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:10.15199/48.2023.06.43

A Review of techniques for security information for agent approaches in networks

Abstract. *The development of communication technology has led to an increase in the risks associated with sending crucial information across a communication channel. One of the security details is defending against data theft over expanding networks by concealing sensitive information by employing agent techniques for hidden transmission. As a result, it is often used to solve data security issues. Researchers applied AI and agent-based algorithms to help secure information concealment since it may be challenging to choose the ideal cover image to conceal crucial information. The agent-based strategy and its applicability in various security information modalities are examined in this paper. This paper also discusses several important problems with creating other types of agents, such as basic reflex agents, reflex agents based on models, goal-based agents, utility-based agents, and learning agents. This paper concludes with an overview of the literature on agent-based methods for security information. The overall finding of our research is that agent-based techniques seem to be particularly fit for this area, although this still needs to be confirmed by more widely deployed systems.*

Streszczenie. *Rozwój technologii komunikacyjnych doprowadził do wzrostu zagrożeń związanych z przesyłaniem kluczowych informacji kanałem komunikacyjnym. Jednym ze szczegółów bezpieczeństwa jest ochrona przed kradzieżą danych w rozszerzających się sieciach poprzez ukrywanie poufnych informacji za pomocą technik agentów do ukrytej transmisji. W rezultacie jest często używany do rozwiązywania problemów związanych z bezpieczeństwem danych. Badacze zastosowali sztuczną inteligencję i algorytmy oparte na agentach, aby pomóc zabezpieczyć ukrywanie informacji, ponieważ wybór idealnego obrazu okładki w celu ukrycia kluczowych informacji może być trudny. W tym artykule przeanalizowano strategię opartą na agentach i jej zastosowanie w różnych trybach informacji o bezpieczeństwie. W tym artykule omówiono również kilka ważnych problemów związanych z tworzeniem innych typów agentów, takich jak podstawowe agenty refleksyjne, agenty refleksyjne oparte na modelach, agenty oparte na celach, agenty oparte na użyteczności i agenty uczące się. Artykuł ten kończy się przeglądem literatury dotyczącej agentowych metod uzyskiwania informacji o bezpieczeństwie. Ogólnym wnioskiem z naszych badań jest to, że techniki oparte na agentach wydają się szczególnie pasować do tego obszaru, chociaż musi to jeszcze zostać potwierdzone przez szerzej stosowane systemy*. (***Przegląd technik informacji o bezpieczeństwie dla podejść agentów w sieciach***)

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

Introduction

Because of the development of the Internet and communication technology, it has become important to consider data security as one of the important elements in our daily lives as is the privacy of the individual. Many applications need information security, and for these reasons, improving agent algorithms that rely on steganography is an urgent need [9], [17]. The proposed method depends on increasing the imperceptibility of the image and hiding the data in it by way of alternating bits of the LSB. As well as using two artificial intelligence algorithms to choose the appropriate image cover.

The problems related to the security and concealment of information have recently received great attention, especially in images, which are one of the most widely used media today. In applications that depend on images, it has attracted researchers to develop data security through it, and it has become a wide field for studies in this scope, which is the security and hiding of information in images [1], [2].

Hiding data is one of the ways to maintain its security, which is one of the basics of the term steganography. The method of choosing the cover of the image in order to hide the data inside it depends on artificial intelligence algorithms as it is in the software agent [3], There are many methods to embedding secret data and techniques that take many dimensions in terms of the type of method, which are mainly divided into Frequency Domain and Spatial Domain. One of the most important method is the LSB [4]. Using LSB bits in different ways in terms of location, and this method is used to increase imperceptibility during transmission, as is the case in the proposed method. In addition to linking the method with one of the artificial intelligence algorithms to choose the best image cover for the addition [5].

Addition to that, selecting an appropriate cover image to conceal a specific secret message is crucial for the security of the stego-image [6]. 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 steganography results [4], [5].

Agent Software

Agent software is a piece of software that functions as an agent for a user or another program, working autonomously and continuously in a particular environment [7]. The development of software systems basically begins with two activities, the first is the analysis of software requirements and the second is the approved design of these software. The analysis phase of the requirements includes understanding the problem and then reducing the possibility of errors resulting from those requirements, which may be ambiguous and incomplete. Requirements analysis is one of the main requirements of any software which is a contract between software designers and users [8]. It is done in the form of requirements and a logical analysis of all work and its development to suit the beneficiary, as work is like a contract between the programmer and the designer.

Despite the use of traditional methods in Artificial Intelligent (AI), in the analysis and design of complex programs, there is still a challenge in which of these programs is appropriate and which one should be relied upon [9]. This is what a specialized analysis of the problem does, depending on the characteristics of the system to be implemented. The software agent has the ability to deduce the appropriate solutions and choose any of the solutions that will be the best solutions in the future from among more than one way. traditional methods can be used efficiently in systems that do not need to analyze data at the beginning or predict the future for a particular solution [10]. Many

programs can use a software agent, but a logical analysis of the problem is required in advance and the best result we need is to have an idea of it. The increasing use of the Internet in all areas, which is the backbone of all associated devices, has made peripheral systems very complex and of unlimited size. The unlimited number of users in a particular system increases the complexity of the program and the independence of each user must be preserved and each user is dealt with reliably.

Software agents have some special characteristics, for example, autonomy, that is, exclusivity of special output, adaptation, and building a suitable environment for its work, which is one of the basics in artificial intelligence systems [11]. As with the concept of computing, it includes ubiquitous activities and users connected to the Internet, which provides a concept for modeling complex systems, and many articles about software agent presented in literature and solutions in complex programs [12], [13].

The Fate Agent Technique has received a lot of attention nowadays. Therefore, industries have developed this interest in using technology and become more efficient. Despite the advances in this field from many aspects such as agent developers, languages, and agent-based applications, only a few were intended to define the architecture that is concerned with the design and development of applications that use a software agent. One of the most important roles of the agent is software to help develop applications that depend primarily on it. The methodologies support this development as in [14].

In the field of our research, there are three main related areas of work, first working on the modeling used in previous research of the agent system, working and developing systems that are entirely based on the agent, and finally making use of the previous systems of the agent in building an integrated model based on the agent software.

There are several definitions by which a software agent can be known, and from these definitions it can be said that it is an integrated entity with characteristics, including [3], [15]:

- The work environment should be a homogeneous one.
- The ability of the system to interact with other systems or other agents.
- There is always a specific goal.
- The ability to determine the variables of the surrounding environment.
- It is part of the working environment.
- It contains skill in providing the services entrusted to it.

According to previous studies [16] there are important characteristics such as independence, reactivity, social ability, and proactivity. They represent programs that have the authority to make decisions in the performance of tasks. There are several definitions by which a software agent can be known, and from these definitions it can be said that it is an integrated entity with characteristics, including:

- The work environment should be a homogeneous one.
- The ability of the system to interact with other systems or other agents.
- There is always a specific goal.
- The ability to determine the variables of the surrounding environment.
- It is part of the working environment.
- It contains skill in providing the services entrusted to it.

According to previous studies, there are important characteristics such as independence, reactivity, social ability, and proactivity. They represent programs that have the authority to make decisions in the performance of tasks.

Agent as a term can be "agent-based computing", "multi-factor system" or "agent-based system". It is very widely used in information technology because it is used to describe a wide range of computations. These entities range from simple systems to complex expert systems, and from simple systems, for example (Microsoft's TIP WIZARD) that work to provide advice to beneficiaries or desktop agents who work on email administrations and others, either to expert and interoperable systems or large databases that need complex processing. Like (EXCEL 5) therefore there are three levels of software agent, namely the simple level and agents (ARCHON) which works directly without complexity according to specific rules and is of a high-level task and finally the last level which works to predict and anticipate the result in order to avoid future errors.as shown in Fig.1.

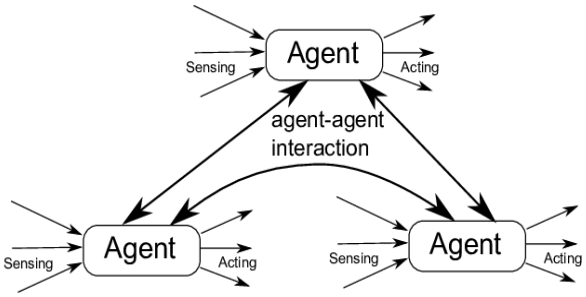

Fig.1: Agent system architecture [16]

As is the diversity in the definition of a software agent, it is clear and important to first define the common characteristics between the agent systems and the systems whose developers worked on the agency feature [17]. As defined in our research field as an artificial intelligence classifier. The agent is an entity in itself that solves problems in a connected way, as in our research, or separately. There are some characteristics to software agent should consider as:

- Autonomy: It is a characteristic that parents must be able to solve the majority of their own problems without outside interference. The agent must have a high degree of control over his activities and the internal state.
- Social ability: It is the agent's ability to interact when needed. Dealing with different industrial factors and humans to complete complex solutions to problems and activities. This requires the software agent to have the ability to receive and deliver variables inside and outside the system.
- Responsiveness: It is the agent's ability to perceive his environment, which could be the physical world, the user himself, the Internet, other agents, and so on. Immediate response to any change in the data or resulting from the duties of the agent.
- Reactiveness: It is simply that the agent does not have to respond to his environment, but in the simplest form it must be able to show opportunistic behavior towards the target in demand and act accordingly.

Type of Agents

Agents are classified into five classes according to the degree of intelligence and perceived abilities[18], [19]. The agent's performance can be improved and its effectiveness increased over time, as follows:

- Simple Reflex Agent
- Model-based reflex agent
- Goal-based agents
- Utility-based agent
- Learning agent

A. Simple Reflex

Simple reflexes are usually simple and of a simple practical nature. The software agent makes decisions based on existing perceptions, i.e. current, while ignoring the history of perception. This type only succeeds in the environment fully monitored by the user, and this type of software agent does not care about the cognitive history at work and has nothing to do with decision-making [18]. His work is based on a conditional basis for work, as he works in a situation, and he is assigned an order from the beneficiary, and one of his problems is that the process of intelligence in it is limited and does not work only according to the current data and does not care about the outputs and does not adapt to the work environment. As shown in Fig.2.

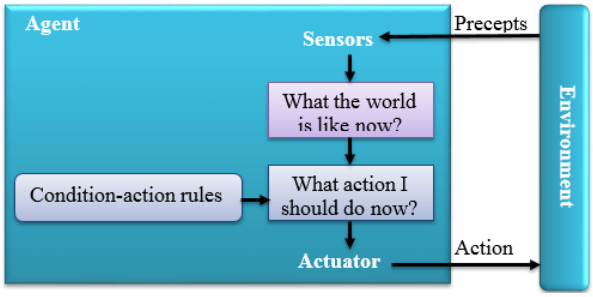

Fig.2: Simple Reflex Agent illustration [18]

B. Model-based reflex agent

The agent here relies on a particular business model that can be partially monitored and the business situation tracked as well. It has two main factors: the model, which means knowing how things happen and the program works according to the algorithm given, so it is called the model-based agent, and the second factor is the internal state, and it is a representation of the current state of the program state, which depends on the history of perception. This species possesses knowledge about the whole system so that when building such a model it must be fed with the evolutionary machinery and how it is affected by the remaining agents [20]. As shown in Fig.3.

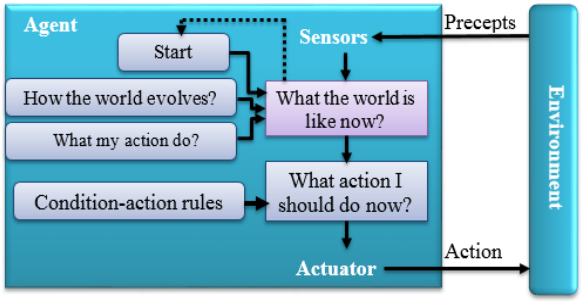

Fig.3: Model-based reflex agent [20]

C. Goal-based agents

The amount of knowledge of the current business environment is not always sufficient to make the appropriate decision by the agent and what to do. It is important for the agent to know in advance the purpose for which it was established. Through this goal, the agent's capabilities and capabilities in correct estimation of different environments are expanded [20]. To be able to get the target, preliminary decisions must be made about the agent's guessing algorithm. In order to achieve the desired goal of the agent, it performs a set of procedures in a sequential manner in terms of priorities, and then decides whether achieving the goal is possible or not. Research and anticipation scenarios make the agent proactive in making decisions. As shown in Fig.4.

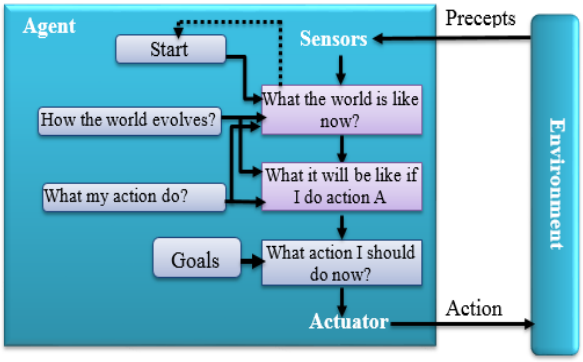

Fig.4: Goal-based agents [20]

D. Utility-based agent

In this type, he takes care of the main goal through which he sets the work strategy to reach the goal. The measure of success depends on the extent to which the goals are achieved and works on the benefit derived from the data and considers it the best way to achieve the goal [19]. This utility-based type is only effective when alternatives are available, so the process of selecting an agent for a particular system is rather difficult. The function of the tool helps to achieve the actual resulting change into the form of real numbers in order to know the efficiency of the agent in question. As shown in Fig.5.

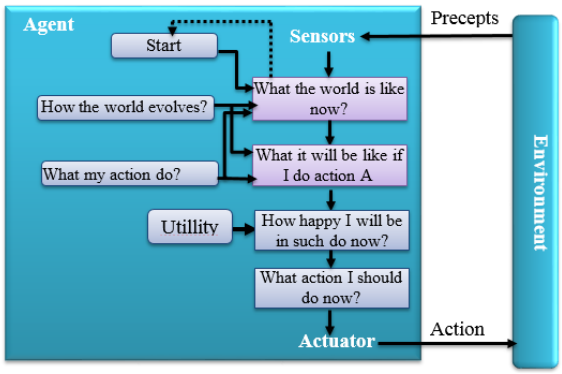

Fig.5: Utility-based agent [19]

E. Learning agent

Learning the agent using artificial intelligence, which is the agent who learns from its previous experiences, where it is built on the basis of retrieving the initial results as inputs in order to determine the correct paths in the work. Building knowledge through the mechanism of trial and error is one of the most important methods of artificial intelligence, which allows the possibility of managing the machine by itself without human intervention in order to achieve results. There are four concepts that make up the education-based agent [21]:

- The learning element: Its responsibility is to make improvements in this area.
- Critic: It is the one who determines the ingenuity of the system and is responsible for the performance according to certain criteria used for measurement.
- The performance element: It is responsible for the external procedure and the selection of the appropriate action.
- Problem generator: It defines new procedures in the work in proportion to the volume of work, which is determined by the amount of information useful in tracking the chain of operations.

From here we know that software agents are able to learn, analyze and check performance, in addition to the possibility of storing past experiences in the work stages.as shown in Fig.6.

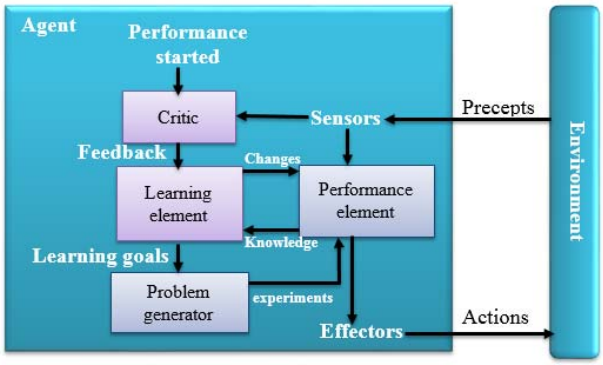

Fig.6: Learning agent strategy [21]

Agent in AI

Artificial intelligence is defined as the ability to study the rational factor in the machine and its relation to its environment. The software agent can sense the surrounding environment through sensors attached to it, which transmit information into the system. The intelligent system can have multiple characteristics, such as rationality, knowledge, belief, and intention for a specific action, and so on [22].

A software agent is designed on the basis of perceiving the work environment through the hardware and software that connects to it and acting rationally through the work engines. The software agent acts as the act of perceiving, thinking, and acting upon it. In general, the agent is as follows:

- *Human Agent:* It is the human being and the senses associated with him about his environment. And it has the ability to act by its physical components, as it is considered a machine for entering and exiting the processed data.
- *Automated Agent:* It is a mechanism that contains entrances and exits such as cameras, sensors, and radiological devices, and it is processed on the basis of the information entered and gives an instant reaction to that.
- *Software Agent:* It is programs and algorithms that are written in the form of input steps from the keyboard and the outputs are on the screen.

The environment around us is full of influences and agents of all kinds, such as people, machines, and intelligent algorithms.

There are three main factors effects the agent in term of software as:

- *Sensors:* It is a device that detects changes in the environment, whether physical or digital, and sends information to other devices or other stages of the program. The agent monitors the environment through it.
- *Actuators:* They are those that convert energy from one form to another, or transfer programs from one work to another according to the reaction. It shall be responsible for controlling the work of the agent. It can be automatic or logical to change the direction of work.
- *Effectors:* Are they responsible for the reaction with the impact on the environment? It can be changing an action, stopping it, its speed, or the accuracy of the result. As shown in Fig.7.

Related Work

The creation of programs that can attach information to binary image files is discussed by Lu et al. (2018) [23]. In order to create stego images, a variety of techniques, including local structural characteristics, global statistical features, and flipping position optimization, are applied. This is done in order to lessen the amount of distortion that happens in stego photos, which is notably visible when they are embedded in binary images. The effect may be seen most clearly when they are placed in binary images. When doing this test, there is a considerable decrease in the amount of distortion that occurs.

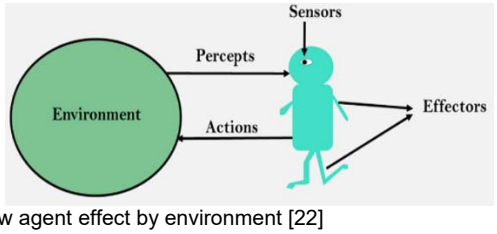

Fig.7: How agent effect by environment [22]

It is conceivable to apply watermarks to a spatial domain by authors Ghadi et al. (2018) [24], this technique lays an emphasis on examining word textures and establishing relationships between distinct words. The writers propose hiding up the watermark by putting it in portions of the cover image that have a lot of texture. Because of this, embedding will become more stable and will be much simpler to disguise. Following the selection of four image characteristics by a grayscale histogram, the apriori technique is utilized to build the rules that connect the distinct image features.

In the prior study by Evsutin and Kokurina. (2018) [25], information in the DFT phase spectrum is steganographically buried using different ways. In order to ensure that the information will be recovered without any errors, the authors propose that the embedding procedure be carried out in steps. In order to achieve this, data is gathered during the embedding phase and then analyzed for mistakes that need to be repaired by re-embedding the phase value block that has already been modified. This is done so that the intended effect may be reached.

A hybrid strategy for embedding watermarks is detailed in the research work that has the Authors Cherifi and El. (2018) [26] and is available online. In the discrete cosine transform (DCT), the watermark may be observed in the center band, which corresponds to the DFT magnitude. The authors claim that combining DFT and DCT enhances invisibility and resilience as a consequence of the combination of DFT and DCT. The watermark is first encrypted using the Arnold transform, and then, in order to increase the watermark's degree of security, its bits are swapped with portions of a "pseudo-random sequence."

Additionally, quantum image processing is studied in the work (El-latif et al. (2018) [27]. This article discusses many ways for embedding information for the purposes of digital steganography and digital watermarking. Next the expansion of the concealed image created by the steganographic approach, the next step is to encrypt it. In the process of watermark embedding, the Arnold's cat map is used to conceal the meaning of the expanded watermark image, making it more difficult to understand. Information is concealed in a cover image by employing XORing, the least significant qubits, and the most significant qubits.

The Authors Hou et al. (2018) [28] shows how to conceal data in compressed JPEG images by utilizing reversible steganography. This approach is distinct from the typical way of computing DCT coefficients, which eventually results in the inserted cover image having less distortion. Along with the actual message itself, the length of the message as well as the coefficients that were used to

embed the message are buried inside the image so that reversibility may be preserved.

According to the authors of Puteaux et al. (2018) [29], the optimum approach of embedding information is one that is based on the most important bit (MSB) (MSB). There are two distinct plans that may be executed within the boundaries of this technique. The first technique is a high-capacity data-hiding solution that is reversible and incorporates prediction error correction. It is also capable of storing a substantial quantity of data and recovering images to a condition that is pretty comparable to the originals. On the other side, you will not have access to the complete original information. The second approach, high-capacity reversible data hiding with built-in prediction errors, is similarly entirely reversible; however, its capacity is substantially restricted due to the employment of a location map. This technique also has the additional advantage of incorporating prediction faults.

Refer to the authors Qin et al. (2018) [30] source for further information on the spatial embedding procedure that is utilized in encrypted images. If you wish to employ this method, you will also need to be acquainted with the embed key and the encryption key in order to get all of the data and the initial image in its original form. It is necessary to delete the fixed additional information blocks that appear before the primary payload in order to acquire access to the data and retrieve the cover image.

The application of resilient watermarking in a spatial domain is illustrated further by authors Su et al. (2019) [31], which presents an example of this. The capacity of the proposed system to calculate the current (DC) coefficient of the embedded discrete Fourier transform is a property that sets it apart from previous systems (DFTdirect) (DFTdirect). One other aspect that sets the proposed technique different from others is that it calculates the DC-coefficient in the spatial domain without employing true 2D-DFT.

This approach, which has witnessed increased levels of application throughout the previous few years, is illustrated by the author Zhou, Luo and Liu. (2019) [32], describes a technique that employs LSB as its base for digitally watermarking color quantum images. The process of embedding may be made more secure by making use of the gray code transform.

With the use of the authors Biswas and Kumar. (2019) [33], it is possible to conceal information in color photographs. Data is stored in the DCT coefficients by employing the LSB technique of data storage. In this specific scenario, the RGB plane of the image is pre-processed so that random pixels may be implanted at a later time. The approach is robust to major attacks and performs well when compared to benchmark tools for decoding steganography. This is owing to the fact that pixels are taken at random in the procedure. When a GA is utilized, embedding has the potential to become more secure and more difficult to detect.

The authors of the publication Chuang et al. (2019) [34] describe a reversible technique for hiding data in the color indices of a digital image, using this artwork as an example. It's feasible that this method may serve as an example. Each index fits into one of these three classes according to the method in which it interacts with its surrounding environment. There are two main kinds of indices that may be used to keep sensitive information, and which one is utilized will depend on how much space is required to contain the information.

Another example of reversible JPEG image embedding can be found by authors Di et al. (2019) [35], which can be viewed here. In this specific circumstance, the authors claim that employing zero DCT coefficients all throughout the embedding process will result in better embedding capacity. There are some who suggest that the only embedding zero coefficients that should be selected are the optimal ones. This would prevent the JPEG file size from rising while keeping the amazing quality of the photo.

An additional strategy for integrating image encryption with steganography is explored by the authors Liu and Pun. (2019) [36], which may be accessed here. When an image is encrypted, it leads in the development of two additional data blocks. This block has been condensed for your convenience. A single sequence is formed by merging the message with any additional data that was recovered from the encrypted image. Only the encryption key is needed to complete either the embedding or the encryption process.

Within the framework of the authors effort Ren, Lu and Chen. (2019) [37], binary image blocks are separated into similar and distinct sections. This is done in order to permit the insertion of extra information to photos that have been encrypted. After that, a type image is formed, in which black pixels indicate areas that are unique from one another and white pixels represent spots that are identical. The image will first have a type image applied to it before it is encrypted. This makes it a great lot simpler to discover the image in its original form.

Only binary photographs are deemed to be digital watermarks that need to be applied to other images by the authors of Yao et al. (2019) [38]. The hiding areas for data are selected so that they are less noticeable by applying a model that accounts for how the human eye interprets information. With the use of encryption and embedded keys, the digital watermark may be totally removed, enabling the original image to be reconstructed.

The authors of Xiong and Xu. (2019) [39] provide instructions on how to apply minuscule watermarks that enable users to detect and correct modifications made to photos. Even after the image has been modified, these watermarks will still be visible in the image. The process of establishing a digital watermark results in the generation of bit sequences, and these bit sequences have the potential to be employed for restoration purposes in the future. K-means clustering is a technique that may be used to rapidly reconstruct photographs that have been damaged or altered.

Ma and Wang. (2019) [40], used the necessary bit planes of high-frequency coefficients employed in the building of maps. In addition, sensitive data and position maps are adjusted in such a manner that only the most significant high-frequency wavelet coefficients are employed. This may be done without any information being lost in the process. Even if both the embed key and the encryption key are known, it will not be able to retrieve the original image in its entirety from the storage media in question. This is because the embed key is used in conjunction with the encryption key. If you have the encryption key, you will be able to see the photo; but, since the image contains embedded data, the image that you see will not be an exact copy of the one that was originally shown. IWT is used rather than other methods of frequency modulation because it retains information, which distinguishes it from those other methods and makes it preferable to use. IWT of encrypted photographs is another use for the technology stated by Xiong and Xu. (2019) [39], which is possible.

The authors of Liu et al. (2019) [41] express a similar concern over the confidentiality of the medical information of patients. Two distinct kinds of data make up the watermark: authenticity data, which is generated by hashing a logo, and integrity data, which contains information on detecting tampering, identifying the watermark, and

recovering it if it has been altered. The authenticity data is generated by hashing the logo, and the integrity data contains information on identifying the watermark. Hashing the logo results in the generation of the authenticity data, and the integrity data includes instructions on how to restore the watermark in the event that it has been corrupted in any way. The solution that has been presented stands out from others because it differentiates between regions of interest and areas that do not have any interest in the region where the watermark is generated, which results in an effective recovery function. This is what makes the solution stand out. Numerous methods, including as the Slantlet transform, recursive dither modulation, and SVD, are used in the process of adding a watermark to a medical image. These methods are among the many that are utilized.

It was shown by Verma, Muttoo and Singh.(2020) [42] how to hide digital graphics or text by blending them in with the RGB pixels of a photograph. The phrase "embedding" refers to this kind of activity. In order for sensitive information to be embedded, it must first be converted into a sequence of numbers, each of which must only include two digits. One digit is encoded in one pixel by shifting the value of the pixel in the cover image to the next closest value depending on the least significant bit of the pixel and the message digit. This encoding method results in one digit being stored in one pixel. The encoding of one digit is achieved as a consequence of this operation. If you use this tactic, you may be able to conceal one of the numbers.

Over the course of the past few years, there has been an upswing of interest surrounding the application of neural networks for the goal of concealing data in digital images. Neural networks, for instance, are utilized in the process of embedding and removing digital watermarks by Emami. (2020) [43]. In addition, embedding may be done in the domain of a great many distinct frequency transformations. Because of this, the recommended system has the needed degree of flexibility.

Sahu and Swain, (2020) [44] shows how they conceal data using steganography in the pixels that are regarded to be of the least relevance. The embedding process may be split down into two independent components. In the first step of the process, two bits of information are written into each pixel of the image. After that, a pair of intermediate pixels are generated by joining two of the altered pixels into a single pixel. In the second step, you may achieve a high capacity for embedding by employing a pair of intermediate pixels to make two unique pairs of identical pixels and to conceal four extra hidden bits. This will help you to acquire a high capacity for embedding. In order to achieve this, the concealed components are veiled as counterparts that look to be identical.

The outcomes of study by Li et al. (2020) [45] suggest that reversible steganographic embedding has the potential to be made more secure and difficult to detect. As a direct outcome of their study, the authors have proposed a technique for the reversible concealment of data that is based on the difference value and retains statistical features. There are three similar stego photos that are constructed in order to obscure the message that is contained in the primary image by Xie. (2020) [46]. This is one of the distinctive aspects of the approach that sets it different from others. The embedding procedure takes use of the order of pixel values as well as the shifting of the prediction error histogram. Both of these things are important for the procedure.

The technique of steganography generally makes use of approaches and strategies for reversible embedding. On the other hand, there are occasions when we speak about digital watermarks that have the capacity to be added or removed. For instance, the authors Das et al. (2020) [47], illustrates how to develop an updated reversible contrast mapping technique for the aim of reversible invisible watermarking. The image includes a very faint watermark that is embedded into its spatial domain.

Huang and Wang. (2020) [48] explains how to inject data into the vacant area around encrypted photos. When data is stored in particular pixels, the bits that are most important to the information are all set to zero. It is needed to establish which pixels in the image were changed in order to restore the image to its original condition. A location map is first compressed with the help of a mathematical process; after which it is joined to the encrypted message that is contained in the cover image.

The approach described by Chang. (2020) [49] is similar. It achieves this by utilizing a median-edge detector that can forecast where the image's pixels will be positioned. When the prediction error is smaller than a predefined threshold, the pixels in question are embedded. In addition to this, it is vital to have a comprehension of the label map, which is produced before the message is implanted. It is included in the image along with the message, and Huffman coding is employed in order to decrease the size of the image.

The embedding system that is provided by Chen. (2020) [50] is supported by homomorphism as well as matrix embedding. The Golay algorithm is utilized in the implementation of the matrix embedding decision. The majority of encrypted digital photos contain the geographical coordinates of the photograph's site of origin. On the other hand, a second line of inquiry recommends adding data to the frequency domain of an encrypted image.

The approach of applying a technique of weak watermarking is proposed in the study by Molina-Garcia et al. (2020) [51] as a means to identify and reverse modifications that have been made to color images. This method may be used to detect and undo the changes that have been done. By utilizing the data from the cover image, a digital watermark can be created. After that, the digital watermark is disassembled into its component watermarks so that each of those watermarks may be independently retrieved and authenticated. In order to generate the recovery watermark, a half-toning technique and a block-based approach are used as the two primary approaches. After that, the XOR technique is utilized so that an authenticating watermark may be created. After that, the watermarks are appended to the LSB pixels in order to make it possible for those pixels to be used in the process of validating the image and determining whether or not any modifications have been done.

The work presents a technique for the protection of data that takes use of watermarking in both its visible and its undetectable forms by Cedillo-hernandez et al. (2020) [52]. The information gathered about the patient is used as a factor in the generation of a covert watermark, which is then appended to a medical image. The coding for the zero-watermark is kept safe at all times since it is kept in a separate location from both the image and the invisible watermark. In order to extract the feature pattern, the presently active image is used. This pattern is then put through an XOR operation so that the authentication process may be brought to a successful finish.

Conclusion

This paper aims to conduct a thorough evaluation of the literature on agent-based steganography systems. Many academics and professionals in the sector would benefit from this, particularly in realizing how costly and time-

consuming choosing the ideal cover picture is. This paper provided comprehensive details on choosing cover pictures in relation to agent strategies and AI contributions. Assessing various articles that detail the benefits, challenges, and suggestions related to agent-based steganography and identifying distinct gaps. 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 the methodology.

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

REFERENCES

[1] I. O. P. C. Series and M. Science, “Steganalysis of Intra Prediction Mode and Motion Vector-based Steganography by Noise Residual Convolutional Neural Network Steganalysis of Intra Prediction Mode and Motion Vector- based Steganography by Noise Residual Convolutional Neural Network,” 2020.

[2] A. Kuznetsov, A. Onikiychuk, and A. Arischenko, “Adaptive Pseudo-Random Sequence Generation for Spread Spectrum Image Steganography,” pp. 161–165, 2020.

[3] D. G. Cory, “Development of a Method for Building a Trusted Environment by Using Hidden Software Agent Steganography Development of a Method for Building a Trusted Environment by Using Hidden Software Agent Steganography,” pp. 0–6.

[4] R. D. Rashid, “Edge Based Image Steganography : Problems and Solution,” *2019 Int. Conf. Commun. Signal Process. their Appl.*, pp. 1–5, 2019.

[5] S. Rustad, D. R. Ignatius, M. Setiadi, A. Syukur, and P. N. Andono, “Inverted LSB image steganography using adaptive pattern to improve imperceptibility,” *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, 2021.

[6] Y. P. Astuti, D. R. Ignatius, M. Setiadi, E. H. Rachmawanto, and C. A. Sari, “Simple and Secure Image Steganography using LSB and Triple XOR Operation on MSB,” *Int. Conf. Inf. Commun. Technol.*, pp. 191–195, 2018.

[7] E. Antonov, E. Lopatina, K. Ionkina, E. Lopatina, and K. Ionkina, “ScienceDirect ScienceDirect Agent data merging Agent data merging,” *Procedia Comput. Sci.*, vol. 169, no. 2019, pp. 473–478, 2020.

[8] H. Abdul, J. Park, and J. Suh, “Use of Software Agent Technology in Management Information System : A Literature Review and Classification,” vol. 29, no. 1, pp. 65–82, 2019.

[9] R. Hafezi, “How Artificial Intelligence Can Improve Understanding in Challenging Chaotic Environments,” no. July, 2019.

[10] J. Qiao and M. Sun, “Consensus Control via Iterative Learning for Singular Multi-Agent Systems With Switching Topologies,” vol. 9, no. Ilc, 2021.

[11] H. O. W. Can, O. N. E. Evaluat, E. A. C. Ional, S. Ware, and A. Framework, “CHAPTER 15 - FUNCTIONAL LINGUISTIC BASED MOTIVATIONS FOR A CONVERSATIONAL.”,2019.

[12] S. Kaur, S. Bansal, and R. K. Bansal, “Image steganography for securing secret data using hybrid hiding model,” 2020.

[13] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, “AC US CR,” *Neurocomputing*, 2018.

[14] C. Savaglio, M. Ganzha, M. Paprzycki, C. Bădică, M. Ivanović, and G. Fortino, “Agent-based Internet of Things : State-of-the-art and research challenges,” *Futur. Gener. Comput. Syst.*, vol. 102, pp. 1038–1053, 2020.

[15] Carleo, G., Cirac, I., Cranmer, K., Daudet, L., Schuld, M., Tishby, N., Vogt-Maranto, L. and Zdeborová, L., Machine learning and the physical sciences. *Reviews of Modern Physics*, 91(4), p.045002,2019.

[16] K. Rakić, M. Rosić, and I. Boljat, “A Survey of Agent-Based Modelling and Simulation Tools for Educational Purpose,” vol. 3651, pp. 1014–1020, 2020.

[17] N. H. Jaafar, A. Ahmad, N. Hamimah, and A. Hamid, “A Workload Manager : The Pre-assessment in Sincere Software Agent Environment,” *2018 Int. Symp. Agent, Multi-Agent Syst. Robot.*, pp. 1–5, 2018.

[18] O. Boissier *et al.*, “Autonomous Agents on the Web To cite this version : HAL Id : emse-03313806 Autonomous Agents on the Web,” vol. 11. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany, pp. 20–24, 2021.

[19] Obuhuma, J.I., Okoyo, H.O. and McOyowo, S.O., September. A Software Agent for Vehicle Driver Modeling. *In 2019 IEEE AFRICON* (pp. 1-8). IEEE,2019.

[20] E. Guerrero, M. Lu, H. Yueh, and H. Lindgren, “Autonomous adaptation of software agents in the support of human activities,” pp. 1–13.

[21] D. Lee, “Comparison of Reinforcement Learning Activation Functions to Improve the Performance of the Racing Game Learning Agent,” vol. 16, no. 5, pp. 1074–1082, 2020.

[22] S. Kraus *et al.*, “AI for Explaining Decisions in Multi-Agent Environments,” 2020.

[23] W. Lu, L. He, Y. Yeung, Y. Xue, H. Liu, and B. Feng, “Secure Binary Image Steganography based on Fused Distortion Measurement,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. PP, no. c, p. 1, 2018.

[24] M. Ghadi, L. Laouamer, L. Nana, and A. Pascu, *Robust Image Watermarking Based on Multiple-Criteria Decision-Making A blind spatial domain-based image watermarking using texture analysis and association rules mining*, no. December. Multimedia Tools and Applications, 2018.

[25] O. Evsutin and A. Kokurina, *The adaptive algorithm of information unmistakable embedding into digital images based on the discrete Fourier transformation*. Multimedia Tools and Applications, 2018.

[26] H. Cherifi and M. El, “Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform,” 2018.

[27] A. A. A. B. D. El-latif, B. Abd-el-atty, M. S. Hossain, and S. Member, “Efficient Quantum Information Hiding for Remote Medical Image Sharing,” *IEEE Access*, vol. 6, pp. 21075–21083, 2018.

[28] 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.

[29] P. Puteaux, S. Member, W. Puech, and S. Member, “An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images,” vol. 6013, no. c, pp. 1–13, 2018.

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

[31] Q. Su *et al.*, “New Rapid and Robust Color Image Watermarking Technique in Spatial Domain,” *IEEE Access*, vol. 7, pp. 30398–30409, 2019.

[32] W. H. R. Zhou, J. Luo, and B. Liu, “LSBs-based quantum color images watermarking algorithm in edge region,” *Quantum Inf. Process.*, vol. 123, 2019.

[33] Biswas, R. and Bandyapadhay, S.K., Random selection based GA optimization in 2D-DCT domain color image steganography. *Multimedia Tools and Applications*, 79(11), pp.7101-7120,2020.

[34] J. Chuang, Y. Hu, C. Chen, Y. Lin, and Y. Chen, “Joint index coding and reversible data hiding methods for color image quantization,” *Multimed. Tools Appl.*, 2019.

[35] Di, F., Zhang, M., Huang, F., Liu, J. and Kong, Y., 2019. Reversible data hiding in JPEG images based on zero coefficients and distortion cost function. *Multimedia Tools and Applications*, *78*(24), pp.34541-34561.

[36] Liu, Z.L. and Pun, C.M., 2019. Reversible image reconstruction for reversible data hiding in encrypted images. *Signal Processing*, *161*, pp.50-62.2019.

[37] Ren, H., Lu, W. and Chen, B., Reversible data hiding in encrypted binary images by pixel prediction. *Signal Processing*, *165*, pp.268-277.

[38] Yao, Y., Zhang, W., Wang, H., Zhou, H. and Yu, N., 2019. Content-adaptive reversible visible watermarking in encrypted

images. *Signal Processing*, *164*, pp.386-401.
[39] L. Xiong and Z. Xu, “An integer wavelet transform based scheme for reversible data hiding in encrypted images,” *Multidimens. Syst. Signal Process.*, 2019.
[40] G. Ma and J. Wang, “Signal Processing : Image Communication Efficient reversible data hiding in encrypted images based on multi-stage integer wavelet transform ☆,” *Signal Process. Image Commun.*, vol. 75, no. March, pp. 55–63, 2019.
[41] X. Liu *et al.*, “Scheme for Protecting Authenticity and Integrity of Medical Images,” *IEEE Access*, vol. 7, pp. 76580–76598, 2019.
[42] V. Verma, S. K. Muttoo, and V. B. Singh, “Enhanced payload and trade-off for image steganography via a novel pixel digits alteration,” 2020.
[43] A. Emami, *ReDMark: Framework for Residual Diffusion Watermarking based on Deep Networks*. Elsevier Ltd, 2020.
[44] A. K. Sahu and G. Swain, “Reversible Image Steganography Using Dual - Layer LSB,” *Sens. Imaging*, 2020.
[45] T. Li, H. Li, L. Hu, and H. Li, “A Reversible Steganography Method With Statistical Features Maintained Based on the Difference Value,” pp. 12845–12855, 2020.
[46] X. Xie, “A hybrid reversible data hiding for multiple images with high embedding capacity,” *IEEE Access*, vol. PP, p. 1, 2020.
[47] S. Das, A. K. Sunaniya, R. Maity, and N. P. Maity, “Parallel Hardware Implementation of Efficient Embedding Bit Rate Control Based Contrast Mapping Algorithm for Reversible Invisible Watermarking,” *IEEE Access*, vol. 8, pp. 69072–69095, 2020.
[48] D. Huang and J. Wang, “Signal Processing : Image Communication High-capacity reversible data hiding in encrypted image based on specific encryption process ☆,” *Signal Process. Image Commun.*, vol. 80, no. July 2019, p. 115632, 2020.
[49] C. Chang, “Separable Reversible Data Hiding in Encrypted Images With High Capacity Based on Median-Edge Detector Prediction,” pp. 29639–29647, 2020.
[50] S. Chen, “Fidelity Preserved Data Hiding in Encrypted Images Based on Homomorphism and Matrix Embedding,” vol. 8, pp. 22345–22356, 2020.
[51] J. Molina-Garcia, B. P. Garcia-Salgado, V. Ponomaryov, R. Reyes-Reyes, S. Sadovnychiy, and Clara Cruz-Ramos, “Signal Processing : Image Communication An effective fragile watermarking scheme for color image tampering detection and self-recovery ☆,” *Signal Process. Image Commun.*, vol. 81, no. July 2019, p. 115725, 2020.
[52] M. Cedillo-hernandez, A. Cedillo-hernandez, M. Nakano-miyatake, and H. Perez-meana, “Biomedical Signal Processing and Control Improving the management of medical imaging by using robust and secure dual watermarking,” *Biomed. Signal Process. Control*, vol. 56, p. 101695, 2020.