cryptography and Deep Neural Network," *J. Artif. Intell. Syst.*, vol. 1, no. 1, pp. 143–162, 2019.

[81] Z. L. Yang, X. Q. Guo, Z. M. Chen, Y. F. Huang, and Y. J. Zhang, "RNN-Stega: Linguistic Steganography Based on Recurrent Neural Networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 5, pp. 1280–1295, 2019.

[82] R. Meng, S. G. Rice, J. Wang, and X. Sun, "A fusion steganographic algorithm based on faster R-CNN," *Comput. Mater. Contin.*, vol. 55, no. 1, pp. 1–16, 2018.

[83] W. Tang, B. Li, S. Tan, M. Barni, and J. Huang, "CNN-Based Adversarial Embedding for Image Steganography," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 8, pp. 2074–2087, 2019.

[84] S. D. Desai, N. Patil, S. R. Nirmala, S. Kulkarni, P. D. Desai, and D. Shinde, "Deep Neural Network based Medical Image Steganography," in *2022 International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN)*, 2022, pp. 1–5.

[85] R. Meng, Q. Cui, Z. Zhou, Z. Fu, and X. Sun, "A Steganography Algorithm Based on CycleGAN for Covert Communication in the Internet of Things," *IEEE Access*, vol. 7, pp. 90574–90584, 2019.

[86] S. Kumar, A. Singh, and M. Kumar, "Information hiding with adaptive steganography based on novel fuzzy edge identification," *Def. Technol.*, vol. 15, no. 2, pp. 162–169, 2019.

[87] H. S. Yusuf and H. Hagras, "Towards Image Steganography Using Type-2 Fuzzy Logic and Edge Detection," *2018 10th Comput. Sci. Electron. Eng. Conf. CEEC 2018 - Proc.*, pp. 75–78, 2019.

[88] I. Shafi *et al.*, "An adaptive hybrid fuzzy-wavelet approach for image steganography using bit reduction and pixel adjustment," *Soft Comput.*, vol. 22, no. 5, pp. 1555–1567, 2018.

[89] S. Wu, S. Zhong, and Y. Liu, "Deep residual learning for image steganalysis," *Multimed. Tools Appl*, vol. 77, 2018.

[90] Y. Ge, T. Zhang, H. Liang, Q. Jiang, and D. Wang, "A novel technique for image steganalysis based on separable convolution and adversarial mechanism," *Electron.*, vol. 10, no. 22, pp. 1–15, 2021.

[91] L. Xiang, G. Guo, J. Yu, V. S. Sheng, and P. Yang, "A convolutional neural network-based linguistic steganalysis for synonym substitution steganography," *Math Biosci Eng*, vol. 17, no. 2, pp. 1041–1058, 2020.

[92] Z. Yang, N. Wei, J. Sheng, Y. Huang, and Y.-J. Zhang, "TS-CNN: Text Steganalysis from Semantic Space Based on Convolutional Neural Network," no. Bennett 2004, 2018, [Online]. Available: http://arxiv.org/abs/1810.08136.

[93] Z. Jin, Y. Yang, Y. Chen, and Y. Chen, "IAS-CNN: Image adaptive steganalysis via convolutional neural network combined with selection channel," *Int. J. Distrib. Sens. Networks*, vol. 16, no. 3, 2020.

[94] C. Li, Y. Jiang, and M. Cheslyar, "Embedding image through generated intermediate medium using deep convolutional generative adversarial network," *Comput. Mater. Contin.*, vol. 56, no. 2, pp. 313–324, 2018.

[95] X. Duan, K. Jia, B. Li, D. Guo, E. Zhang, and C. Qin, "Reversible image steganography scheme based on a U-net structure," *IEEE Access*, vol. 7, pp. 9314–9323, 2019.

[96] J. Mondal and M. Das, "A Novel Multilevel RDH Approach for Medical Image Authentication," *Advances in Intelligent Systems and Computing*, vol. 1311 AISC. pp. 513–520, 2021.

[97] A. A.-N. Patwary *et al.*, "Towards secure fog computing: A survey on trust management, privacy, authentication, threats and access control," *Electron.*, vol. 10, no. 10, 2021.

[98] M. H. Barkadehi, M. Nilashi, O. Ibrahim, A. Zakeri Fardi, and S. Samad, "Authentication systems: A literature review and classification," *Telemat. Informatics*, vol. 35, no. 5, pp. 1491–1511, 2018.

[99] C.-C. Chang, "Neural Reversible Steganography with Long Short-Term Memory," *Secur. Commun. Networks*, vol. 2021, 2021.

[100] X. Zhu, Y. Dang, and S. Ding, "Using a self-adaptive grey fractional weighted model to forecast Jiangsu's electricity consumption in China," *Energy*, vol. 190, p. 116417, 2020.

[101] P. Wu, Y. Yang, and X. Li, "StegNet: Mega Image steganography capacity with deep convolutional network," *Futur. Internet*, vol. 10, no. 6, pp. 1–15, 2018.

[102] X. Duan, N. Liu, M. Gou, W. Wang, and C. Qin, "SteganoCNN: Image steganography with generalization ability based on convolutional neural network," *entropy*, vol. 22, no. 10, pp. 1–15, 2020.

[103] O. Byrnes, W. La, H. Wang, C. Ma, M. Xue, and Q. Wu, "Data Hiding with Deep Learning: A Survey Unifying Digital Watermarking and Steganography," vol. 1, no. 1, pp. 1–35, 2021, [Online]. Available: http://arxiv.org/abs/2107.09287.

[104] M. K. Hasan *et al.*, "An improved watermarking algorithm for robustness and imperceptibility of data protection in the perception layer of internet of things," *Pattern Recognit. Lett.*, vol. 152, pp. 283–294, 2021.

[105] H. Fu, X. Zhao, and X. He, "Improving Anticompression Robustness of JPEG Adaptive Steganography Based on Robustness Measurement and DCT Block Selection," *Secur. Commun. Networks*, vol. 2021, 2021.

[106] A. Priyadharshini, R. Umamaheswari, N. Jayapandian, and S. Priyananci, "Securing medical images using encryption and LSB steganography," 2021.

[107] L. Aversano, M. L. Bernardi, M. Cimitile, and R. Pecori, "A systematic review on Deep Learning approaches for IoT security," *Comput. Sci. Rev.*, vol. 40, p. 100389, 2021.

[108] H. Ruiz, M. Chaumont, M. Yedroudj, A. O. Amara, F. Comby, and G. Subsol, "Analysis of the Scalability of a Deep-Learning Network for Steganography 'Into the Wild,'" *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12666 LNCS. pp. 439–452, 2021.

[109] I. Alodat and M. Alodat, “Detection of Image Malware Steganography Using Deep Transfer Learning Model,” *Lecture Notes in Networks and Systems*, vol. 287. pp. 323–333, 2022, DOI: 10.1007/978-981-16-5348-3_26.

[110] F. T. A. Hussien, A. M. S. Rahma, and H. B. A. Wahab, “A Secure E-commerce Environment Using Multi-agent System,” *Intell. Autom. Soft Comput.*, vol. 34, no. 1, pp. 499–514, 2022.

[111] S. Basu, M. Karuppiah, M. Nasipuri, A. K. Halder, and N. Radhakrishnan, “Bio-inspired cryptosystem with DNA cryptography and neural networks,” *J. Syst. Archit.*, vol. 94, pp. 24–31, 2019.

[112] X. Hao, W. Ren, R. Xiong, T. Zhu, and K.-K. R. Choo, “Asymmetric cryptographic functions based on generative adversarial neural networks for Internet of Things,” *Futur. Gener. Comput. Syst.*, vol. 124, pp. 243–253, 2021.

[113] W. Lin, X. Zhu, W. Ye, C.-C. Chang, Y. Liu, and C. Liu, “An Improved Image Steganography Framework Based on y Channel Information for Neural Style Transfer,” *Secur. Commun. Networks*, vol. 2022, 2022.

[114] C.-C. Chang, “Bayesian Neural Networks for Reversible Steganography,” *IEEE Access*, vol. 10, pp. 36327–36334, 2022.

[115] S. M. Thampi and K. C. Sekaran, “Content Based Image Retrieval with Mobile Agents and Steganography,” p. 6, 2004, [Online]. Available: http://arxiv.org/abs/cs/0411041.

[116] B. Rahul and K. Kuppusamy, “Efficiency Analysis of Cryptographic Algorithms for Image Data Security at Cloud Environment,” *IETE J. Res.*, 2021.

[117] H. Sun and Z. Qu, “High Efficiency Quantum Image Steganography Protocol Based on ZZW Framework,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Bioinformatics)*, vol. 12737 LNCS. pp. 400–411, 2021.

[118] M. Hussain, A. W. A. Wahab, Y. I. Bin Idris, A. T. S. Ho, and K.-H. Jung, “Image steganography in spatial domain: A survey,” *Signal Process. Image Commun.*, vol. 65, pp. 46–66, 2018.

[119] B. Yamini and R. Sabitha, “Image steganalysis: real-time adaptive colour image segmentation for hidden message retrieval and Matthew’s correlation coefficient calculation,” *Int. J. Inf. Comput. Secur.*, vol. 17, no. 1–2, pp. 83–103, 2022.

[120] R. Gurunath, A. H. Alahmadi, D. Samanta, M. Z. Khan, and A. Alahmadi, “A Novel Approach for Linguistic Steganography Evaluation Based on Artificial Neural Networks,” *IEEE Access*, vol. 9, pp. 120869–120879, 2021.