Research Article

Fatmah Abdulrahman Baothman* and Budoor Salem Edhah

Toward agent-based LSB image steganography system

https://doi.org/10.1515/jisys-2021-0044
received March 23, 2021; accepted May 14, 2021

Abstract: In a digital communication environment, information security is mandatory. Three essential parameters used in the design process of a steganography algorithm are Payload, security, and fidelity. However, several methods are implemented in information hiding, such as Least Significant Bit (LBS), Discrete Wavelet Transform, Masking, and Discrete Cosine Transform. The paper aims to investigate novel steganography techniques based on agent technology. It proposes a Framework of Steganography based on agent for secret communication using LSB. The most common image steganography databases are explored for training and testing. The methodology in this work is based on the statistical properties of the developed agent software using Matlab. The experiment design is based on six statistical feature measures, including Histogram, Mean, Standard deviation, Entropy, Variance and Energy. For steganography, an Ensemble classifier is used to test two scenarios: embedding a single language message and inserting bilingual messages. ROC Curve represents the evaluation metrics. The result shows that the designed agent-based system with 50% training/testing sample set and 0.2 Payload can pick out the best cover image for the provided hidden message size to avoid visual artifact.

Keywords: steganography, digital security, software agents LSB steganography, ensemble classifier, steganography datasets

1 Introduction

Information security is an essential factor required for exchanging messages or information communication via the internet. Securing communication confidentiality is done using many techniques; cryptography is among the top ones used for multimedia. Sometimes keeping the secrecy of messages' content is not enough, and it may be safer to conceal the existence of the message, which is known as steganography. It is known as the tactic of concealing a confidential message in digital files, e.g., photos, audio, or video files [1]. Steganography's core objective is to hide embedded information – a "Payload" – in a cover object in which the Payload's existent object is invisible. Steganography is gaining internet communication attention [2,3] because of a general weakness in cryptography. Although cryptography can protect an encoded message, its visible presence exposes the message to decryption attacks which a message invisible to an eavesdropper avoids. Of course, both can be applied, and steganography becomes more secure if its Payload message is also encrypted with a key known only to the intended recipient [4,5]. Steganography is becoming a highly attractive area of research with many applications. Selecting a proper cover image to hide a specific secret message is highly important for the stego image's security. This paper aims to present

* **Corresponding author: Fatmah Abdulrahman Baothman,** Department of Information Systems, Faculty of Computing & Information Technology, King Abdulaziz University, Jeddah, 21431, Kingdom of Saudi Arabia, e-mail: fbaothman@kau.edu.sa
Budoor Salem Edhah: Department of Information Systems, Faculty of Computing & Information Technology, King Abdulaziz University, Jeddah, 21431, Kingdom of Saudi Arabia, e-mail: beidhah@stu.kau.edu.sa

an information protection approach through images using the Least Significant Bit (LSB) steganography and agents technique.

Information hiding is a subfield of security; it involves numerous methods for hiding information digitally. Moreover, various purposes can be employed, such as securing messages or creating covert channels. Figure 1 illustrates the Information hiding classification adapted from Bauer [6]. A significant zone of information hiding is known as steganography, and it is the discipline of concealing messages into objects. Aside from steganography, copyright marking requires additional robustness against possible attacks. Marking is divided into robust and fragile ones. Robust watermarks cannot be removed without destroying the object. Fragile watermarking is meant to be changeable. Fingerprinting uses embedded serial numbers in objects that enable the protection of the copyrights and detect when a license agreement has been broken and the product copied illegally. Watermarks can be visible or hidden [7]. In this work, we are interested in steganography. Technical steganography is described in the literature review II below. More modern linguistic steganography is a set of techniques for embedding a message in a carrier and can use the following techniques [8]:

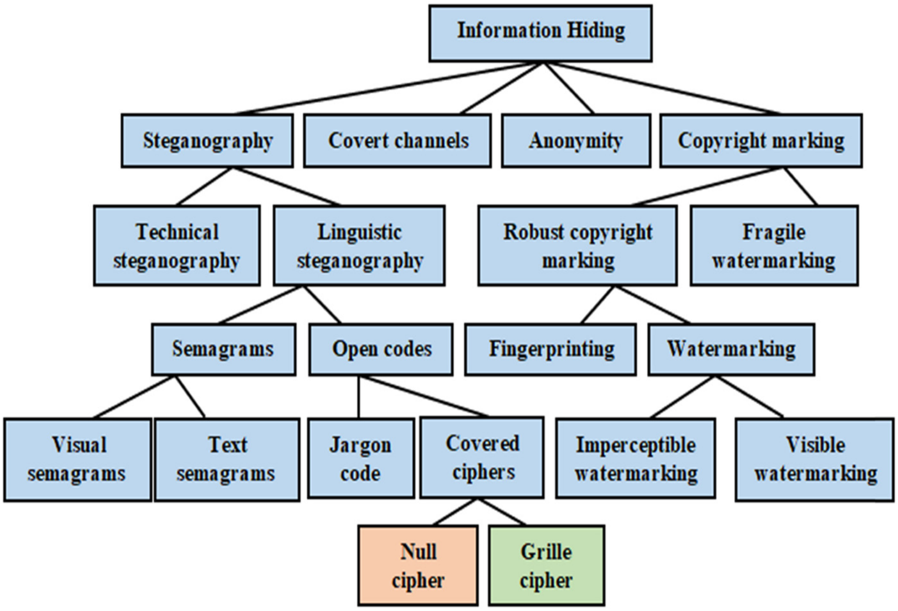

Figure 1: Information hiding classification adapted from Bauer [6].

- Text semagrams, where the information is concealed by using different methods for presenting the data.
- Visual semagrams, where innocent-looking object hides the message.
- Jargon code, where the utilization of understood language by agreed parties is used in a different way to common usage.
- Covered null cipher, in which the Payload is concealed into a collection of interlacing instructions agreed upon by the users.
- Covered grille cipher, in which a template is used over a cover object that enables the selection of specific characters which constitute the meant message to be shown while the others are characters that are covered.

Steganography means covered writings originated from two Greek words, “Stegos” and “Graphia.” Steganography is defined as the science of hiding communication in objects [9]. The assigned person to receive the message is informed in advance about concealed communication [10]. Hence, the secret message is concealed on a cover medium that has redundant bits [11]. The medium that carries the embedded message is called the cover media, while the hidden note is known as the stego message [12]. Thus, steganography's key objective is to conceal information by preventing an unauthorized person from reading the contents of the message using professional algorithms. Likewise, revealing the hidden data requires high expertise and complex techniques, as discussed in this work. The process of steganography involves four components; the first is the **c**over object (**C**) which is a carrier of the concealed message; the second is the secret **m**essage (**M**) which is concealed in the cover object; the third is the technique used for applying steganography; and finally, the stego **k**ey (**K**) that encodes and decodes the Payload. Figure 2 illustrates the steganography workflow inspired by the work in [13].

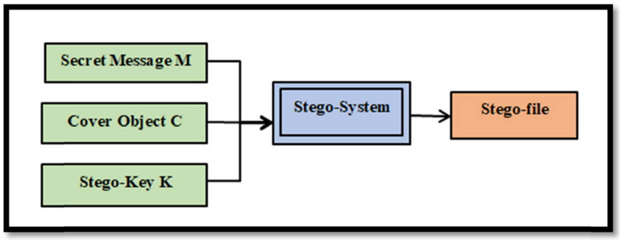

Figure 2: Steganography workflow.

Steganography is another term for covert communication that hides messages in an innocent medium and then sends it to the intended recipient. A steganographic system's key condition is to make it unfeasible for an observer to identify a stego object (the object that contains the hidden message) [14]. Steganography is a way of securing information exchange by hiding the message within an object [15].

Johannes Trithemius (1462–1516) used the term steganography for the first time in his trilogy Polygraphia and Steganographia [14]. The first documented manuscript tells about steganography being used for communication is due to Herodotus [16]. When Histiaeus wanted to transmit a secret message to Miletus, they shaved the slave's hair and tattooed the secret message on his scalp; the slave travelled and after his hair grew upon arriving, his hair was shaved again to disclose the hidden message [17]. Moreover, Herodotus documented the story of Demeratus, who used steganography to alert Sparta about the intended invasion of Greece by the Persian Greet King Xerxes. Demeratus applied steganography by scraping the wax off the outward of a wooden writing tablet, writing the secret message on the wood, and then coating the tablet with wax to make it look like a regular new writing tablet, not to raise the suspicion. Beside, Aeneas the Tactician is credited with describing some simple techniques for concealing a text message by manipulating letters' length or placing letters inside the text using small holes [18].

Hiding messages in the text are known as linguistic steganography or acrostics. An example of linguistic steganography is what was performed by Cardan's Grille, which was originally considered in China and reinvented by Cardan (1501–1576). His method worked by putting a mask over a text that points to random letters from the text; thus, the mask plays a secret stego key that communicates between the coder and the encoder [11]. Brassil's robust text steganography method worked by slightly shifting the text lines up or down by 1/300 of an inch [19]. In 1857, Brewester proposed a steganography technique that shrank the message size to resemble specks of dirt that can still be read under high magnification [20]; this method was actually used in wars through nineteenth and the twentieth centuries. During World War I, the Germans implemented "microdots" hidden in postcards' edges sealed with starch and opened with a knife. Another form of steganography is the use of invisible ink composed of organic liquids such as milk, lemon, urine, or sugar solution in which messages written with such ink become perceptible once the paper is heated [21,22]. With the extensive use of e-media, a great interest has been developed in applying steganography to such media.

During the steganography process, the redundant bits of a digital file can carefully be used for embedding without leaving significant artifacts that lead to easy detection. Steganography classification can be based either on the kind of cover work or the embedding method adopted. Examples of steganographic cover objects are text, image, video, or protocol. In contrast, the embedding method's type is either insertion, substitution, or generation method [23,24]. The insertion method attaches a message in the cover objects' areas that are disregarded by applications. Therefore, the stego object's size is expected to be larger than the original cover object size. The substitution method hides secret messages by substituting the bits of low importance in the cover object with the Payload bits; hence, the stego file size is different from its original identical version. The generation method uses messages to generate cover and stego files. Therefore, this method is hard to detect a hidden message since a cover object without a Payload does not exist for comparison [25,26]. Figure 3 illustrates the classification of the steganography system.

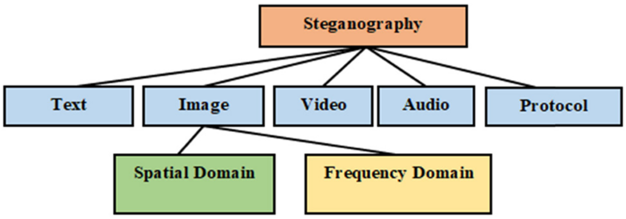

Figure 3: Steganography classifications.

Secret messages can be hidden inside diverse categories of cover such as text files, an image, audio, video file, even programs, networks, etc. There is wide popularity for applying steganography to images due to the high proportion of redundant bits present. One standard method of applying steganography is embedding information inside photo image files. Many steganographic tools are available to store secret messages inside different types of cover objects. The hidden message is stored inside the photo without altering or changing its features and is considered the essential cover object's property. If the cover becomes distorted due to the Payload's embedding process, the image may be classified as a suspicious item and could be checked for any steganography application [27]. Steganography techniques are associated with algorithms categorized based on the domain and the file formats [28]. An example of an algorithm suitable for the spatial domain is the LSB algorithm, while the so-called discrete cosine transform algorithm operates on bits of a frequency transform [29,30]. Harmony search algorithm (HSA) is a metaheuristic created in the last decade by Geem et al. [31] in 2001. It mimics the behavior of a singer who achieves complete harmony. The improvisational phase of musicians influenced HSA. A musician seeks out the ideal notes in order to create perfect harmony. HSA was created based on this idea to find a successful solution to an optimization problem. Clustering problems, engineering problems, scheduling, machine vision problems, and global optimization are some of the problems that can be solved using HSA. The HSA is regarded as an effective algorithm with an efficient application. Due to its ease of implementation over other metaheuristics, it solved a broad range of real-world optimization problems. During a search, it has the potential to find a balance between investigation and exploitation [32].

Image enhancement using image processing techniques has many applications related to enhancing images of advanced space technology, medical diagnosis, biometrics, and imagery satellite for weather prediction. In such several applications, image enhancement is also used to extract useful information from raw images. Many studies apply intelligent algorithms to improve raw images, and thus image enhancement is a necessary preprocessing step in a broad range of computer vision techniques. Edge preservation is essential in edge-sensitive analytic applications such as image in painting and microscopic image evaluation. In this work, we will use the LSB method for hiding the secret message. The research contributions of our study include:

- Designing a framework for an agent-based image steganography system concerning embedding and extracting secret messages within images.
- The extracted features from an image include six statistical metrics: histogram, mean, standard deviation, variance, entropy, and energy.

- Using LSB, the developed software agent can pick out the best cover image suitable for the hidden message size to avoid visual artifacts.

This paper is organized as follows: section two discussed the related studies of image steganography using the LSB method; section three explains the LSB steganography technique; section four introduces the insertion and extraction algorithms of a stego system using the LSB technique; section five covers the agent System properties and Ensembled classification; sections six and seven present our proposed steganography method using an agent-based steganography system and its implementation, respectively; section eight covers the evaluation metrics used to evaluate the produced stego images; and finally, section nine presents the conclusion of the work.

2 Related work

Yedroudj et al. [33] proposed steganography designs depending on the 2-player game that considered stego noise power and improved communication between the hiding and the revealing networks. Elharrouss et al. [34] designed an image steganography system using K LSB coding that hides k least bits of secret message in an image. To extract the embedded message, he designed a technique that detects regions in an image to identify the blocks held by the secret message. Horng et al. [35], in applied image steganography, implemented quotient value difference and the LSB methods to implant information within a unique block of an absolute moment for extracting the coded image. Their proposed embedding method contains three steps: applying the quotient value difference and the LSB replacement to embed secret message, embedding additional bit by changing both the high mean and the order of low, then adding up the secret digits by replacing the bitmap of smooth blocks. Chang et al. [36] designed an optimal LSB method for hiding the image into another image using a genetic algorithm that searches for an optimal approximated image hiding. The experiment results showed that the stego image and the image cover are alike. The work of ref. [37] discussed the design of a parallel processing image method based on reactive agents that would detect the image features. They suggested a technique for continuity perception using a multi-agent system where agents can check an image containing light and dark rings. Agents were given names, darkening agent and lightening agent, and were able to exchange messages in asynchronous manner. Thampi and Sekaran [38] proposed an image steganalysis method that depends on image feature, steganography, and mobile agents. They showed that the important features of an image could be concealed inside an image without altering the quality. A mobile agent can manage the query phase of a steganographic system. The projected system provided high efficiency in hiding the message bits and quick message extraction. The authors of ref. [39] implemented agent software to select the best cover object from a database of cover images to hide a specific message using several features. The proposed agent helped in enhancing the stego image quality from the server. Zeng et al. [40] designed a framework for a hybrid deep-learning that can utilize quantization and truncation for large-scale JPEG steganalysis. They conducted extensive experiments on 500,000 cover images extracted from Image-Net and found out that the combination of quantization and truncation improves the uncovering performance by a clear margin. We agree with the proposed work of ref. [41] for image steganography using the LSB method if used with a software agent which would conceal and obtain the hidden message from images. AbdelRaouf in ref. [42] uses adaptive LSBs to propose a novel data hiding technique for steganography images based on human visual properties LSB. In order to improve the visual presentation of the output stego image, they employed two approaches: first, the human eye sensitivity to RGB color channels; second, photographs usually concentrate on their middle region, allowing the secret message to be hidden in a spiral pattern that runs from the image's edges to its core. Fateh et al. in ref. [43] suggested an enhanced LSB matching technique. Their proposed scheme consists of two phases: message insertion and message extraction. They converted the secret message into a bit-stream in the embedding process and then divided the bit-stream into a series of blocks with n bits in each block, and they hid those n bits in selected pixels. Swain [44] discusses high-capacity data, steganography technology mistreatment differentials, and substitution mechanisms. Segmenting the image into 3 × 3 pixel blocks without overlapping to provide clear region that can be encrypted correctly. The least important piece replacement is employed on the least big piece for each rectangle pixel, and QVD is also applied to the remaining six pieces. Priyadharshini et al. [45] used steganography to add another layer of protection to the medical picture. For example, "The medical image is encrypted using a one-time pad encryption algorithm, and the encrypted image is then implanted into a cover image to create a stego image, making the device more resilient to the intruder"[45]. Gupta et al. in ref. [46] introduced information protection for people who exchange information with one another. They compared and contrasted various methods of image steganography replacement techniques. They used replacement techniques for the LSB and the Most Significant Bit. The secret message was concealed into an image file, which was decoded afterward to reveal details. Sasmal et al. in ref. [47] used the pixel indicator technique to hide details in RGB images, where at least two major bits were used as opposed to one for the networks. The presence of data in the other two channels was shown by the colors red, green, or blue. Random nature indicator bits are generated in the channel based on the picture.

3 Image steganography using LSB method

LSB is a simple steganography insertion method in which the lower bit of the original image, in particular, is substituted by a bit of the confidential message [48]. The 8 bit planes of an image detail the LSB plane of the replaced message during the embedding process, as illustrated in Figure 4.

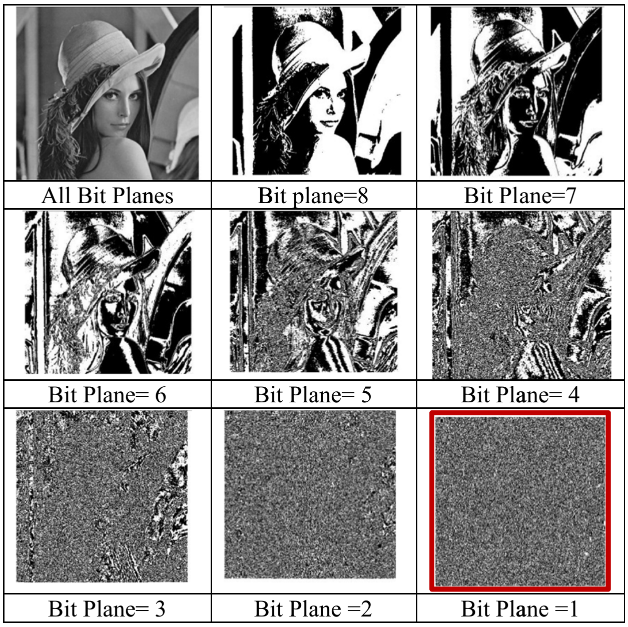

Figure 4: The 8 bit planes of the gray scale image.

In a 24 bit image, a single bit can be used from the RGB color components since every pixel is saved as a byte. Therefore, every pixel may store 3 bits of Payload data [49]. For more illustration, the binary representation of the number 200 is equal (11001000). When embedding the binary equivalent of the number 200 in the modified image grid, a replacement process is applied to the rightmost binary value in the first 8th bytes of the 3 pixels grid, resulting in a replacement of the 8 bit value (00101101) from the original grid above by the value (0010110**1**) in the modified grid. Though the integer 200 was substituted with the LSB of the first 8 bytes, only 3 bits actually need to be changed on the cover image based on the resulted embedded message. This indicates that not all the LSBs are needed to be changed. Usually, the variation between the original file and the stego one is not perceptible to the human visual system, as exemplified below by an original image grid of 3 pixels times 24-bit, as can be viewed in Table 1:

Table 1: LSB method for embedding secret message in an image

The pixel	The RGB bit planes of each pixel	The character	The hidden character in the pixels
🟧	(00101101 00011100 11011100)	**(11001000)**	(0010110**1** 0001110**1** 1101110**0**)
🟧	(10100110 11000100 00001100)		(1010011**0** 1100010**1** 0000110**0**)
🟧	(11010010 10101101 01100011)		(1101001**0** 1010110**0** 01100011)

Note: The significance of bold and underlined values present in Table 1 as samples for LSB method for embedding secret message in an image.

The main disadvantage of the LSB is related to its weak binary system of encoding and decoding. However, several advantages that encouraged the authors to use the LSB algorithm in image steganography include its robustness, capability to embed sizable messages, high similarity in generated input/output image, methodology included in other complicated algorithms, and straightforward when applied.

4 Experiment design using LSB embedding and extracting algorithm

For implementation setting up, the authors reviewed several databases in search of a benchmark steganographic dataset; our findings indicated a need for building one. The most popular ones in the google hits are Lena and Baboon, Lena, ImageNet, COCO and Wikiart.org, BOSSbase and celebA, MNIST and celebA, USC-SIPI, Div2K, SZUBase, Pascal VOC, BOWS2, BURSTbase, ALASKA, Greenspun, NRCS, NRCS, UCID, Kodak PhotoCD PCD0992, STEGRT1, and BOSSrank. These datasets vary in total size, training/testing samples, image size/quality, image format, and the creation purpose. The initial decision was made to select a dataset created mainly for steganography with training/test samples for gray images; size of datasets being not less than 10K with at least 512 × 512 dimensions. For the purpose of this work, we had to form criteria for the cover image as well as the number of features, which eventually would affect the processing time. It was observed that the size of the hidden message correlates with the quality and size of the image. Thus, the final decision was based on five characteristics: the creation purpose, image size, image quality, size of the database, and training/testing samples. Therefore, the BOSSbase was the best choice for this work since more than 10K uncompressed huge resolution images. This dataset was created for steganography purposes and converted to grayscale.

In this work, we present the embedding and the extracting LSB algorithm for hiding a secret message in images in subsections A and B. Then, we show the implemented pseudo-random generator for the hiding process to increase the security of the message hidden. Figure 5 depicts the embedding process.

A.LSB Embedding Algorithm

```
Input: photo cover (p) ∈$P^l$,  secret message (x) ∈$\{0, 1\}^m$, key (k)
Output: stego photo (g) with x implanted note bits
PRNG Seed with k
route = comb (l);
//comb (l) is a pseudo-random combination of {1,2,. l}
g = c;
z = min(x,n);
for j = 1 to z {
    g[route[j]] = c[route[j]] + m[i] − c[route[j]] mod 2;
    }
```

B.LSB Extracting Algorithm

```
Input: stego image (g) $\in P^l$, key (k)
Output: secret message (msg)
PRNG Seed with k
route = comb (l);
//comb (l) is a pseudo-random combination of {1,2,. l}
for i = 1 to m {
    msg[i] = s[route[i]] mod 2;
    }
```

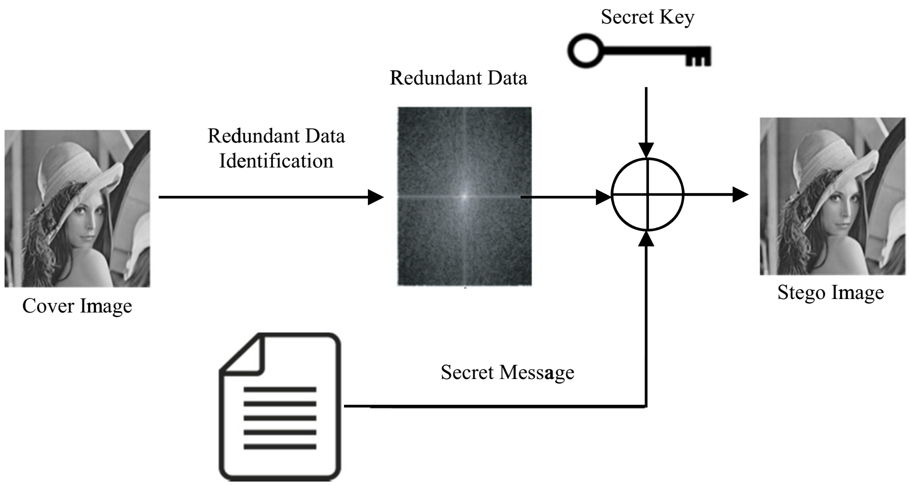

Figure 5: The embedding process for a confidential message into an image using the LSB method.

5 Agent system properties and ensemble classification

An agent is software built to act in a specific environment to perform an independent action to meet its designed objective. The properties of the software agent are listed as following [50]:

- Autonomous: autonomous is one property that distinguishes an agent from an object; thus, the agents are independent and capable of making their own decisions.
- Situated: the agent is situated in an environment.
- Being able to identify changes in the environment.
- Has skills and can offer services.
- Flexibility: an agent is flexible in terms of being responsive in which the agent can observe its surroundings and react to transformation, proactive as the agent can show resourceful actions and take the initiative when needed, and socially in which the agent can interact with other agent or human to find solutions to problems.

An agent can be classified as a mobile or learning agent. They can also be classified based on the tasks they do, such as agents that collect information or agents that filter emails or control architecture or sensitivity. Further, the agent can apply an Ensemble classifier for different parameters as Payload and LSB methods for the best cover image and image steganography. The agent can arbitrarily divide the dataset into training/testing, which equals 2/3 and 1/3 of the data samples, respectively, for Ensemble Classification. The Payload was set to 0.2, meaning a single bit of secret message is inserted into every defined ($n = 3$) pixel of the original image. The Ensemble classifier performance in both training and testing was evaluated in two different scenarios. The first scenario is tested with message length ranging between 16777 and 55929 bits using the English language with a minimum 20% training dataset. The following sequence of (1,0) displays the binary representation.

010001100110000101110100011011010110000101101000000100000010000100110000101101111011101000110100001101101011000010110111000100000000001010

The second scenario uses a bilingual (Arabic/English) message in the range between 16777 and 55929 bits. The following sequence of (1,0) displays the binary representation with a maximum 50% training dataset.

01000110011000010111010001101101011000010110100000010000001000010011000010110111101110100
0110100001101101011000010110111000100000000001010 11000101000110001100111100100010100100000011
0001001111100100010011001000100110010001110010000011000100111110010001001100011000111000101
10111001000101110010001100010000011000100111110010001001100011000111000101101110010010101100
1000101

The Receiver Operating Characteristics (ROC) curves show both Ensemble classifier scenarios in Figures 6 and 7. The area under the ROC curve displays the accuracy measure; if the Ensemble classifier has an area of 1.0, it means that the accuracy is perfect. The vertical axis represents the True Positive Rate, while the horizontal axis represents the False Positive Rate. The closer the curve to the top, the more accurate the classifier becomes. It is clear that a strong accuracy rate was generated using bilingual messages; the reason could be related to the training techniques.

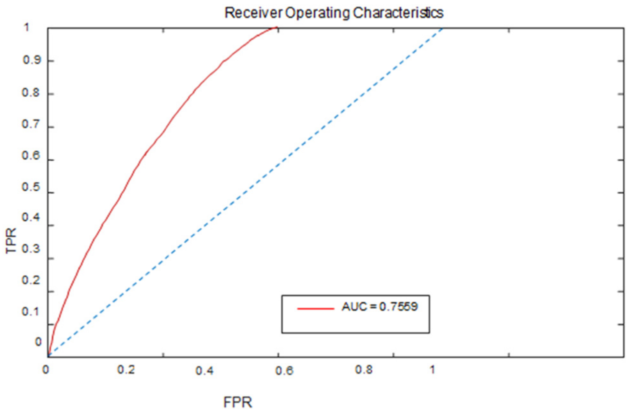

Figure 6: The first scenario medium accurate detector.

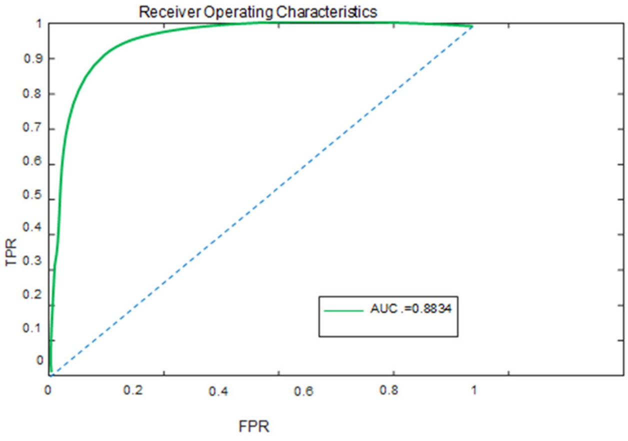

Figure 7: The second scenario strong accurate detector.

6 The proposed method using agent-based steganography system

The proposed agent system would perform the embedding and extracting the secret message's task in an image for the end-user. The recommended selection should be based on some extracted statistical features from an image. Hence, the agent would analyze several image properties; and based on the tested properties results, the agent would select the best cover image to perform steganography. The image statistical feature properties calculated by the agent are:

- Histogram: it is a plot diagram for displaying the numerical distribution of data indicating gray level values against the pixels' number.

$$P(g) = \frac{N(g)}{M} \tag{1}$$

  where $N(g)$ is some pixels at gray level g, and M is some pixels in an image.
- Mean: represents the average value of the general brightness of the image.

$$g = \sum_{r}\sum_{c}\frac{I(r,c)}{M} \tag{2}$$

  where $I(r,c)$ is the value of the image pixel.
- Standard deviation: represents the square root of variance. It will identify the contrast in an image

$$\sigma_g = \sqrt{\sum_{L-1}^{g=0}(g-g)p(g)} \tag{3}$$

- Entropy: entropy is a measure bits' number needed for coding the image's data. The entropy increases if the pixels' values distributed fall more within the gray area.

$$\text{Entropy} = \sum_{L-1}^{g=0} p(g)\log_2[p(g)] \tag{4}$$

- Variance: variance measures "roughness" in image's regions

$$\sigma_g^2 = \sum_{g=0}^{L-1}(g-g)^2 p(g) \tag{5}$$

- Energy: energy measures the intensity variation in an image region

$$E = \sum_{g=0}^{L-1}(p(g))^2 \tag{6}$$

The designed steganographic agent seeks to find a cover image from the database with high variance, deviation, and entropy. The agent selects the object's cover suitable to insert a less or nearly similar message to the cover image size. The framework of proposed steganography-based agents is presented in Figure 8. In summary, the agent would be situated at random on the image (the environment). Selecting a proper cover image based on the above-mentioned six statistical features (Histogram, Mean, Standard deviation, Entropy, Variance, and Energy) for steganography is highly significant as it impacts the result obtained significantly from the proposed system and influenced the security of the produced stego image.

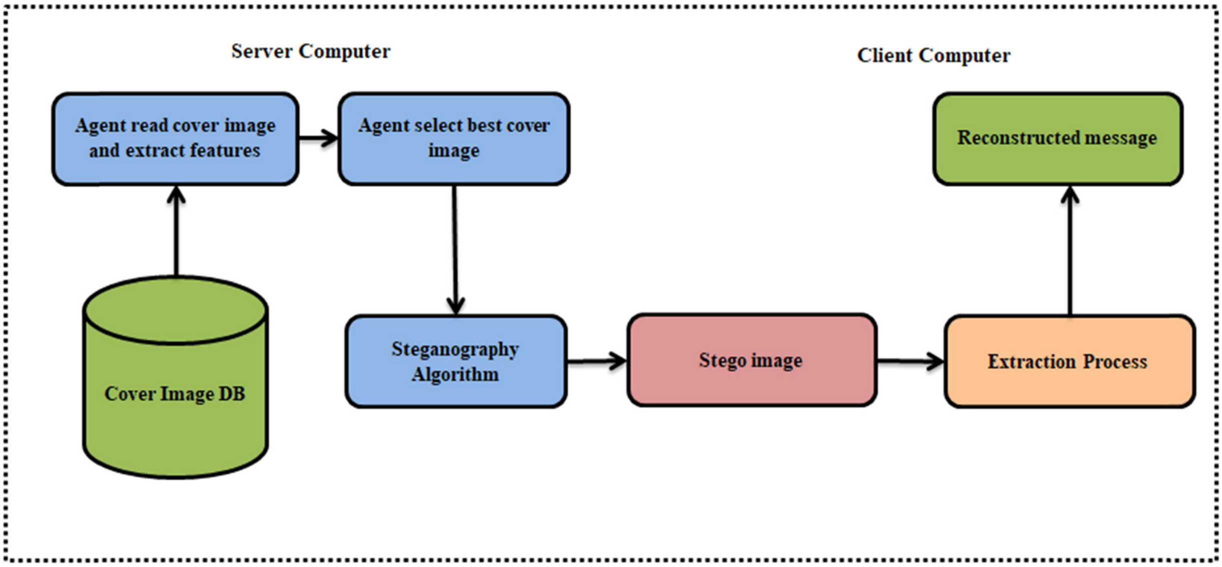

Figure 8: The framework of proposed steganography-based agent.

7 The implementation

An agent helps in the steganography task by deciding on the best cover image from a set of images; thus, the selection of the cover image is highly significant because it impacts the security of the stego systems and the visual appearance artifacts after performing the steganography task. The agent analyzes the images' features and accordingly selects the images to perform LSB steganography on them with minimum artifacts. The image features include mean, entropy, variance, contrast, energy, and standard deviation. For example, the agent would look for images with high contrast, entropy, and energy value to be used as cover images for high Payload. Table 2 presents an example of the six extracted statistical features from a grayscale cover image Lena downloaded from the SIPI image database page with a 256 × 256 dimension

Table 2: A sample of cover image's features

Image	Mean	Entropy	Variance	Contrast	Energy	Standard deviation
	124.0397	7.4645	2390.966	4.771852	1.123891×10^{-1}	4.889745×10^{1}

The implementation of the features' extraction by applying the LSB steganography algorithm (see Section 4) was conducted using Matlab. In this context, an architecture based on software agents was developed using Matlab that works as a development platform, receiving the requests and processing their respective requisitions. Below is a snippet of Matlab code for the embedding.

```
key = 994;
msg = 'A secret message to be hidden';
msgBin = dec2bin(msg,8)';
length_msgBin = length(msgBin);
img = imread('Image.jpg');
nPixels = numel(img)
imgCopy = img;
rand('state',key);
path = randperm(nPixels);
message = min(nPixels,length_msgBin);
   for i = 1:message
imgCopy(path(i)) = img(path(i)) + msgBin(i)- mod(double(img(path(i))),2);
   End
```

The software agent performs the decision-making; the architecture is characterized as a simple reflection agent due to the user's limited interaction and is relatively autonomous. The agent performs a preestablished action, thus being purely reactive. When the user is interested in performing some tasks (insert an image, secret message, steganography), the system sends a request to the agent to execute the task; the agent performs the request and responds to the user whether the task was executed or not as illustrated in Figure 9.

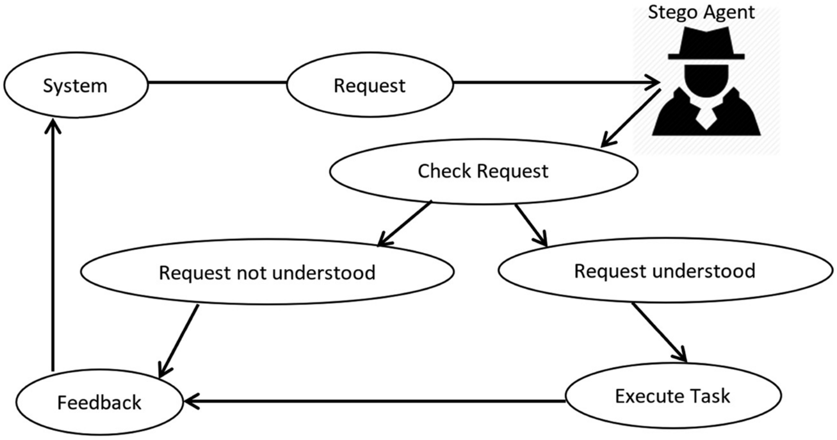

Figure 9: Agent-based image steganography schema.

8 Evaluation of stego images

Steganographic techniques are commonly assessed using three criteria: imperceptibility, capacity, and security. Imperceptibility is considered the most important, but in the following subsections, all three are discussed in subsection A–D below [51,52]. A further important numerical metric is the peak signal-to-noise ratio outlined in subsection E.

8.1 Imperceptibility

Reducing any suspicions about the Payload presence in cover work is very critical. Any speculation about the integrity of the cover detracts from the purpose of stenography and invites cryptanalysis.

8.2 Payload capacity

Capacity represents the size ratio between the cover medium and the secret message [53]. Steganography aims to hide Payload; hence, the more Payload capacity an algorithm achieves, the better this aim is served. There is, however, a balance between the capacity's Payload and invisibility/imperceptibility.

8.3 Security – robustness against statistical attack

Statistical attacks aim to detect a Payload's embedding by applying a set of statistical tests of image data. Some steganographic systems generate signatures or artifacts when hiding a secret message. An algorithm must not leave an artifact to guide statistical attacks [52].

8.4 Security – robustness against image manipulation

During the transmission of a stego message over a communication channel, changes might occur through channel noise. It is also cropping, rotating, or resizing, causing the Payload to be corrupted. Vulnerability to corruption depends on the method used for embedding the Payload. An embedding algorithm should show as little vulnerability as possible [27,46].

8.5 PSNR – peak signal to noise ratio

PSNR indicates a performance image measure alteration captured during a Payload embedding procedure [54]. PSNR measures the level of similarity that the cover and the stego share. PSNR uses decibels (db) for measurements. It can be performed on stego photos to evaluate the quality. A considerable PSNR value reflects a high-quality image which indicates that both the original photo and the stego photo are very similar to each other [55–59]. To calculate PSNR using log:

$$\mathrm{PSNR} = 10\log\frac{(255)^2}{\mathrm{MSE}} \tag{7}$$

where (255) is the maximum 8 bits value representation of a pixel; while MSE indicates the mean squared error or difference between the cover and the stego photo in pixel's values, given as

$$\mathrm{MSE} = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{x,y} - C_{x,y})^2 \tag{8}$$

where M and N represent the photo's dimensions, x and y denote the photo coordinates, $C_{x,y}$ denotes the cover photo, and $S_{x,y}$ represents the stego photo.

The authors considered the LSB steganography method using the developed steganography agent-based technique to embed a random secret message into the original images. In this pass of evaluation, the above six different features were implemented for the set 0.2 Payload [60–73]. The training/testing samples were set both equal to 50%. Figure 10 shows the very strong accuracy rate for the developed agent-based LSB steganography and its capability to select the best cover image for the provided secret message size, almost without noticeable changes to the original image as shown in Figure 11(a–c).

The primary study limitations include no standard steganography dataset, and new techniques such as deep-learning could be used. Quantum technology is recommended to handle multi-agents, multilingual, and multiprocessing systems.

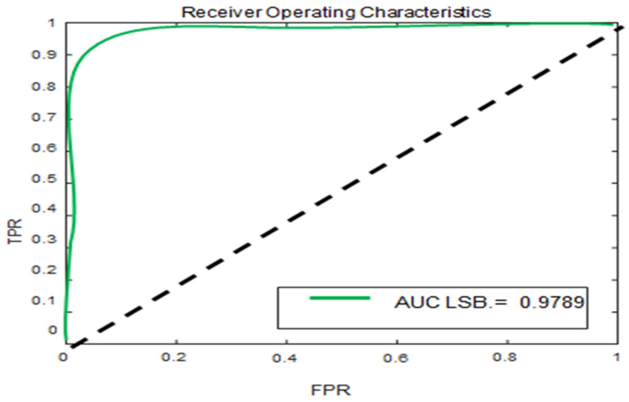

Figure 10: LSB agent-based steganography's strong accuracy.

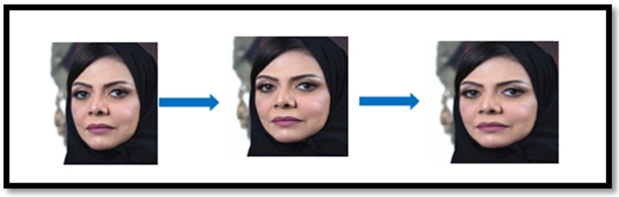

Figure 11: Secret message from original image, normalized image, and stegno image.

9 Conclusion

The past few years have revealed a growing interest in image steganography research. Three essential parameters used in the design process of a steganography algorithm are Payload, security, and fidelity. The Payload is known as the amount of hidden information embedded in the cover object. Security is the inability of the steganalysis system to discover the embedded secret messages. Fidelity is also known as imperceptibility, which refers to how hard it is for humans to distinguish the image's cover from the secret message. Deciding on a proper image to implant a secret message to an end-user requires an understanding of the cover image, which may not be compatible with the length of the secret message. This work investigated a novel steganography technique based on the agent technology framework using LSB. The experiment used six statistical feature measures: histogram, mean, standard deviation, entropy, variance and energy. A steganography Ensemble classifier was implemented to evaluate the suggested metrics using ROC curve. The result shows that the designed agent-based system could select the best cover image for the provided secret message size to avoid visual artifact.

For future work, multi-processing multi-agent software can be designed to handle massively comparative studies with different techniques and generate a single dataset from all available open-access steganography datasets with unified features and parameters.

Acknowledgment: The authors, therefore, gratefully acknowledge DSR's technical and financial support.

Funding information: This project is funded by the Deanship of Scientific research (DSR), King Abdulaziz University, Jeddah, under grant No. (DF-665-165-1441).

Conflict of interest: The authors declare that there is no conflict of interest regarding the publication of this paper.

References

[1] Mehboob B, Faruqui RA. A stegnography implementation. Biometrics and security technologies, 2008. ISBAST 2008. International Symposium on 2008. Isalambad, Pakistan: IEEE; 2008. p. 1–5.

[2] Kumar A, Pooja K. Steganography – a data hiding technique. Int J Comp Appl. 2010;9(7):19–23.

[3] Bailey K, Curran K. An evaluation of image based steganography methods. Multimed Tools Appl. 2006;30(1):55–88.

[4] Wang H, Wang S. Cyber warfare: steganography vs steganalysis. Commun ACM. 2004;47(10):76–82.

[5] Anderson RJ, Petitcolas FA. On the limits of steganography. IEEE J Sel Areas Commun. 1998;16(4):474–81.

[6] Bauer FL. Decrypted secrets: methods and maxims of cryptology. Berlin, Germany: Springer Science & Business Media; 2013.

[7] Petitcolas FA, Anderson RJ, Kuhn MG. Information hiding – a survey. Proc IEEE. 1999;87(7):1062–78.

[8] Castiglione A, Alessio BD, Santis De A. Steganography and secure communication on online social networks and online photo sharing. 2011 International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA). Barcelona, Spain: IEEE; 2011. p. 363–8.

[9] Provos N, Honeyman P. Hide and seek: an introduction to steganography. Sec Privacy IEEE. 2003;1(3):32–44.

[10] Chee A. Steganographic techniques on social media: investigation guidelines. Auckland, New Zealand: Auckland University of Technology; 2013.

[11] Cheddad A, Condell J, Curran K, Kevitt Mc P. Digital image steganography: survey and analysis of current methods. Signal Process. 2010;90(3):727–52.

[12] Hamid N, Yahya A, Ahmad RB, Al-Qershi OM. Image steganography techniques: an overview. Int J Comp Sci Sec (IJCSS). 2012;6(3):168–87.

[13] Li B, He J, Huang J, Shi YQ. A survey on image steganography and steganalysis. J Inf Hiding Multimed Signal Process. 2011;2(2):142–72.

[14] Fridrich J. Steganography in digital media: principles, algorithms, and applications. Cambridge, United Kingdom: Cambridge University Press; 2009.

[15] Cox I, Miller M, Bloom J, Fridrich J, Kalker T. Digital watermarking and steganography. Massachusetts, United States: Morgan Kaufmann; 2007.

[16] Marincola J. Herodotus: the histories. Trans. by A. de Sélincourt. Rev. with introductory matter and notes by J. Marincola. Harmondsworth: Penguin Books; 1996.

[17] Khare P, Singh J, Tiwari M. Digital image steganography. J Eng Res Stud. 2011;2:101–4.

[18] Tacticus A. How to survive under siege/aineias the tactician (Clarendon ancient history series). Oxford, UK: Clarendon; 1990.

[19] Brassil J, Low S, Maxemchuk N, O'Gorman L. Hiding information in document images. Proceedings of Conference on Information Sciences and Systems (CISS-95). Dublin, Republic of Ireland: IEEE; 1995. p. 482–9.

[20] Brewster D. Microscope, volume XIV. Encyclopaedia Britannica Dict arts, sciences, gen literature, Edinburgh, IX – application photography microscope. London, UK: IEEE; 1857. p. 801–2.

[21] Rizwan U, Ahmed HF. A new approach in steganography using different algorithms and applying randomization concept. Int J Adv Res Comp Commun Eng. 2012;1(9):348–66.

[22] Johnson NF, Jajodia S. Exploring steganography: Seeing the unseen. Computer. 1998;31(2):26–34.

[23] Hussain M, Hussain M. A survey of image steganography techniques. Tirunelveli, India: IEEE; 2013.

[24] Hariri M, Karimi R, Nosrati M. An introduction to steganography methods. World Appl Program. 2011;1(3):191–5.

[25] Bhattacharyya S. Data hiding through multi level steganography and ssce. J Glob Res Comp Sci. 2011;2(2):13762.

[26] Rabah K. Steganography-the art of hiding data. Inf Technol J. 2004;3(3):245–69.

[27] Pope MB, Warkentin M, Bekkering E, Schmidt MB. Digital steganography – an introduction to techniques and tools. Commun Assoc Inf Syst. 2012;30(1):22.

[28] Kaur J, Kumar S. Study and analysis of various image steganography. Tech IJCST. 2011;2(3):2229–433.

[29] Kaur S, Kaur A, Singh K. A survey of image steganography. IJRECE. 2014;2(3):102–5.

[30] Madhuravani B, Reddy PB, Lalith Samanth Reddy P. International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) Chennai, India: IEEE; 2017. p. 1308–14.

[31] Geem ZW, Kim JH, Loganathan GV. A new heuristic optimization algorithm: harmony search. Simulation. 2001;76(2):60–8.

[32] Dubey M, Kumar V, Kaur M, Dao T-P. A systematic review on harmony search algorithm: theory, literature, and applications. Math Probl Eng. 2021;2021, 1–22.

[33] Yedroudj M, Comby F, Chaumont M. Steganography using a 3-player game. J Vis Commun Image Represent. 2020;72:102910.

[34] Elharrouss O, Almaadeed N, Al-Maadeed S. An image steganography approach based on k-least significant bits (k-LSB). 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT). Doha, Qatar: IEEE; 2020. p. 131–5

[35] Horng J-H, Chang C-C, Li G-L. Steganography using quotient value differencing and LSB substitution for AMBTC compressed images. IEEE Access. 2020;8:129347–58.

[36] Chang C-C, Hsiao J-Y, Chan C-S. Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. Pattern Recog. 2003;36(7):1583–95.

[37] Bergenti F, Gleizes M-P, Zambonelli F. Methodologies and software engineering for agent systems: the agent-oriented software engineering handbook. Berlin, Germany: Springer Science & Business Media; 2006.

[38] Thampi SM, Sekaran KC. Steganography based WWW distributed image retrieval with mobile agents, Vol. 4. London, United Kingdom: CoRR; 2004. p. 1–9.

[39] Sadkhan SB, Al-Barky A, Muhammad NN. An agent based image steganography using information theoretic parameters. MASAUM J Comput. 2009;1(2):258–64.

[40] Zeng J, Tan S, Li B, Huang J. Large-scale JPEG image steganalysis using hybrid deep-learning framework. IEEE Trans Inf Forens Sec. 2017;13(5):1200–14.

[41] Nascimento DDL, Couto FRP, Wolski LZ, Kuhnen IA. Image steganography using LSB and software agents. Int J Eng Res Tech. 2017;6(3):191–5.

[42] AbdelRaouf A. A new data hiding approach for image steganography based on visual color sensitivity. Multimed Tools Appl. 2021;80:23393–417.

[43] Fateh M, Rezvani M, Irani Y. A new method of coding for steganography based on LSB matching revisited. Sec Commun Netw. 2021;2021:6610678.

[44] Swain G. Very high capacity image steganography technique using quotient value differencing and LSB substitution. Arab J Sci Eng. 2019;44(4):2995–3004.

[45] Priyadharshini A, Umamaheswari R, Jayapandian N, Priyananci S. Securing medical images using encryption and LSB steganography. 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT). Bhilai, India: IEEE; 2021. p. 1–5

[46] Gupta LK, Singh A, Kushwaha A, Vishwakarma A. Analysis of image steganography techniques for different image format. 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT). Bhilai, India: IEEE; 2021. p. 1–6

[47] Sasmal MM, Mula MD. An enhanced method for information hiding using lsb steganography. J Phys Conf Ser. 2021; 1797(1):012015. Kalyani, West Bengal, India: IOP Publishing.

[48] Sharma VK. Vishal shrivastava,"A Steganography Algorithm for Hiding Images by improved LSB substitution by minize detection." J Theor Appl Inf Technol. 2012;36(1):14564.

[49] Neeta D, Snehal K, Jacobs D. Implementation of LSB steganography and its evaluation for various bits. 2006 1st International Conference on Digital Information Management. Bangalore, India: IEEE; 2006. p. 173–8.

[50] Ker AD. Quantitative evaluation of pairs and RS steganalysis. Security, steganography, watermarking multimed contents VI. Vol. 5306, California, United States: International Society for Optics and Photonics; 2004. p. 83–97.

[51] Solanki R, Chuahan M, Desai M. Survey of image steganography techniques. Kollam, India: IEEE; 2017.

[52] Morkel T, Eloff JH, Olivier MS. An overview of image steganography. ISSA. 2005;1(2):1–11.

[53] Sallee P. Model-based steganography. International Workshop on Digital Watermarking. Seoul, Korea: Springer; 2003. p. 154–67.

[54] Sharda S, Budhiraja S. Image steganography: a review. Int J Emerg Technol Adv Eng. 2013;3(1):707–10.

[55] Al-Mohammad A. Steganography-based secret and reliable communications: Improving steganographic capacity and imperceptibility. Uxbridge, England: Brunel University, School of Information Systems, Computing and Mathematics Theses; 2010.

[56] Hemalatha S, Acharya UD, Renuka A, Kamath PR. A secure and high capacity image steganography technique. Signal mage Process. 2013;4:83.

[57] Podder AK, Bukhari AA, Islam S, Mia S, Mohammed MA, Kumar NM, et al. IoT based smart agrotech system for verification of Urban farming parameters. Microprocess Microsyst. 2021;82:104025.

[58] Ghani MKA, Mohammed MA, Ibrahim MS, Mostafa SA, Ibrahim DA. Implementing an efficient expert system for services center management by fuzzy logic controller. J Theor Appl Inf Technol. 2017;95:13.

[59] Mohammed MA, Al-Khateeb B, Ibrahim DA. Case based reasoning shell frameworkas decision support tool. Indian J Sci Technol. 2016;9(42):1–8.

[60] Mostafa SA, Mustapha A, Gunasekaran SS, Ahmad MS, Mohammed MA, Parwekar P, et al. An agent architecture for autonomous UAV flight control in object classification and recognition missions. Soft Comput. 2021;22:1–14. doi: 10.1007/s00500-021-05613-8.

[61] Lakhan A, Mastoi Q-Ul-A, Elhoseny M, Memon MS, Mohammed MA. Deep neural network-based application partitioning and scheduling for hospitals and medical enterprises using IoT assisted mobile fog cloud. Enterprise Information Systems; 2021:1–23. doi: 10.1080/17517575.2021.1883122.

[62] Liang C, Li Y, Luo J. Realizing an effective COVID-19 diagnosis system based on machine learning and iot in smart hospital environment. IEEE Inter Things J. 2016 May–June;13:549–56. doi: 10.1109/JIOT.2021.3050775.

[63] Mohammed MA, Gunasekaran SS, Mostafa SA, Mustafa A, Ghani MKA. Implementing an agent-based multi-natural language anti-spam model. 2018 International Symposium on Agent, Multi-Agent Systems and Robotics (ISAMSR). Putrajaya, Malaysia: IEEE; 2018. p. 1–5. doi: 10.1109/ISAMSR.2018.8540555.

[64] Liang C, Li Y, Luo J. A review of fog computing and machine learning: concepts, applications, challenges, and open issues. IEEE Access. 2019;7:153123–40. doi: 10.1109/ACCESS.2019.2947542.

[65] Mostafa SA, Mustapha A, Hazeem AA, Khaleefah SH, Mohammed MA. An agent-based inference engine for efficient and reliable automated car failure diagnosis assistance in. IEEE Access. 2018;6:8322–31. doi: 10.1109/ACCESS.2018.2803051.

[66] Mutlag AA, Khanapi Abd Ghani M, Mohammed MA, Maashi MS, Mohd O, Mostafa SA, et al. MAFC: multi-agent fog computing model for healthcare critical tasks management. Sensors. 1853;2020:20. doi: 10.3390/s20071853.

[67] Lahoura V, Singh H, Aggarwal A, Sharma B, Mohammed MA, Damaševičius R, et al. Cloud computing-based framework for breast cancer diagnosis using extreme learning machine. Diagnostics. 2021;11:241. doi: 10.3390/diagnostics11020241.

[68] Makhadmeh SN, Al-Betar MA, Alyasseri ZAA, Abasi AK, Khader AT, Damaševičius R, et al. Smart home battery for the multi-objective power scheduling problem in a smart home using grey wolf optimizer. Electronics. 2021;10:447. doi: 10.3390/electronics10040447.

[69] Mostafa SA, Gunasekaran SS, Mustapha A, Mohammed MA, Abduallah WM. Modelling an Adjustable Autonomous Multi-agent Internet of Things System for Elderly Smart Home. In: Ayaz H, editor. Advances in neuroergonomics and cognitive engineering. AHFE 2019. Advances in intelligent systems and computing. Vol 953. Cham: Springer; 2020. doi: 10.1007/978-3-030-20473-0_29.

[70] Mujahid A, Awan MJ, Yasin A, Mohammed MA, Damaševičius R, Maskeliūnas R, et al. Real-time hand gesture recognition based on deep learning YOLOv3 model. Appl Sci. 2021;11(9):4164.

[71] Khalaf BA, Mostafa SA, Mustapha A, Mohammed MA, Mahmoud MA, Al-Rimy BAS, et al. An Adaptive protection of flooding attacks model for complex network environments. Sec Commun Netw. 2021;2021:1–17.

[72] Kashinath SA, Mostafa SA, Mustapha A, Mahdin H, Lim D, Mahmoud MA, et al. Review of data fusion methods for real-time and multi-sensor traffic flow analysis. IEEE Access; 2021;9:51258–76.

[73] Zhou X, Ma Y, Zhang Q, Mohammed MA, Damaševičius R. A reversible watermarking system for medical color images: balancing capacity, imperceptibility, and robustness. Electronics. 2021;10(9):1024.