EasyChair Preprint

№ 5544

Highly Secure Steganography-Based System with Three Layers of Protection

Hajar Alhelow

May 19, 2021

Highly Secure Steganography-Based System With Three Layers of Protection

Hajar ALhelow
Department of Computer Science
Fahad Bin Sultan University,
(Tabuk City), King Saudi Arabia
hajar.m.alhelow@hotmail.com

***Abstract*—Communication and exchanging information via the internet are essential to perform daily tasks in this technological age. Recently, steganography has received great attention from researchers due to its valuable applications in practice. Steganography-based systems suffer from some challenges, and (1) guaranteeing perfect matching between the cover and the stego object and (2) ensuring high resistance against attacks are the most important ones. In this work, a steganography-based system is proposed. The system hides the secret data within the Least Significant Bit (LSB), which forms the first layer against attackers when it comes to discovering the communication between sender and receiver. The LSB is supported by an encryption layer so that if the attacker tries to obtain the secret data, a decryption process is required. The encryption layer is also supported by a randomization layer so that if the attacker has the ability of decryption, a reassembling process is required. Both the session key of the encryption algorithm and the seed of the randomization algorithm are exchanged safely using symmetric and asymmetric algorithms. In terms of PSNR, SSIM, payload capacity, and retrieved bit error rate, the proposed system shows better performance, especially against rotation and bilinear attacks.**

Keywords — hidden secret data, cover, stego object, attack, FBSU logo, PSNR, SSIM, RBER

I. INTRODUCTION

The advancement of data technology and the widespread use of internet have contributed to the ever-growing frequency of interpersonal communication. Data can be leaked through intentional actions of personnel or illegal activity during data transmission, resulting in severe losses. Steganography is an effective way to transmit confidential data. Advanced data hiding techniques are extensively applied to various modern digital images and other media.

A. Background

Steganography can be defined as the science that addresses the process of hiding top secret information within a cover, which can be a text, audio, or image file. The main objective of steganography is distracting the attacker so that they cannot recognize the sender and the receiver within the communication process [1, 2]. There are many applications of steganography that can be used in everyday life. Examples include the following [3]:

1. Confidential communication and secret data storage.
2. Protection from data alteration.
3. Access control system for digital content distribution.

In the medical sector, for example, steganography can be used to ensure the integrity of the medical content so that the content is protected against modification attack [4]. Moreover, steganography can be used as an effective tool to ensure copyright protection [5].

B. Problem Statement

Despite the valuable benefits of steganography, it is not without problems. Since this research field falls in the cybersecurity domain, the problem it is related to is tightly coupled with attacks that can be applied by an attacker. To state the problem, we start with the classic scenario of a steganography-based system. Figure 1 illustrates the classic scenario.

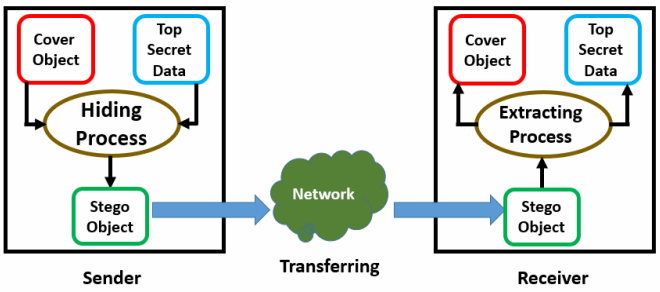


Fig. 1. Classic scenario of steganography-based system.

As shown in Figure 1, the system has two parts, which are the sender and the receiver. In addition, there are three objects that are represented by rectangles. They are as follows:

1. Cover object, which is the file that is used as a container of the data. In common situation, it is an image file.
2. Top secret data, which is the file of the data that is intended to be hidden within the cover object. The data file can be of any data type (e.g., image, text, or audio file).

3. Stego object, which is the file that is generated from hiding the top secret data within the cover object.

At each side, there is a process. At the sender side, it is called hiding process; while at the receiver side, it is called extracting process.

The classic scenario of a steganography-based system has a security gap, which is illustrated by Figure 2.

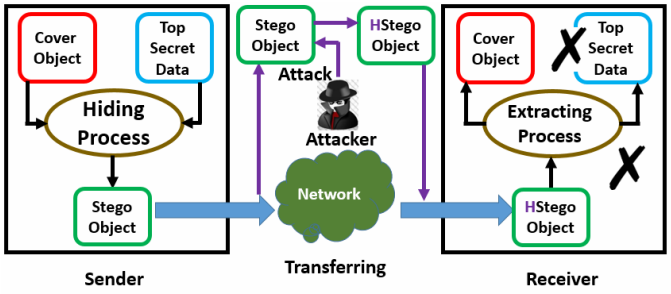


Fig. 2. Security gap of the classic scenario of steganography-based system.

As shown in Figure 2, an attacker (the figure in the middle) is found on the path between the sender and receiver. This attacker can obtain the stego object and then apply an attack on it for the purpose of destroying the hidden data. The altered stego object is called Harmed stego object (HStego object). The attacks applied at the attacker side may be geometric attacks [6], such as rotation, or non-geometric attacks [7], such as Gaussian noise.

C. Research Questions

To protect the hidden data from being destroyed, the steganography-based system should be robust against both geometric and non-geometric attacks [8]. In addition, the level of distortion caused by hiding the secret information should be minimal. In other words, there should be a perfect matching, as far as possible, between the cover object and stego one [9]. Therefore, the research questions can be listed as follows:

1. How can a perfect matching between the cover and stego objects be ensured so that a human cannot recognize the distortion caused by the hiding process while achieving a high level of protection at the same time?
2. How can high resistance against both geometric and non-geometric attacks be guaranteed?

D. Contribution

The contribution of this work can be summarized as follows:

- In responding to the first part of the first research question, we present a LSB-based steganography system that has the ability to hide different types of secret data (text, audio, image) in image or audio files.
- A three protection layers-based approach is proposed to address the second part of the first research question. The LSB layer is supported by an encryption layer followed by a randomization layer to ensure a higher level of protection against security analysis.
- In responding to the second research question, hiding within blocks of LSB of colour pixels is employed to prevent the success of bilinear, rotation, and Gaussian noise attacks.
- Extensive experiments are conducted to evaluate the proposed system in terms of level of distortion, resistance against attacks, and payload capacity.

E. Organization of Paper

The rest of paper is organized as follows. In section 2, the related work is presented. Section 3 provides the proposed system. The results and discussions are documented in section 4. Finally, section 5 concludes the paper.

II. RELATED WORK

In general, the approaches proposed previously in the steganography research field can be classified into three categories, as shown in Figure 3.

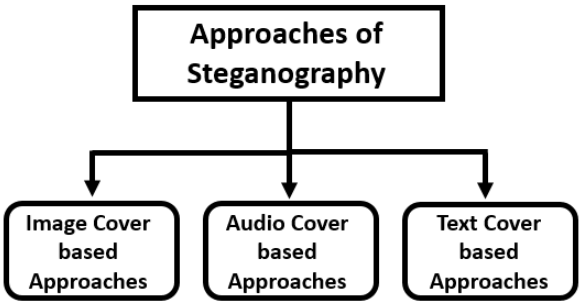


Fig. 3. Classification of steganography approaches.

A. Text Cover-Based Approaches

The authors of [10] presented a comparative analysis of characteristics of information-hiding techniques. They focused on copyrighting the content of digital texts through modifying the structure of the content. They also described types of attacks and advantages and weaknesses of techniques used for hiding in text files.

The authors in the research [11] presented a character-level linguistic steganographic method to encode different secret bit into characters. They employed long short-term memory prediction probability values that train a character-level text.

The authors of [12] proposed the list-based steganography methodology (Listega) that establishes a covert channel within text. The key idea was to hide within types of lists that provide a good chance for robust hiding against attacks (e.g., numeric or dotted).

In [13], researchers proposed a text steganography-based scheme to increase the capacity of hiding. A white space with extended line was adopted in this method with the aim of increasing the efficiency.

Hiding secret data within Arabic text was presented in [14]. The authors relied on engaging Unicode standard

encoding. This method guarantees high-capacity payload embedding and a high level of security.

The research provided in [15] suggested a hybrid technique that combines cryptography and steganography. It worked in the spatial domain of a text written on images. Results showed a considerable enhancement in the mean squared error (MSE), peak signal-to-noise ratio (PSNR), and qualitative and quantitative values.

B. Audio Cover-Based Approaches

The authors of [16] proposed a LSB-based hiding method using a compression algorithm. The key idea was utilizing dictionary-based text for ASCII to reduce the redundancy of data representation. Then, the redundancy was hidden in the LSB of an audio file that provides a cover. This method obtained good performance for hiding various document sizes in germs of high capacity.

The authors in [17] devised an effective MP3 steganalytic algorithm based on joint point-wise and block-wise correlations. Quantified and modified discrete cosine transfer (DCT) coefficients were used to form a matrix representing a MP3 cove. Then, updating the coefficients of the DCT was used for hiding.

The authors of the work [18] designed an audio steganography-based system that was robust against adversarial attacks. The key feature of this work was that it was adapted by the cost, where the cost was adjusted gradually until satisfactory security performances were obtained.

Exploiting a compression mechanism, the researchers in the work [19] proposed a dictionary-based compression in which bits were hidden in the LSB of audio signals. Here, dictionary refers to the secret data represented by the text file. This audio steganography was conducted for various compression algorithms with dictionary-based compression. Audio steganography-based dictionary compression achieved a better value of signal-to-noise ratio (SNR).

Because traditional encrypting methods easily arouse suspicion, an adaptive audio steganography method was proposed in [20]. The authors relied on interval and variable low bit coding, which can be applied to covert wireless communication. The interval for embedding secret messages into the audio file was for selecting the embedding location and embedding bits adaptively. Experimental results show that the proposed approach has better performance in terms of embedding rate and invisibility.

An audio-to-audio steganography-based system was presented in [21]. The authors used the LSB technique in the process of hiding to ensure the lowest level of distortion. This system added an extra layer of security because a transformation function was applied on amplitude bits of secret audio before embedding. Moreover, the provided system was also suitable for embedding secret audio during real time audio communication because processing time was low while embedding capacity was high.

C. Image Cover-Based Approaches

The authors of [22] presented a hybrid method for hiding secret data in image in the transform domain. The key idea behind the hybrid method was the combination of steganography using DCT and cryptography using the One-Time Pad (OTP) or vernam cipher implemented on a digital image. OTP can be seen as a second layer of security on the sender side, where attackers have to overcome this obstacle to obtain secret hidden data.

In [23], a modified Discrete Wavelet Transform- (DWT) based steganography image-to-image system was provided. The authors applied DWT on the cover image to generate four sub-images represented by four sub-bands of frequencies. To overcome the distortion challenge, the authors employed the least variation concept, which refers to hiding secret data only within the low bands of frequencies.

Four techniques were used in [24] to build a steganography system that ensured integrity of medical images. The first technique was the Redundant Integer Wavelet Transform, which was responsible for protecting against non-geometric attacks. The second and third techniques were the DCT and the Singular Value Decomposition (SVD), which were responsible for hiding medical images. The final technique was the logistic chaotic map, which was responsible for encrypting the medical images before hiding.

III. PROPOSED SYSTEM

This section is structured so that the threat model is presented first. Then, the architecture of the proposed system with the roles of components is presented in detail. Finally, the security analysis is discussed to demonstrate the resistance of the proposed system.

A. Threat Model

To define the threat model, four parts are required, which are the identity of the attacker, the malicious goal, the capabilities of the attacker, and the type of the attacks.

The attacker is the Man-In-The-Middle (MITM), and his malicious goal is to destroy the embedded secret information. Figure 4 illustrates the first two parts of the threat model.

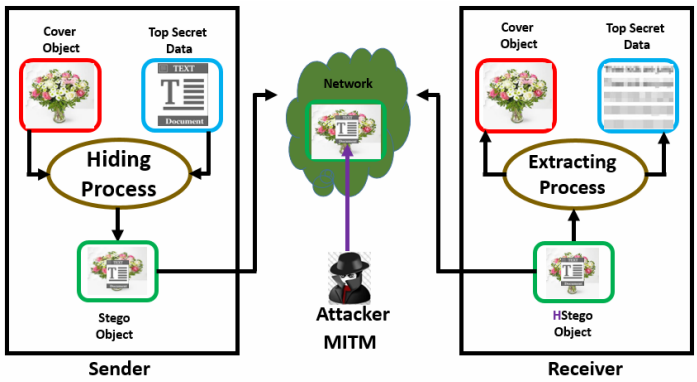


Fig. 4. MITM attacker and malicious goal.

As shown in Figure 4, the attacker is eavesdropping on the network. When the sender sends the stego object, the attacker receives it and then attacks the embedded secret data. This

Identify applicable sponsor/s here. If no sponsors, delete this text box (*sponsors*).

results in a blurry extracted file that represents the damaged secret data.

As for the capabilities of the attacker and the type of the attacks, Table I summarizes these two parts of the threat model.

TABLE I. TABLE TYPE STYLES

Capability number	Name of attack	Kind of attack	Type of attack
1	Bilinear	Geometric	Active
2	Rotation	Geometric	Active
3	Gaussian Noise	Non-geometric	Active

A bilinear attack negatively changes the boundaries of the stgo image file randomly so that it appears that all boundaries are inconsistent [25]. Figure 5 shows the negative impact of the bilinear attack.

Fig. 5. Effect of bilinear attack.

A rotation attack negatively changes the boundaries of the stgo image file so that it modifies the direction of the boundaries [26], as shown in Figure 6.

Fig. 6. Effect of rotation attack.

A Gaussian noise attack changes the resolution of the pixels of the stgo image file so that it negatively modifies the general appearance of the image [27], as shown in Figure 7.

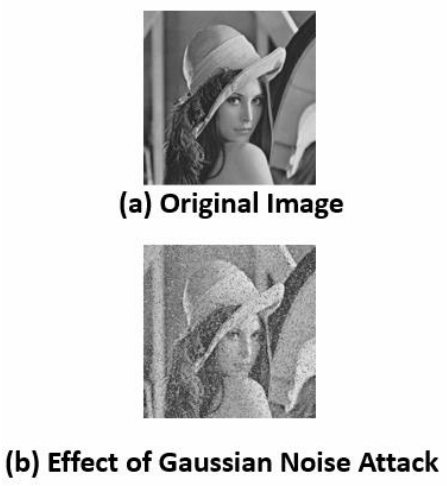


Fig. 7. Effect of Gaussian noise attack.

The three mentioned attacks are considered active type. This means that the attack alters the embedded secret data through the mechanism followed by each attack.

B. *Architecture of the Proposed System*

The objective of the proposed system is to build security layers to make strong defences against the threat model defined above. Figure 8 shows the architecture of the proposed system.

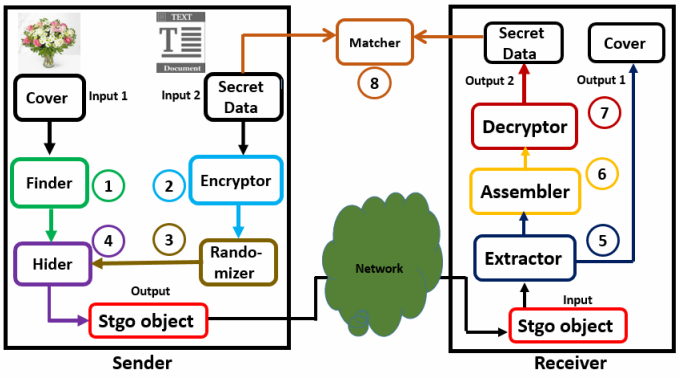


Fig. 8. Architecture of proposed system.

As shown in Figure 8, there are eight elements. Each one has its own task to perform. Table II below summarizes the elements, their tasks, inputs, outputs, and where they are installed.

It is worth mentioning that when the scenario is reversed, the elements that are installed at the sender side will be installed at the receiver side and vice versa. This means that all components are practically installed at both the sender and receiver sides.

TABLE II. ELEMENTS OF PROPOSED SYSTEM.

Name of element	Input	Task	Output	Location
Finder	Image cover	Searching for the suitable location for hiding	LSB	Sender side
Encryptor	Secret data	Encryption	Encrypted secret data	Sender side
Randomizer	Encrypted secret data	Randomization	Randomized encrypted secret data	Sender side
Hider	LSB, Randomized encrypted secret data	Hiding process	Stego object	Sender side
Extractor	Stego object	Extracting process	Cover image, Randomized encrypted secret data	Receiver side
Assembler	Randomized encrypted secret data	Recollection	Encrypted secret data	Receiver side
Decryptor	Encrypted secret data	Decryption	Secret data	Receiver side
Matcher	Input 2, output 2	Matching	Degree of matching	Receiver side

C. Roles of Elements

This section provides the responsibility of each element involved in constructing the architecture of the proposed system, as described in detail below.

1) Role of finder element.

This element is responsible for finding the best location within the cover image to hide the secret data. This task is important because it addresses the first research question regarding perfect matching between the cover object and stego one. A given cover image is represented by a matrix of zeros and ones. The column located on the right side is called the LSB. The column located on the left side is called Most Significant Bit (MSB). Selecting the LSB to be the place where the secret data is embedded ensures that the least distortion is caused by the hiding process. In contrast, selecting the MSB to be the place for hiding the secret data is not suitable due to generating a high level of distortion that can be noticed by attackers. In details, the cover image consists of pixels. Each pixel is a mixture of three main colours (Red, Green, Blue) with different percentages. Each colour is represented by a series of bits, which has LSB and MSB. Figure 9 illustrates the general representation of a cover image in digital world.

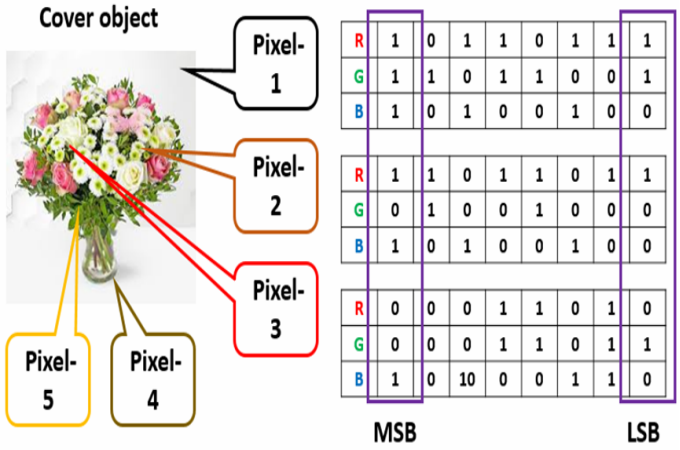


Fig. 9. General representation of a cover image in the digital world.

To prove that replacing (or hiding) the bits of the secret data within the LSB leads to minimum error (or distortion), the values of a given pixel are calculated and changed mathematically, as shown in Figure 10.

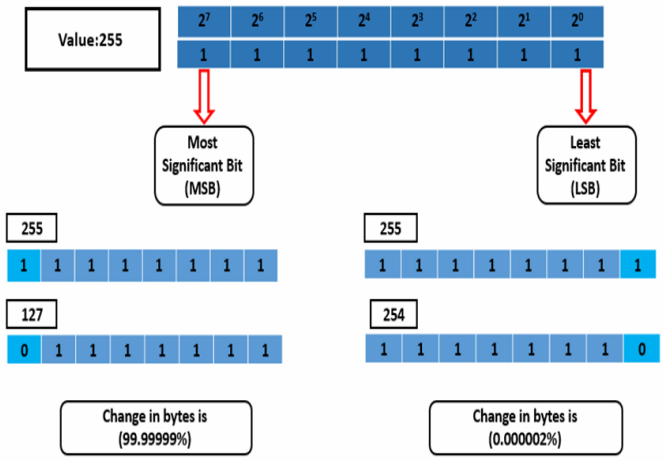


Fig. 10. Low distortion caused by the LSB.

It is worth mentioning that hiding in the LSB is considered the first layer of protection since the attacker does not notice any distortion on the cover image.

2) Role of Encryptor element.

This element is responsible for receiving the secret data and adds the second layer of protection, which is represented by encryption. The encryption process involves two kinds of encrypting algorithms: symmetric and asymmetric. The purpose of the symmetric algorithm (3DES) is actual encryption using session key (S_key). The purpose of the asymmetric algorithm (RSA) is exchanging the session key in a safe way depending on both the private and public keys of both the sender and receiver. Figure 11 shows the mechanism of exchanging the session key between the sender and receiver in a safe way.

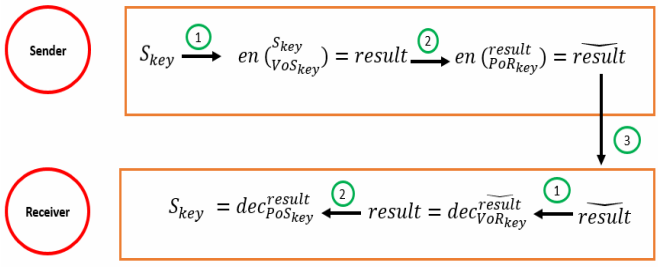


Fig. 11. Mechanism of exchanging the session key.

As shown in Figure 11, the session key is first encrypted using the private key of the sender, and this generates ($result$). Then the $result$ is encrypted using the public key of the receiver, which generates ($\widetilde{result}$). Finally, $\widetilde{result}$ is sent to the receiver. On the receiver side, the following steps are performed to get the session key:

1. Receiving the $\widetilde{result}$.
2. Decrypting $\widetilde{result}$ using the private key of the receiver. This generates the $result$. Since the private key of the receiver is used for decryption, the confidentiality security requirement is ensured.
3. The $result$ is decrypted using the public key of the sender. This generates the session key. Since the public key of the sender is used for decryption, the authentication security requirement is achieved.

After the safe exchange of the session key between the sender and receiver, the encryption process is performed using the 3DES encryption algorithm. Figure 12 illustrates the result of the encryption process.

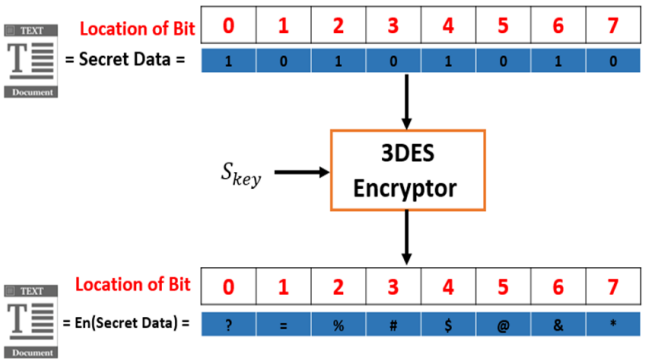


Fig. 12. Result of the encryption process.

3) Role of randomizer element.

This element is responsible for performing randomization, which represents the third layer of protection. Randomization is a process that changes the places of the cells (bits) of the encrypted secret data. Figure 13 illustrates the randomization process.

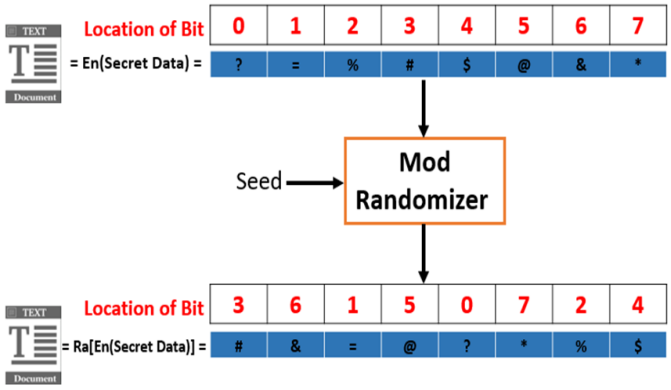


Fig. 13. Key idea behind the randomization process.

Mathematically, the randomization process depends on a mod function that can be used directly by a programming language. This function produces the new location where the encrypted secret bit from the data will be stored. Randomization requires a seed, which is a real number to be used after obtaining the digits. To make randomization flexible in terms of variety, the seed is represented by a variable.

It is worth mentioning that the safe exchange of the seed of the randomization process is achieved by the exact scenario used for exchanging the session key of the encryption algorithm.

4) Role of hider element.

This element is responsible for the actual hiding process. It takes both the randomized encrypted secret data and the LSB as inputs. The output is the stego object. The mechanism of hiding mainly depends on a replacement tactic. In other words, the hider defines the locations of the LSB. Then, it removes the values of the bits. Next, it reads the randomized encrypted secret data. Finally, it puts them in the LSB. Figure 14 shows a flow chart of the hiding process.

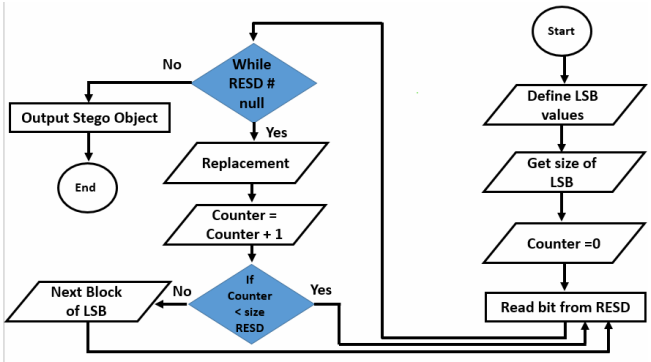


Fig. 14. Flow chart of the hiding process.

At this point, the manipulation done on the sender side finishes. The collaboration among the finder, Encryptor, randomizer, and hider components forms a triple layer of protection. Figure 15 illustrates the overall tasks of the three components.

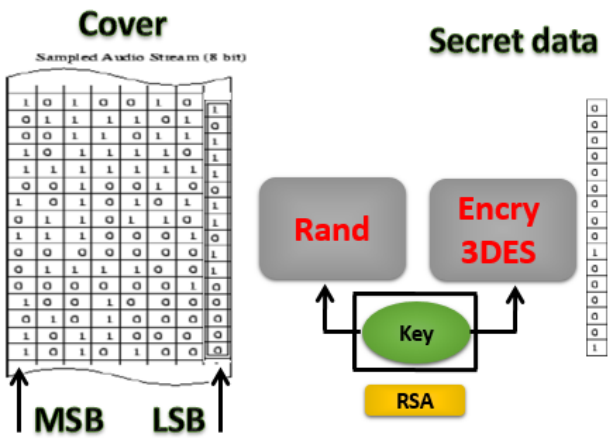


Fig. 15. Three layers of protection.

Algorithm 1 summarizes the pseudo code of the proposed hiding system.

Algorithm 1: Three layers of protection

Input: CO (cover object), SD (secret data)
Output: $Stego\ Object$
Begin
1: read (CO);
2: $LSB = Finder\ (CO)$;
3: $Blocks_{LSB} = Divide\ (LSB)$;
4: read (SD);
5: $EnSD = Encryptor\ (SD)$;
6: $REnSD = Randomizer\ (EnSD)$;
7: **while** $Blocks_{LSB} <> null$ **do**
8: **begin while**
9: read $(REnSD)$;
10: $Stego\ Object = Hider\ (REnSD, Blocks_{LSB})$;
11: **end while**
12: return $(Stego\ Object)$;
End

5) Role of extractor element.

This element is responsible for extracting the hidden data from the LSB of the stego image. Therefore, it manipulates the stego image as an input and generates the randomized encrypted secret data as an output. The mechanism used in the extracting process mainly depends on two operations: reading the data from the LSB of the stego object and storing the read data into a buffer. Figure 16 shows the flow chart of the task performed by the extractor element.

6) Role of assembler element.

This element is responsible for reassembling the randomized encrypted data correctly. This means that the assembler takes the buffer generated from the extractor element as an input, and then it produced an encrypted secret data ordered as they encrypted. Figure 17 illustrates the task of the assembler element.

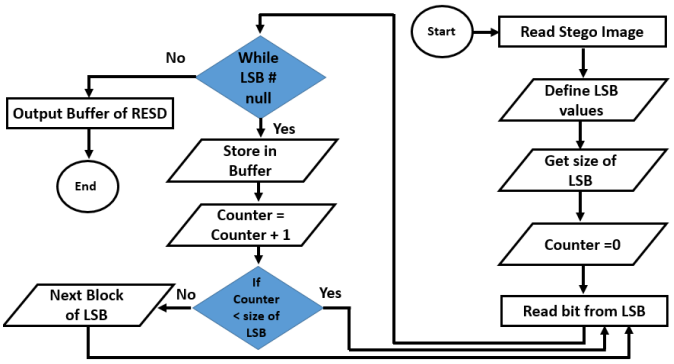


Fig. 16. Flow chart of the extracting process.

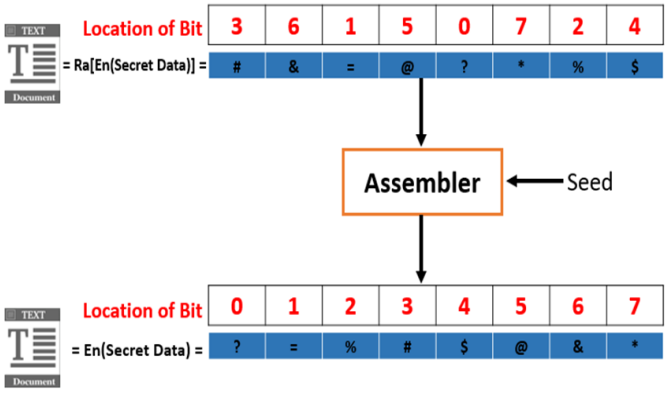


Fig. 17. Reassembling process.

7) Role of Decryptor element.

This element is responsible for decrypting the assembled encrypted data. This means that the Decryptor takes the output of the assembler as an input, and then it produces the original secret data. The session key is exchanged safely and used for the decryption process. Figure 18 illustrates the task of the Decryptor element.

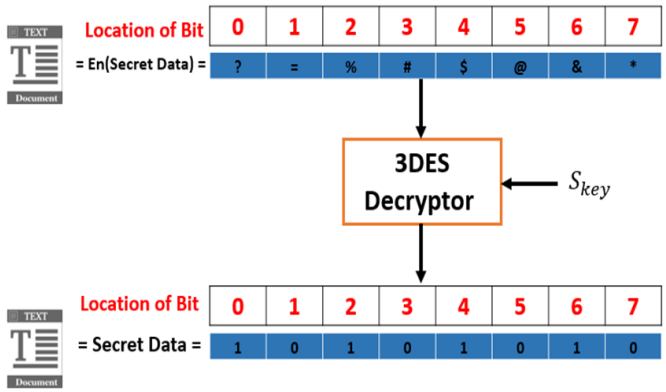
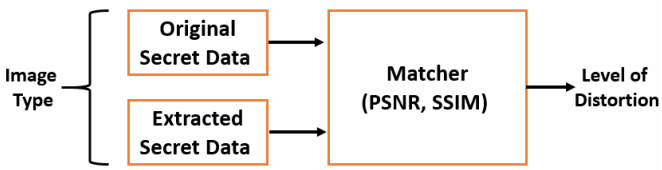


Fig. 18. Decryption process.

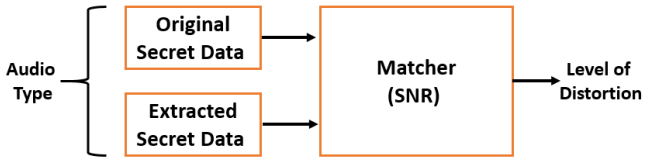
8) Role of matcher element.

This element is responsible for conducting the matching process. The matching process is performed between the original secret data (input at the sender side) and the extracted secret data (output at the receiver side). The main mission of

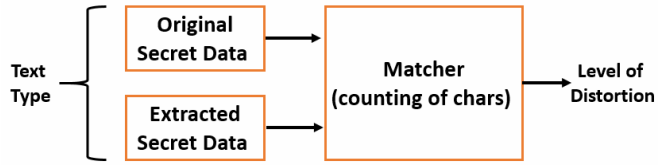
the matching process is to calculate the level of distortion that is caused by the hiding process. Since there are three types of secret data that can be embedded within the cover object, there are three scenarios of the matching process, as shown in Figure 19.



(a): Type of secret data is image.



(b): Type of secret data is audio.



(c): Type of secret data is text.

Fig. 19. Matching process for each type of secret data.

In addition, the matching process is also conducted between the cover object and the stego object. Figure 20 illustrates the scenario of the matching process.

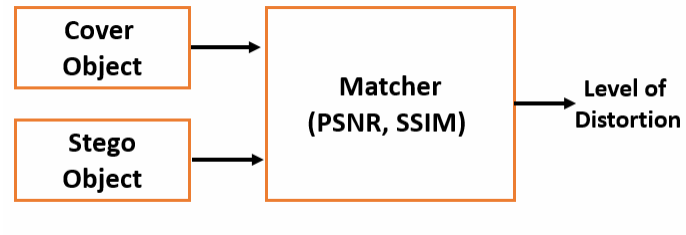


Fig. 20. Matching process between cover object and stego object.

As shown in Figure 20, the PSNR and Structural Similarity (SSIM) metrics are utilized in the process of matching.

The PSNR metric focuses on the distortion caused to the cover object by the hiding process. If the PSNR has a high value, this means that the distortion of the cover object is low. Mathematically, the PSNR is defined as:

$$\text{PSNR} = 10 \times \log_{10} \frac{255^2}{\text{MSE}\left(img_{object}^{cover}.img_{object}^{stego}\right)} \quad (2)$$

where MSE is given by:

$$MSE = \frac{1}{a \times b} \sum_{b=1}^{a} \sum_{a=1}^{b} \left[img_{object}^{cover} - img_{object}^{stego}\right]^2 \quad (3)$$

where a and b denote the size of the image.

The SSIM metric is used to measure the variation of structural information between the cover object and the stego object. Mathematically, it is defined as:

$$\text{SSIM}\left(img_{object}^{cover}.img_{object}^{stego}\right) = \left[\text{lum}\left(img_{object}^{cover}.img_{object}^{stego}\right)\right]^{\alpha} \times \left[\text{con}\left(img_{object}^{cover}.img_{object}^{stego}\right)\right]^{\beta} \times \left[\text{str}\left(img_{object}^{cover}.img_{object}^{stego}\right)\right]^{\vartheta} \quad (4)$$

where $(\alpha, \beta, \vartheta > 0)$ are parameters used to control the luminance, contrast, and structural elements, respectively.

According to the value of SSIM, which falls within the range $(SSIM \in [1.0])$. The highest value is one, indicating that the quality of image is perfect (no distortion), and vice versa.

The SNR is the ratio between the desired information, or the power of a signal, and the undesired signal, or the power of the background noise. SNR is defined as:

$$SNR = 10 \times log_{10} \times \frac{\sum_n (x)^2 \times (n)}{\sum_n [x(n) - y(n)]^2} \quad (5)$$

D. Security Analysis

This section discusses the trials of the attacker to obtain the secret data that is embedded within the cover object. Since there are three layers of protection, the attacker tries to make a gap in each layer to attack the secret data, as shown in Figure 21.

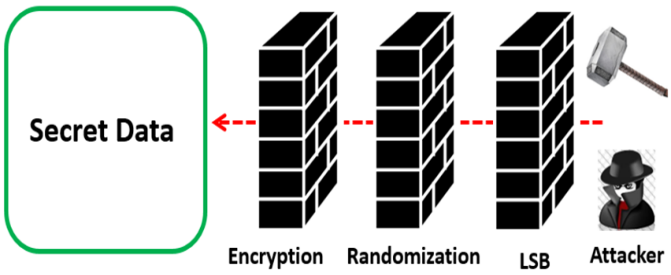


Fig. 21. Trials of attacker to overcome the security layers.

Since the secret data is embedded within the LSB, and there are no seen differences between the cover object and the stego object, the secret embedded data is safe. However, if the attacker is sceptical, the first step performed on their side will be obtaining the content of the LSB from the stego object. The attacker gains nothing because the content of the LSB is randomized and encrypted. The attacker moves to the second step, which is trying to re-randomize the content of the LSB (i.e., reordering the bits) if the attacker knows the seed of the randomization process. The attacker gains nothing because the ordered content of the LSB is encrypted. The attacker moves to the third step, which is trying to decrypt the ordered content of the LSB. The attacker gains nothing because the decryption process requires the decryption key (session key). Since the session key is exchanged safely between the sender and receiver, the attacker cannot obtain the session key. As a result, even if the attacker is sceptical, has the ability of re-randomizing the content of the LSB, and is an expert in decryption, the embedded secret data is safe.

IV. RESULTS AND DISCUSSIONS

This section is structured so that first the setup of the proposed system is provided, followed by the metrics used for evaluation. Finally, the actual results with discussions are provided.

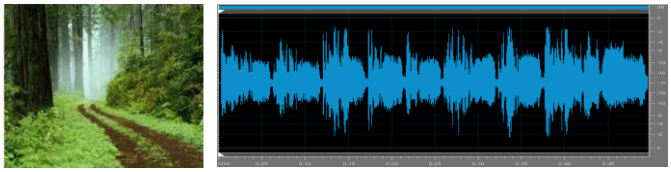
A. Setup

The proposed system was implemented using Python programming language. A machine with specifications summarized in Table III was used for applying the system.

TABLE III. SPECIFICATIONS

Item	Details (value)
Operating system	Microsoft Windows 10 Home
System type	x64-based PC
System model	HP Laptop 15-bs0xx
Processor	Intel(R) Core(TM) i5-7200U CPU @ 2.50 GHz
RAM	4 GB
Display chip type	Intel(R) HD Graphics Family

The system was set by a cover image and cover audio (shown as a signal of spectrum) seen in Figure 22.



(a) Image cover. (b) Audio cover.

Fig. 22. Covers used.

B. Metrics Used

In addition to the metrics used by the matcher component, a histogram was used as a visual metric to evaluate images. In image processing, histogram is a term utilized to represent a given image by the number of colours represented by bars. The difference in the histogram reflected a visual distortion after the hiding process. The second metric was the retrieval bit error rate ($RBER$), which represents the error while retrieving the hidden bits from the stego object during extraction process. It is given by:

$$RBER = \frac{N_{sb}^{e}}{N_{sb}^{r}} \times 100 \quad (6)$$

where N_{sb}^{e} denotes the number of secret bits that are embedded, and N_{sb}^{r} refers the number of secret bits that are successfully retrieved.

The third metric was the payload capacity ($PaCa$). It is defined as the ratio between the size of the stego image and the size of the hidden secret data. Z_{stego} and $Z_{hidden\ data}$ denote the size of stego image and hidden data, respectively. Then, the payload capacity is defined as:

$$PaCa = \frac{Z_{stego}}{Z_{hidden\ data}} \times 100 \quad (7)$$

It is worth mentioning that a higher percentage of payload capacity means a better steganography system.

C. Results

The results of two main kinds of experiments are presented. The first kind was related to testing the proposed system only, without applying any threats, and then giving the corresponding recommendations. The second kind of experiments was related to testing the proposed system under threats and also in comparison to other systems.

1) Testing the proposed system without threats.

In this context, we tested the proposed system without any threats, following the evaluation strategy illustrated in Figure 23.

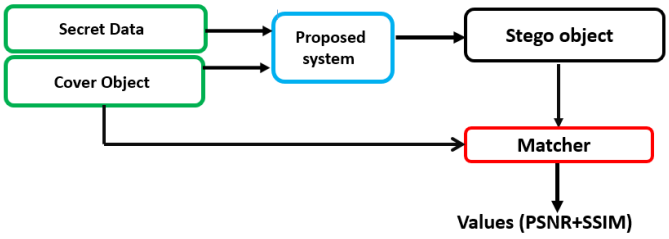


Fig. 23. Strategy of evaluation without any threat.

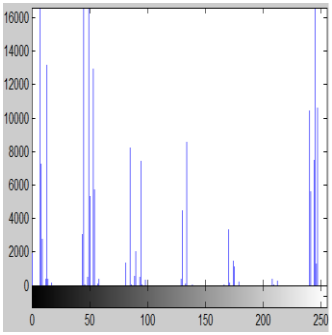
Table IV summarizes the results.

TABLE IV. VALUES OF PSNR (IN DB) AND SSIM WITHOUT ANY THREAT.

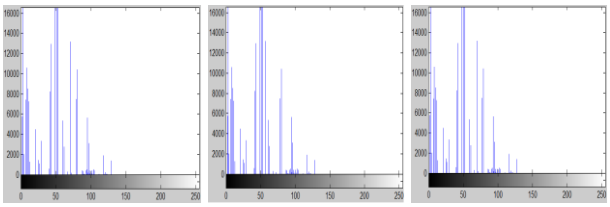
Type of secret data	Metrics	
	PSNR	*SSIM*
Text	53.3150	0.9992
Image	52.1711	0.9899
Audio	51.4018	0.9701

As shown in Table IV, the value of the PSNR decreased according to the type of the embedded secret data. This reflects a gradual increase in the level of distortion caused by the hiding process. Since the amount of secret data included in an audio file was more when compared to the text or image files, the amount of distortion increased. SSIM metric showed high values, and at the same time, it decreased according to the type of the secret data. Since SSIM can be seen as opposite to the PSNR in terms of function, the values of the PSNR supported the values of the SSIM.

To represent the level of distortion visually, histograms of both the cover and the stego object after hiding text, image, and audio files are shown in Figure 24.



(a) Histogram of cover image



(b) After hiding text (c) After hiding image (d) After hiding audio

Fig. 24. Visual evaluation of distortion levels by histograms.

The visual histograms shown in Figure 24 reflect a clear strength related to the proposed system, which is that it was perfect when it comes to hiding text files. Therefore, it is recommended to use the proposed system when dealing with secret data of text type. This strength was evaluated by hiding text files of gradually increasing size. Table V shows the values of PSNR and SSIM.

TABLE V. VALUES OF PSNR (IN DB) AND SSIM AFTER HIDING DIFFERENT TEXT FILES OF GRADUALLY INCREASING SIZES.

Type of secret data	Size	Metrics	
		PSNR	SSIM
Text 1	12 KB	53.3150	0.9992
Text 2	2 × 12 KB	53.0091	0.9989
Text 3	2 × 2 × 12 KB	52.8734	0.9973

Table V supports the recommendation provided about hiding text. Duplicating the size of the hidden text file lead to increasing values of SSIM and slightly decreasing values of PSNR.

Relying on the *RBER* metric, we measured the retrieval of error rate after hiding three types of secret data, where the size was increasing with a step of 50 KB. Figure 25 shows the results.

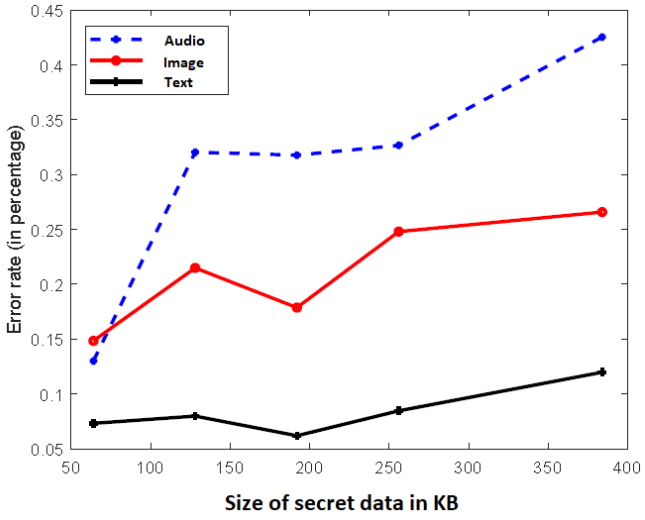


Fig. 25. Values of *RBER* versus size of secret data.

Figure 25 shows that hiding a text file as secret data corresponded with the lowest error rate. This was because the retrieved text file was perfect, except for some chars located at the end of the file when the size increased dramatically. Compared to the image file as a secret data, hiding an audio file gave the highest error rate in the retrieving or extracting process, except at the binging. At the beginning, hiding audio provided a better error rate since the file audio used as a secret data had a simple silent part when starting.

As for the *PaCa* metric, Figure 26 shows the average of the payload capacity that was calculated from the error rate (i.e., one minus the average of the error rates illustrated in Figure 25).

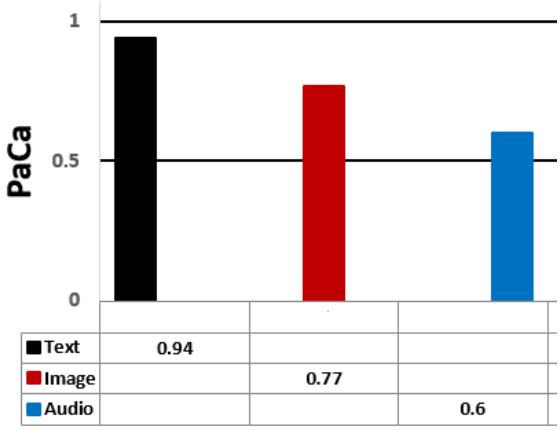
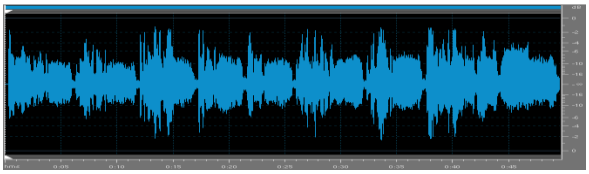


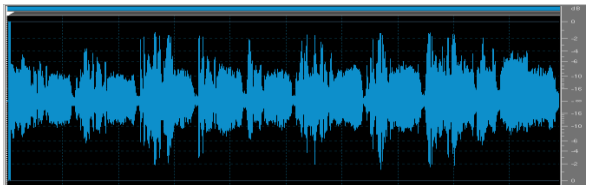
Fig. 26. Average *PaCa* metric values.

Figure 26 provides results that support those shown in Figure 25 with a reverse relationship between the amount of error rate of retrieving and the capacity of the payload (size of the hidden data).

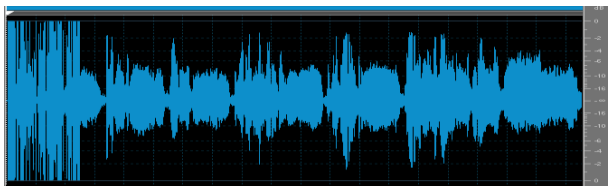
When using an audio file as a cover object, we used the spectrum form of the wave to represent the differences between the cover audio file and the stego object after hiding text, image, and audio files. Figure 27 illustrates the results.



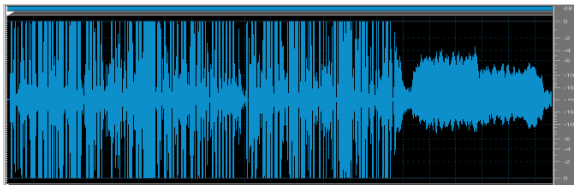
(a) Cover object



(b) Stego object after hiding text file



(c) Stego object after hiding image file



(d) Stego object after hiding audio file

Fig. 27. Spectrum form after hiding within audio file.

As shown in Figure 27, the amount of distortion caused by the hiding process increased dramatically when hiding image and audio files. When hiding text file, the amount of distortion was minimal and could not be recognized by the human ear. The reason behind this is related to the sensitivity of the human ear when compared to the eye.

2) Testing the proposed system under threats.

In this context, we tested the proposed system under the impact of threats and also compared with other systems, following the evaluation strategy illustrated in Figure 28.

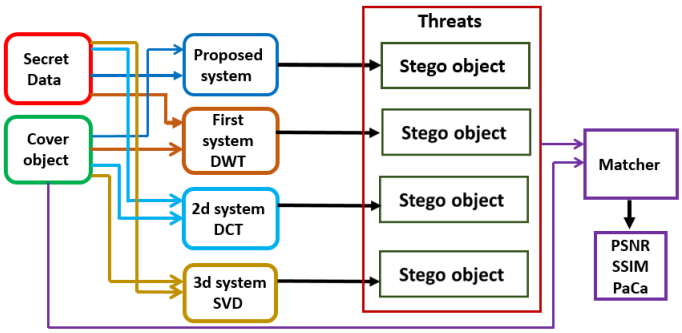


Fig. 28. Strategy of evaluation under threats.

Table VI summarizes the results.

TABLE VI. VALUES OF PSNR (IN DB) AND SSIM UNDER THREATS.

Type of attack	Attack	System	Hiding text		Hiding image		Hiding audio		Capacity
			PSNR	*SSIM*	*PSNR*	*SSIM*	*PSNR*	*SSIM*	*PaCa*
Geometric	Rotation	Proposed system	52.3440	0.9872	51.1331	0.9811	50.33	0.9645	0.93
		DCT-based system [22]	51.7897	0.9755	50.098	0.9611	49.1698	0.9544	0.9
		DWT-based system [23]	51.99	0.9799	50.455	0.9645	49.3899	0.9587	0.88
		SVD-based system [24]	51.44	0.9777	50.111	0.9666	49.1771	0.95493	0.89
	Bilinear	Proposed system	52.221	0.98	51.0221	0.9745	50.1167	0.96149	0.92
		DCT-based system [22]	51. 582	0.973	50. 561	0.9655	49.183	0.9542	0.89
		DWT-based system [23]	51.2616	0.9723	50.3342	0.9666	49.5543	0.9569	0.86
		SVD-based system [24]	51.1817	0.9756	50.1602	0.9691	49.9582	0.95403	0.87
Non-Geometric	Gaussian noise	Proposed system	49.456	0.88	47.555	0.86	46.342	0.80	0.905
		DCT-based system [22]	51.5505	0.973	50.6290	0.9655	49.9114	0.9542	0.8803
		DWT-based system [23]	51.6677	0.9723	50.5633	0.9666	49.6394	0.9569	0.85631
		SVD-based system [24]	51.6658	0.9756	50.3172	0.9691	49.0759	0.95403	0.86788

The results documented in Table 6 show that the proposed steganography system was negatively affected by attacks. However, it had higher resistance against both the rotation and bilinear attacks. That was because changing the dimensions of the stego image does not affect the colour space of the pixels that form the image, and consequently the LSB will not affected largely. Both the DCT- and SVD-based systems' results were near to each other's. This can be explained by the similar mechanism used in both transforms for the hiding process. The DWT-based system provided better results when compared to the DCT- and SVD-based systems. The reason for this was related to the multiresolution property of the DWT transform. As for the payload capacity, the proposed system performed the best. That was because the location of hiding, defined by the LSB of each colour of each pixel, was relatively large when compared to the coefficients of the DCT, DWT, and SVD transforms. Moreover, applied attacks did not affect the capacity widely in all systems. That was because the location of hiding was independent from the actual hiding process and its consequences.

We tested the proposed system under the impact of threats and in comparison with other systems when hiding text secret data (where the text file consisted of 200 chars), following the evaluation strategy illustrated in Figure 29.

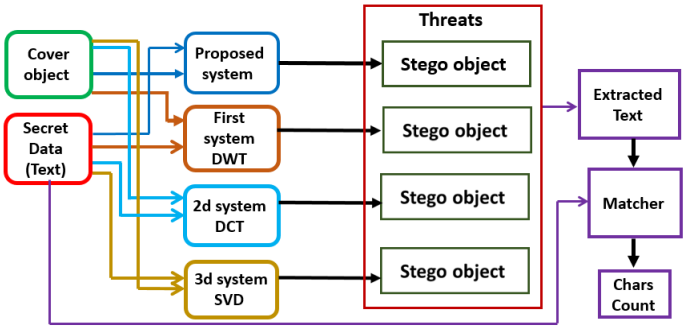


Fig. 29. Strategy of evaluation under threats when hiding text secret data.

Table VII summarizes the results.

TABLE VII. VALUES OF CHAR COUNTS UNDER THREATS.

Type of attack	Attack	System	Char counts	*RBER*
Geometric	Rotation	Proposed system	200	0
		DCT-based system [22]	198	0.01
		DWT-based system [23]	199	0.005
		SVD-based system [24]	198	0.01
	Bilinear	Proposed system	200	0
		DCT-based system [22]	198	0.01
		DWT-based system [23]	199	0.005
		SVD-based system [24]	198	0.01
Non-Geometric	Gaussian noise	Proposed system	199	0.005
		DCT-based system [22]	198	0.01
		DWT-based system [23]	199	0.005
		SVD-based system [24]	198	0.01

Table VII shows that the proposed system was resistant to rotation and bilinear attacks, while the Gaussian noise cut one char from the retrieved file text. This was due to the external points (noise) that can be seen as abnormal parts to be added to the stego object. However, the proposed system was still ranked at the top (on average) when compared to the other systems. As for the retrieval bit error rate, all systems performed well. The proposed system achieved perfect value under rotation and bilinear attacks. However, it degraded slightly under Gaussian noise attack.

We tested the proposed system under impact of threats and in comparison with other systems when hiding audio secret data, following the evaluation strategy illustrated in Figure 30.

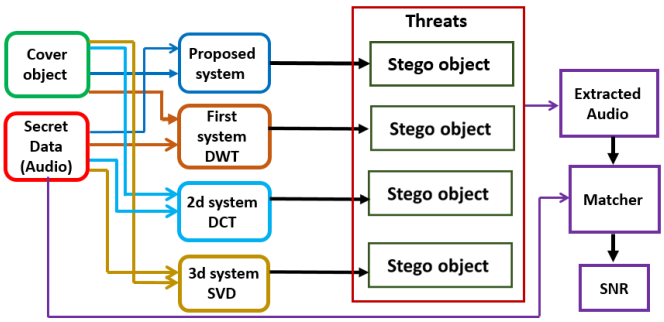


Fig. 30. Strategy of evaluation under threats when hiding audio secret data.

Table VIII summarizes the results.

TABLE VIII. VALUES OF SNR UNDER THREATS.

Type of attack	Attack	System	SNR in dB	*RBER*
Geometric	Rotation	Proposed system	38.3	0
		DCT-based system [22]	32.4	0.02
		DWT-based system [23]	36.3	0.03
		SVD-based System [24]	29	0.035
	Bilienar	Proposed system	37.5	0
		DCT-based system [22]	31.9	0.026
		DWT-based system [23]	35.4	0.038
		SVD-based System [24]	28	0.043
Non-Geometric	Gaussian noise	Proposed system	30.8	0.055
		DCT-based system [22]	30.9	0.03
		DWT-based system [23]	34.6	0.05
		SVD-based System [24]	29.3	0.044

When hiding audio file in the systems involved in the comparison, Table 8 shows that the highest values of the SNR were achieved by the proposed steganography system under geometric attacks. However, the negative impact of the bilinear attack was more when compared to the rotation attack. When applying Gaussian noise attack, the values of the SNR in the four systems degraded. However, the DWT-based system performed the best, and the performances of the DCT and the proposed system were similar, while the SVD system performed the worst. That is because the hiding process in the DCT-, DWT-, and SVD-based systems was conducted in the frequency domain, while the proposed system used spatial technique for the hiding process. As for the retrieved bit error rate, all systems showed lower values when compared to the case where no attacks were applied. The proposed system performed the best under rotation and bilinear attacks when compared to the other systems. That was because these two types of attacks do not affect the hiding location, which is the LSB. Gaussian noise directly affects the LSB. Therefore, the proposed system provided poor results. The other systems had higher resistance against Gaussian attack since the noise signals convert in the frequency domain.

We tested the proposed system under the impact of threats and in comparison with other systems when hiding image secret data, following the evaluation strategy illustrated in Figure 31.

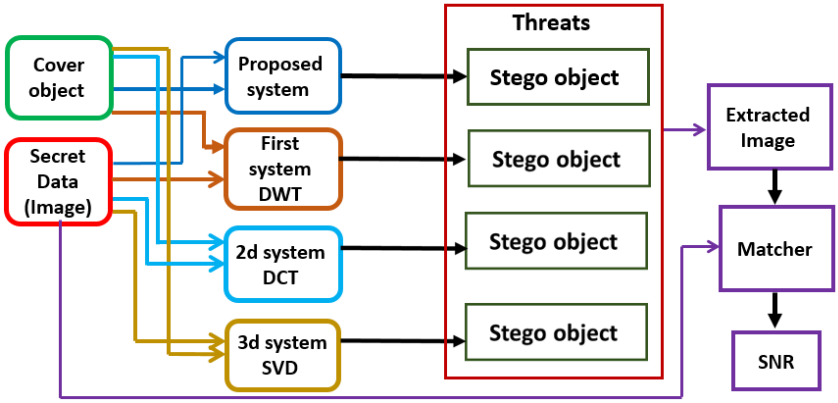


Fig. 31. Strategy of evaluation under threats when hiding image secret data.

Table IX summarizes the results

TABLE IX. VALUES OF PSNR (IN DB) AND SSIM UNDER THREATS.

Type of attack	Attack	System	PSNR	SSIM	*RBER*
Geometric	Rotation	Proposed system	48.175	0.9825	0
		DCT-based system [22]	40.57	0.945	0.022
		DWT-based system [23]	47.08	0.975	0.034
		SVD-based system [24]	42.87	0.9625	0.034
	Bilinear	Proposed system	47.333	0.97531	0
		DCT-based system [22]	40.77	0.931	0.0272
		DWT-based system [23]	47.01	0.939	0.03677
		SVD-based system [24]	42.11	0.95	0.0411
Non-Geometric	Gaussian noise	Proposed system	43.359	0.95321	0.052
		DCT-based system [22]	40.23	0.9	0.0311
		DWT-based system [23]	46	0.91	0.05109
		SVD-based system [24]	41	0.93	0.0465

Table IX shows that under threats of rotation and bilinear attacks, the proposed system's ability for extracting the hidden secret images was highly similar compared to the other systems. However, the value of the SSIM decreased after applying Gaussian noise attack, and this was accompanied by an increasing level of distortion caused to the extracted images (i.e., decreasing values of PSNR). The DCT- and SVD-based systems' values were close to each other's, while the DWT-based system provided the best values under Gaussian attack. As for the retrieved bit error rate, the values were very similar to those documented when hiding audio file. The behaviour of the systems was almost the same in this experiment, where the proposed system outperformed the DCT-, DWT-, and SVD-based systems under rotation and bilinear attacks.

V. CONCLUSION

In this age, information of different types is exchanged on a daily basis. Security is essential when exchanging information since the abilities of attackers increase every day. Steganography is considered the best option for hiding the communication among network users. However, ensuring perfect matching between the cover object and the generated stego object as well as high resistance against attacks are top requirements. In this work, we proposed a steganography-based system that had the ability to hide different types of data (text, audio, and images). The system was managed by eight components, including finder, Encryptor, randomizer, hider, extractor, assembler, Decryptor, and matcher. The system used LSB as a hiding place in the spatial domain, which represented the first layer of protection against attackers. The LSB was supported by two additional layers of security – encryption and randomization. Therefore, even if the attacker was sceptical, they would have to decrypt and reassemble the secret hidden data to obtain the original one. The proposed system was compared to three systems that were built based on DCT, DWT, and SVD transforms. The results of the experiments showed that the proposed system was ranked on the top when it comes to level of distortion (PSNR), similarity between the cover image and the stego one (SSIM), resistance against rotation and bilinear attacks, payload capacity, and retrieved bit error rate.

One limitation was that the system had low resistance against non-geometric attacks (Gaussian noise) when compared to other systems. In addition, responding time was not considered in this work.

In future work, we intend to build the system using parallel platforms to test and enhance the responding time. In addition, the LSB technique used in this work will be supported with a new layer for defence against non-geometric attacks.

VI. REFERENCES

[1] [1] Yange, Terungwa Simon, and Moses A. Agana. "DEVELOPMENT OF A DATA SECURITY MODEL USING STEGANOGRAPHY." Compusoft 6.6 (2017): 2355.

[2] [2] Dhawan, Sachin, and Rashmi Gupta. "Analysis of various data security techniques of steganography: A survey." Information Security Journal: A Global Perspective (2020): 1-25.

[3] [3] Applications of Steganography website. [Online] available: Applications of Steganography (datahide.org). (Accessed 28-Jan-2021)

[4] [4] Rajendran, Sindhu, et al. "An Update on Medical Data Steganography and Encryption." Recent Trends in Image and Signal Processing in Computer Vision. Springer, Singapore, 2020. 181-199.

[5] [5] Oleshchenko, Vladimir, and Vladimir Pevnev. "Development of digital steganography techniques for copyright protection, based on the watermark." Сучасні інформаційні системи 1,№ 1 (2017): 57-60.

[6] [6] Luo, Yuanjing, et al. "Coverless image steganography based on multi-object recognition." IEEE Transactions on Circuits and Systems for Video Technology (2020).

[7] [7] Liu, Qiang, et al. "Coverless image steganography based on DenseNet feature mapping." EURASIP Journal on Image and Video Processing 2020.1 (2020): 1-18.

[8] [8] Alexan, Wassim, Mazen El Beheiry, and Omar Gamal–Eldin. "A comparative study among different mathematical sequences in 3d image steganography." International Journal of Computing and Digital Systems 9.4 (2020): 545-552.

[9] [9] Idakwo, M. A., et al. "An extensive survey of digital image steganography: state of the art." ATBU Journal of Science, Technology and Education 8.2 (2020): 40-54.

[10] [10] Taleby Ahvanooey, M., Li, Q., Shim, H. J., & Huang, Y. (2018). A comparative analysis of information hiding techniques for copyright protection of text documents. Security and Communication Networks, 2018

[11] [11] Xiang, L., Yang, S., Liu, Y., Li, Q., & Zhu, C. (2020). Novel linguistic steganography based on character-level text generation. Mathematics, 8(9), 1558

[12] [12] Desoky, A. (2009). Listega: list-based steganography methodology. International Journal of Information Security, 8(4), 247-261

[13] [13] Shiu, H. J., Lin, B. S., Lin, B. S., Huang, P. Y., Huang, C. H., & Lei, C. L. (2017, September). Data hiding on social media communications using text steganography. In International Conference on Risks and Security of Internet and Systems (pp. 217-224).

[14] [14] Alanazi, N., Khan, E., & Gutub, A. (2021). Efficient security and capacity techniques for Arabic text steganography via engaging Unicode standard encoding. Multimedia Tools and Applications, 80(1), 1403-1431.

[15] [15] Chauhan, S., Kumar, J., & Doegar, A. (2017, February). Multiple layer text security using variable block size cryptography and image steganography. In 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT) (pp. 1-7). IEEE

[16] [16] Begum, M. B., & Venkataramani, Y. (2012). LSB based audio steganography based on text compression. Procedia Engineering, 30, 703-710.

[17] [17] Wang, Y., Yi, X., & Zhao, X. (2020). MP3 steganalysis based on joint point-wise and block-wise correlations. Information Sciences, 512, 1118-1133.

[18] [18] Wu, J., Chen, B., Luo, W., & Fang, Y. (2020). Audio steganography based on iterative adversarial attacks against convolutional neural networks. IEEE Transactions on Information Forensics and Security, 15, 2282-2294

[19] [19] gum, M. B., & Venkataramani, Y. (2012). LSB based audio steganography based on text compression. Procedia Engineering, 30, 703-710

[20] [20] in, G., Liu, Y., Yang, T., & Cao, Y. (2018). An adaptive audio steganography for covert wireless communication. Security and Communication Networks, 2018

[21] [21] Bharti, S. S., Gupta, M., & Agarwal, S. (2019). A novel approach for audio steganography by processing of amplitudes and signs of secret audio separately. Multimedia Tools and Applications, 78(16), 23179-23201.

[22] [22] Rachmawanto, Eko Hari, and Christy Atika Sari. "Secure image steganography algorithm based on dct with otp encryption." Journal of Applied Intelligent System 2.1 (2017): 1-11.

[23] [23] Kumar, Vijay, and Dinesh Kumar. "A modified DWT-based image steganography technique." Multimedia Tools and Applications 77.11 (2018): 13279-13308.

[24] [24] Arunkumar, S., et al. "SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images." Measurement 139 (2019): 426-437.

[25] [25] Zhang, Yue, et al. "Zernike moment-based spatial image steganography resisting scaling attack and statistic detection." IEEE Access 7 (2019): 24282-24289.

[26] [26] Hosam, Osama. "Attacking image watermarking and steganography-a survey." International Journal of Information Technology and Computer Science 11.3 (2019): 23-37.

[27] [27] Yousif, Adel Jalal. "Image Steganography Based on Wavelet Transform and Color Space Approach." Diyala Journal of Engineering Sciences 13.3 (2020): 23-34.