A systematic overview of secure image steganography

Bakhan Tofiq Ahmed
Department of Computer Science, College of Science, University of Garmian, Kalar, Sulaimani, Kurdistan Region, Iraq
Department of Information Technology, Technical College of Informatics, Sulaimani Polytechnic University, Sulaimani, Kurdistan Region, Iraq

Article Info

Article history:

Received Jul 28, 2020
Revised Feb 28, 2021
Accepted Mar 6, 2021

Keywords:

Discrete cosine transform
Least significant bit
Steganography
Stego-image
Stego-key

ABSTRACT

Information is a vital thing that needs to be secured and well protected during transmission between two or more parties over the internet. This can be achieved by steganography technology. Steganography is the concealing science in which the information is concealed inside other information in a way that the concealed information cannot be detectable by the human eye. Many ways are available to hide data inside a cover media for example text, image, and audio steganography, but image steganography is the most utilized technique among the others. Secure image steganography has a high-security level than traditional technique by combining steganography with cryptography due to encrypting secret information by cryptography algorithm before embedding it into the cover media by steganography algorithm. In this paper, a systematic review has been presented about secure image steganography and its renowned types. Many researchers proposed secure image steganography by using various cryptography and steganography algorithms which have been reviewed. The least significant bit 'LSB' was the renowned steganography algorithm which has been used by researchers due to its simplicity, while various cryptography algorithms like advanced encryption standard (AES) and blowfish have been used to propose secure image steganography in the reviewed papers. The comparison among the reviewed papers indicated that the LSB with hash-RSA gave a greater peak signal-noise ratio 'PSNR' value than the others which was 74.0189 dB.

Corresponding Author:

Bakhan Tofiq Ahmed
Department of Information Technology
Technical College of Informatics
Sulaimani Polytechnic University
Sulaimani, Kurdistan Region, Iraq
Email: bakhan.tofiq.a@spu.edu.iq

1. INTRODUCTION

The fast technology development and automated life elevated the prerequisite for an additional security level. All over the globe, security is a growing requisite because a lack of security can result in great damage [1], [2]. The internet and technology are enhanced rapidly day by day. Every day a huge amount of data and information are moved to the internet so providing security for sensitive information is extremely important. Secured communication is an important issue for a long time. Two main techniques are used for providing security, namely, Cryptography and Steganography. A technique that has been created for securing the data is known as Cryptography and several various techniques have been improved to encrypt or encode and decrypt or decode data to provide safety for the information in terms of content not the existence of data that is not enough. Another technique that has been created for protecting and hiding the message's existence is called Steganography. It is the art, science, and technique utilized for hiding the existence of secret information. Steganography and Cryptography are two different techniques that provide security, in cryptography the contents of secret data are kept whereas in steganography the existence of secret information is kept. As a result, steganography is more secure than cryptography [3]. Steganography is a Greek word that means ‘secure writing’. A technique which is used to hide information inside information is known as Steganography which was practiced during the prehistoric time [4]. The major aim of steganography is to conceal the information inside information in an approach that is unnoticeable by the eyes of humans [5]. The information is text, image, audio, or video. Steganography has five types like text, image, audio, video, and protocol [6].

The types rely on the medium that is used as a carrier. First, a technique that is utilized to hide a secret message inside a text message is known as text steganography. It can be obtained by changing the format of the text. This type is not used often because the amount of redundant data is extremely small. Second, image steganography means that secret information is hidden inside an image medium. In this type, a digital image is used to cover a secret message by using an algorithm with the secret key. It works with a different domain such as the Image domain, Transform domain. Third, when audio is used as a carrier then it is called audio steganography. LSB coding, Parity coding, Phase coding, Spread Spectrum, and Echo Hiding are the main audio steganography methods. Fourth, a technique which hides any file types in any video file extension is called video steganography. In other words, the video is taken as a cover in video steganography [7]. Ultimately, a technique which embeds secret information within network protocols such as TCP/IP is so-called protocol steganography. The secret message is concealed in the TCP/IP packet header. Nowadays, Image Steganography is the most widely used type. In this type, the image is utilized as a carrier to conceal the secret data. Many techniques are used in image steganography, but the most common are spatial domain, Transform domain, spread spectrum, patchwork, etc [8].

The main aim of this study is to present a comprehensive survey about a proposed secure image steganography system which is based on a combination of a cryptographic algorithm with a steganographic algorithm and compare among the relevant up-to-date research papers available in this area. The other parts of this study are structured as follows: in section 2 literature review has been presented about the most related papers in this field. Image steganography and its types have been discussed in section 3. Section 4 is about image steganography in the spatial and transform domain. Evaluation criteria were drawn in section 5 and a comparison between the reviewed papers was revealed in section 6. Ultimately, the conclusion was drawn in section 7. The categories of Steganography are shown in Figure 1.

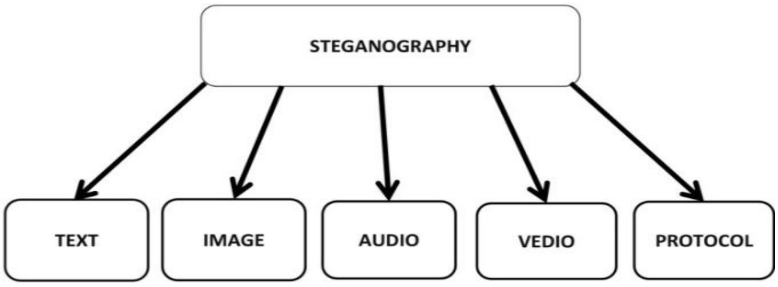

Figure 1. Steganography categories [8]

2. LITERATURE REVIEW

Many researchers worked in this field and proposed secure image steganography to provide high-level security by combining steganography and cryptography technology. Some of these up-to-date relevant researches are reviewed as enlisted as following:

According to Kumar *et al.* [9], this study presented an embedding technique by using a hash function and Rivest Shamir Adelman ‘RSA’ algorithm for encoding data to send secret information in a trustworthy way via an unsecured channel like the Internet. Then, the encoded data has been embedded by the LSB algorithm. The proposed system’s performance has been evaluated by comparing it with the traditional LSB algorithm. The experimental outcomes have shown that the proposed system was efficient because it gave a satisfying value of both mean secure error ‘MSE’ and peak signal-noise ratio ‘PSNR’ for stego images.

Sharma *et al.* [10] recommended a method by joining both cryptography and steganography technology. Blowfish algorithm has taken as cryptography and LSB as steganography technique. First, the secret message is encoded by the Blowfish algorithm. After that, the encrypted secret message is hidden by the LSB algorithm. The concatenation between these two methods gives a higher level of data security. This system is measured as a very secure system because it is tough for the intruders to recover the hidden image.

According to Verma *et al.* [11], a hybrid approach is proposed for image security. First, the image is encrypted by modified advanced encryption standard (MAES) which is based on the cryptography concept to achieve better performance than the original AES. Then, the LSB algorithm is utilized to conceal the encoded image to provide secret communication. Consequently, the communication cannot be predicted by the intruder. The experimental results are shown that the proposed hybrid approach gives higher security against various attacks and a PSNR of 59.4681dB.

Nag *et al.* [12] proposed secure image steganography by mixing LSB and Huffman coding which is a cryptographic algorithm. By the proposed technique a high-security level has been obtained. Firstly, every 8 bits of the secret image is encoded by the Huffman tree. Later, the encrypted bits are split into four slices which have 0 to 3 decimal values. The experiment results showed that attackers can't extract the secret message because mixed techniques made the proposed system very secure. The proposed technique gave PSNR values were about 31 dB.

Sugested by Singh *et al.* [13], a hash-based approach with a Canny edge detection is recommended for proposing a secure color image steganography. A steganography procedure is used for encoding. First of all, various types of color (RGB) image as a cover and text data as a secret message is taken. Edge detection is carried out by the canny method and after that the text data inserted into the cover image by using a hash function. The results are simulated by Matlab2010a. The proposed method is tested by various image type formats such as jpg, jpeg, bmp, and tiff. The results showed that the hash-based approach is a secure method to obtain secure image steganography.

Satar *et al.* [14] aimed to propose two security layers by merging steganography with cryptography. In the proposed system, the RSA and Diffie Hellman algorithm is examined. Encoding and decoding the secret information is done by RSA, while the Diffie Hellman algorithm allows users to embed the secret information in the selected pixel. As a result, both security and high image quality with a PSNR value of 71.9dB is achieved by the proposed system. Also, this model was more complicated and proved that secret data cannot be extracted by attackers.

Zhou *et al.* [15] proposed an enhanced LSB algorithm of a color image with the RSA which is mainly utilized for digital signature. In this research, the vision of the human eye and identity authentication has been incremented because it has relied on the technology of cryptography. Finally, the experiment demonstrated that the enhanced LSB is more robust than the traditional LSB method because it gave a higher security level and higher PSNR.

According to Sharma and Srivastava [16], a new mechanism has been implemented by combining cryptography and steganography. The advanced encryption standard (AES) algorithm has been utilized as cryptography to encode secret images before hiding them in the cover image and the 2-dimensional haar discrete wavelet transform (2-D HDWT) was applied on the cover image to extract its coefficient features. Then, alpha blending function used to mix cover image and secret image and stego image obtained after applying 2- dimensional haar inverse discrete wavelet transform (2-D HIDWT) on the result of alpha blending. The proposed system gave a higher imperceptibility and trustworthiness due to the combination of steganography and cryptography.

Kusuma *et al.* [17] in this study, secure image steganography was proposed by using Arnold’s cat Map (ACM) and inverted 2-bit LSB. The ACM is utilized to encode an image by the pixels’ randomization. After award, the inverted 2-bit LSB is used to embed the ACM result into a cover. In addition, by utilizing Inverted 2-bit LSB two bits in the cover image’s bit plane were replaced with secret information bits. This replacement strategy will confuse intruders when they attempt to decode the cipher images. The experimental outcome was assessed by using PSNR and entropy to compare the stego images and the cipher images’ quality. Consequently, the proposed system gave 57.8493 dB and 7.9948 of PSNR and entropy, respectively.

Tauhid *et al.* [18] in this paper, a new approach was presented by combining AES with LSB to ensure a secure transmission while the information was sent between the sender and receiver. The AES is utilized to encrypt the secret info in the spatial domain of the carrier image, while LSB is used to embed secret information in the transform domain of the same image after applying a discrete cosine transform (DCT) on the pixels of the image. An extra security layer has been added to this work by performing an XOR operation on the encoded secret information with the carrier image’s pixels. The proposed system attained a high PSNR of 62.72 by this the proposed system provided three security layers of the information and error-free decryption.

Ahmed *et al.* [19] in this study, two security layers were proposed by using double XOR operations using binary representation and LSB. Firstly, the message is encrypted by using a double XOR operation using binary representation, and then LSB hid the encoded data into the carrier image. To ensure the quality of their proposed system, renowned evaluation measures like MSE, PSNR, entropy, and histogram distribution have been calculated. The experimental outcomes showed that the proposed system preserved the security of hidden text messages and obtained a PSNR of 55.67 dB and a MSE of 0.18.

3. AN OVERVIEW OF IMAGE STEGANOGRAPHY

Image steganography is the most renowned steganography form. It means that the secret data is hidden in the image medium. In other words, when a digital image is acted as a carrier to conceal data is known as image steganography. In this form, the carrier is an image that covers secret information. The secret message can be a text message or an image that needs to be hidden inside the carrier. An image is made up of pixels. Each pixel is represented by three colors which are red, green, and blue 'RGB'. Each color comprises 8 bits (1 byte). An image can be categorized into a color, black and white, or a grayscale. A color image comprises three planes 'RGB' with pixel values ranging from 0-255, while a grayscale image comprises only one plane with pixel values ranging from 0-255 [20].

3.1. Image compression

In images, there are two main compressions algorithms as "Lossy" Compression and "Lossless" Compression. In the "lossy" form, the amount of information is reduced before transmitting it. This reduction will be done by losing some redundant information. It means that the compressed image is not exactly like the original image. Joint photographic experts group 'JPEG' is the image format that utilizes Lossy Compression. However, in "Lossless" compression the amount of information is not reduced from the target image. After the image is decompressed, all the information can be restored. However, graphical interchange format 'GIF' and bitmap file 'BMP' are image formats that utilize lossless compression [21].

3.2. Image steganography terms

The followings terms are used in image steganography [21]:

- Cover-image: It is an image (or media) that acts as a carrier for concealing secret information.
- Stego-image: The original information is embedded in the carrier image to generate a stego-image.
- Message: It is original information that needs to be concealed. The information can be (plain text, ciphertext, or image).
- Stego-key: A key that plays a vital role named stego-key. It is utilized to embed and extract the secret data from the cover and the stego images.

The two main concepts used in image steganography namely, embedding and extracting process. In the embedding process, the secret message is concealed in the cover-image with help of the stego-key, so no one can extract the information without knowing the stego-key. As a result, a stego-image is attained which is ready to pass through the next process. As shown in figure 2, in the extracting process, a stego-image with the stego-key is passed through the extraction process to attain the secret information. As the stego-key is utilized in the embedding process it is also utilized in the extracting process. So the key is shared between the sender and receiver. Encoding is completed at the sender's side to attain stego-image, whereas decoding is carried out at the receiver's side to attain secret information. Figure 2, depicts the block diagram of the Image Steganography model.

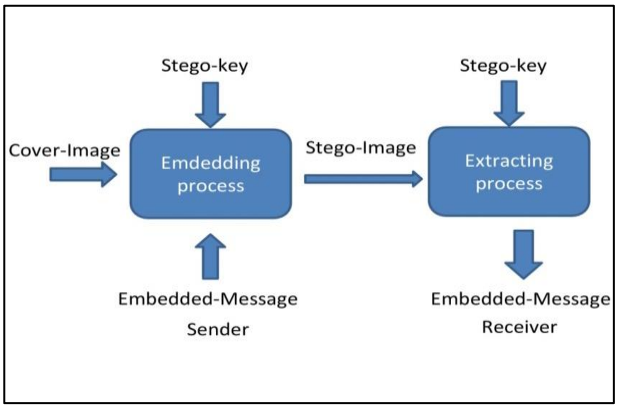

Figure 2. The image steganography's block diagram [22]

3.3. Image steganography techniques

Many techniques can be used for performing image steganography some of them are listed as the following:

Spatial or image domain
- Least significant bit ‘LSB’

Transform or frequency domain
- Discrete cosines transform ‘DCT’
- Discrete wavelets transform ‘DWT’
- Discrete fourier transform ‘DFT’

Spread spectrum.
Patchwork.
Distortion Technique.
Masking and Filtering.

3.3.1. Image or spatial domain

In this domain, the information is inserted directly into the original image pixels’ intensity. This technique relies on the format of the image that is utilized as a cover medium. For hiding the data in this technique some bits are directly changed into the pixel values bitwise of the image. There are many ways to perform embedding files in Spatial Domain but the easiest and simplest one is LSB [23].

3.3.2. Transform or frequency domain

This steganography domain is utilized to conceal a huge data amount. It offers high security, good invisibility, and no loss of secret message. In this domain, firstly the cover image is transformed. After that, the secret message is embedded in significant areas. The transform domain can be categorized into three main kinds such as DCT, DWT, and DFT. The embedding process in this domain is more complicated than embedding data in the spatial domain because the data is not hidden directly in the pixel’s intensity, but it is concealed in the pixel’s coefficient. Furthermore, it is better than the image domain because it hides the data in a medium that is less affected by cropping and compression. JPEG image format is the common file format that is used under this domain especially with DCT [23].

3.3.3. Spread spectrum

In this method, the secret data is scattered all over the cover-image so that it is tough to detect it easily by hackers. Stego-image can be produced by embedding the secret data in noise before it combines with the cover-image. As a consequence, the secret data is impossible to be visible due to that this technique is quite robust against any intruder [23].

3.3.4. Patchwork

It is also known as a statistical method that utilizes redundant pattern encoding. First, the secret data is embedded by adding redundancy and then spreads out through the cover image. The intensity of a pixel might be different in each patch. If the intensity increased in one patch, it will be decreased in the other. The changes are so small that cannot be predicted by human eyes. The main limitation of this method is that solely one bit can be embedded. However, the image can be divided into sub-image, if more bits are to be embedded. In contrast, the main benefit is that if one patch is destroyed others will safe because the secret data is not hidden only in one location, but it is concealed in different locations of the image [23].

3.3.5. Distortion technique

This technique is used to store the embedded info in the signal distortion. Secret messages can be restored if the original message is known during the decoding process. Knowledge and carefulness are required in this method because it is necessary to check the similarity between the original carrier-image and stego-image. The weakness of this technique is that if the cover image is used more than one time then the stego-image can be easily detected by intruders [24]

3.3.6. Masking and filtering

These methods are utilized to conceal the information by marking the image which is similar to the watermarking technique. The masking and filtering technique is applied to the image with 24-bit of size or grayscale type by using different applications to hide a message. In this technique, the information imparts into a more significant image area [24].

4. IMAGE STEGANOGRAPHY IN SPATIAL AND TRANSFORM DOMAIN

4.1. Image steganography in the spatial domain

It is also referred to as the Image domain. It applies a bit insertion between secret information and a carrier image. In this domain, the secret data is directly inserted into the actual image pixel's intensity value. The pixels value is either 8-bit, 16-bit, or 24-bit relied on the standard of the image. The easiest and simplest method under this technique is the LSB method. The secret information is converted into a series of bits before embedding secret information into a cover image [25].

4.1.1. Least significant bit 'LSB'

LSB is the easiest and simplest algorithm. The cover image's least significant bit (8-bit) is altered by the bit of the hidden message. It is utilized to insert hidden data in a cover image sometimes it is referred to as LSB Replacement. Because the LSB method depends on changing the redundant bits that are less important or significant with the secret information bits, particularly the rightmost bits will be replaced with the bits of the secret data because it does not affect the image's quality. The aim of LSB is to transmit the secret data to the receiver without knowing to the attacker that the information is being transmitted. Although LSB is an easy and quick method, it has a weakness, which can be easily detected by an attacker [25].

4.1.2. LSB in bitmap file (BMP)

In this technique, a 24-bit BMP image format is used which consists of RGB color. Each bit of the red, green, and blue 'RGB' colors are changed with the bit of secret information since each color is denoted by a single byte (8-bit). In other words, a 24-bit BMP image format can store 3 pixels. BMP file format uses a lossless compression technique. LSB in BMP images can hide a large amount of information. This is counted as a disadvantage because a large number of bits need to be altered. As a result, it can be easily detectable by the human eye [25]. There is an example for LSB, 3 pixels grid of a 24-bit image can be shown as:

(00100001 00010100 11010101)
(10110111 11010101 00101101)
(11011010 10100101 01101011)

199 taken as an example, a binary representation of this number is that 11000111, is embedded into the least significant bits of this part of the image. The resulting grid is as:

(0010000**1** 0001010**1** 1101010**0**)
(1011011**0** 1101010**0** 0010110**1**)
(1101101**1** 1010010**1** 01101011)

The above number was embedded in the grid. The last bit of each RGB color is altered with the bits of the number. As a result, the last bit is altered in each pixel which is the least significant bits. Consequently, these small changes are invisible to human eyes.

4.1.3. LSB in a graphical interchange format (GIF)

It is also referred to as palette based LSB. In this technique, a GIF image format is used as a cover image. GIF Image has a depth of 8-bit, but can be described by 256 different colors in the palette, since each color has an index which kept in a look-up table. GIF is an image format using a lossless compression technique. In the lossless compression method, the original image's quality is well protected. It means that the compressed image and the actual image are the same. Furthermore, this form has relied on the format of the file and the image and it can hide a large message. The secret message could be visible if a cover image is selected incorrectly. The problem with this approach is that if one change in LSB's pixel occurs, it can result in a completely altered color because the color index is altered. This problem can be tackled by utilizing GrayScale images. In an 8-bit grayScale GIF image, there are 256 gray shades. The colors are gradually changed in the GrayScale GIF image so it is hard to detect these changes [26].

4.2. Image steganography in the transform domain

It is also referred to as the Frequency domain. The transform domain technique aims to conceal a large amount of information in the image which is less visible for cropping, compression, and image processing. By this, high security will be provided and the secret message cannot be noticed by the eyes of the human. Also, the transform domain technique is more robust concerning common image processing operations and lossy compression. There are various methods under this domain that is used for

Steganography like DCT, DWT, and DFT, whereas the most common is DCT. The most utilized image file format that works with this domain is JPEG [27].

4.1.2. Discrete cosine transform ‘DCT’

This form is utilized in the JPEG image. JPEG uses a lossy compression technique. One advantage of JPEG compression is that the size of the file can be reduced by decreasing the color information [28]. In the DCT technique, the actual image is first converted from the image domain into the transform domain. Next, the alteration is carried out by sorting the pixels into n×n blocks, and then DCT is applied on each block. A mathematical calculation is used to change the pixels and then the position of the pixel values is scattered over the image part. Later, the transformed image is divided into three frequency components (low, high, and middle). A large feature of pixels is located in the low-order DCT coefficients, whereas a fine feature of pixels is located in the high-order. As a result, the secret information is embedded in the selected high-order coefficients. The process of embedding is applied by just altering the images’ coefficients [29].

4.1.3. Discrete wavelet transform ‘DWT’

It provides a powerful algorithm for processing the image and accomplishing steganography with DWT became more popular in the information hiding era due to its simplicity. The embedding process is carried out in DWT by modifying the cover-image’s wavelet coefficients to attain a secure transmission. The component frequency band is split into four smaller bands called sub-bands namely low low ‘LL’, low high ‘LH’, high low ‘HL’, and high high ‘HH’ [30], [31]. The major advantage of DWT is that it provides high robustness due to transforming the actual image into its wavelet coefficient [32].

4.1.4. Discrete fourier transform (DFT)

It is the transform of a finite and discrete-time function. The DFT computes the Bk from xn. The DFT is computed based on (1):

$$\mathrm{Bk} = 1\ \mathrm{N} \sum \mathrm{xn}\ \mathrm{N} - 1\ \mathrm{n} = 0\ \mathrm{e}\ - 2\pi \mathrm{ikn}\ \mathrm{N}\ (6)\mathrm{K} = 1{,}2, \ldots \mathrm{N} - 1 \qquad (1)$$

Where the Bk is the amplitude and phase of the various components of the input signal xn [33].

5. EVALUATION CRITERIA

Each steganography algorithm has some strong and weak points, for evaluating these; a steganography method has to meet some basic requirements. The most critical requirement is that the results have to be unnoticeable and undetectable by human eyes.

5.1. Invisibility

The first and most critical requirement of a stenographic algorithm is imperceptibility because the stenography’s strength is based on its ability to be unseen by the human eye [34].

5.2. Payload capacity

It means that how much data can it hide? The main goal of steganography is to conceal secret data as watermarking that embeds only a small amount of copyright information [34].

5.3. Robustness against statistical attacks

Statistical Steganalysis is the observation practice to detect concealed information by performing some statistical tests on image data. Several steganography algorithms leave a “sign” during the embedding process. Thus, these signs can be easily noted by statistical analysis [34].

5.4. Robustness against image manipulation

The image might be altered by an active attacker to obtain the hidden information, while the image is being transmitted via a communication channel. In addition, some image manipulation, for instance, cropping or rotating can be applied to the image before it reaches its target [34].

5.5. Independent of file format

There are several types of file formats on the Internet, so using only the same image file format simultaneously between the sender and receiver might be doubted. The most powerful steganography algorithms are that which can hide information in any image file format.

6. RESULTS AND DISCUSSION

Image steganography is a critical technique for providing secure communication while transmitting information via an unsecured line like the internet. On the other hand, secure image steganography is more securable than the classical method because the secret information encrypts by cryptography technique before concealing it by steganography technique, so two levels of security are done in secure image steganography. In this study, the most relevant and up-to-date research papers that proposed secure image steganography have been reviewed. As a result, a comparison has been done among the reviewed papers in terms of used steganography and cryptography algorithms, image database, PSNR, advantages, and limitations as tabulated in Table 1.

Table 1. The comparison among reviewed papers

Ref.	Year published	Steganography algorithm used	Cryptography algorithm used	PSNR (dB)	Image database used	Advantages	Limitations
[9]	2013	LSB	Hash- RSA	73.5444 74.0189 73.8220 73.8528	Barbara Lena Tulips Baboon	Practical and reliable for sending data, a good MSE and PSNR achieved for stego-image.	The proposed method was tested by using only one image format.
[10]	2013	LSB	Blowfish	-	Baboon	Robustness, it is very difficult for an intruder to recover the secret message.	Secret messages cannot be easily deciphered if the image format is a lossy compression.
[11]	2013	LSB	Modified AES (MAES)	59.4681 - -	Flower House Peppers	Securable against intruders.	-
[12]	2014	LSB	Huffman coding	30.48 30.28 30.91 30.36	Lena Baboon Airplane Boat	Secure and gave acceptable PSNR.	-
[13]	2015	Canny edge detection	Hash function	39.6310 38.6527 41.5895	Lena Peppers Baboon	More credible due to using a hash function.	More complicated.
[14]	2016	Diffie Hellman	RSA	71.8 71.9 71.9	Lena Peppers Baboon	Very secure.	More complex.
[15]	2016	Improved LSB-Insertion	RSA-Digital signature	56.513	Lena	More robust than the traditional LSB.	Implementation is hard due to the complexity of the algorithm.
[16]	2017	2-D HDWT, alpha blending, 2-D HIDWT	AES	58.7501 45.8089 47.9688	Man Pepper Flower	Providing a high level of security for both encryption and decryption.	Implementation is complex.
[17]	2018	Inverted 2-bit LSB	Arnold's transformation or Arnold's Cat Map (ACM), ACM with RSA	57.8493 - - -	Lena Baboon Airplane Boat	Higher capacity and PSNR value.	-
[18]	2019	LSB	AES	62.89 62.72 66.15 62.88	Lena Baboon Cameraman Zelda	3 security layers of the information and error-free decryption.	-
[19]	2020	LSB	double XOR operations using binary representation	40.74 49.23 55.67	Lena Barbara Man	2 layers of security: encryption and hiding.	-

7. CONCLUSION

Nowadays, a huge amount of data moves and transmits via the internet, so providing security for data is critical and vital. This protection can be obtained via a secure image steganography technology combined with cryptography. Cryptography aims to hide the information so no one can know about the information except the sender and receiver. On the other hand, Steganography is the technique for hiding the existence of the information, so it is difficult to detect by human eyes. In this study, a systematic and comprehensive review has been done about secure image steganography. In the literature review, various up-to-date research papers had been reviewed that proposed secure image steganography by combining steganography and cryptography methods to provide a high-security level. Most of the proposed work used LSB for steganography due to its simplicity, while for cryptography various algorithms have been used such as AES, MAES, RSA, and Blowfish. Moreover, in this paper, an overview of steganography types such as text, image, audio, video, and protocol along with its renowned techniques have been presented. A comparison between the spatial domain and transform domain with their various types such as LSB, DCT, DFT, and DWT has been studied. LSB is simpler and less secure than DCT. The required criteria for evaluating steganography techniques are also explained. As a result, a comparison between the reviewed papers that combined both steganography and cryptography algorithms have been done as depicted in table 1. The comparison indicated that the LSB with Hash-RSA attained a higher PSNR value than the other which was 74.0189 dB. It can be concluded that both steganography and cryptography are methods utilized for protecting information but when they are combined a higher level of security can be achieved because the information is first encrypted by cryptography and then concealed by steganography, so it is extremely tough for an intruder to attain the secret data.

For future study, I intend to propose a secure image steganography model by using a combination of a new cryptography algorithm like elliptic curve cryptography (ECC) and a steganography algorithm like pixel value difference (PVD).

REFERENCES

[1] B. T. Ahmed, O. Y. Abdulhameed, “Fingerprint recognition based on shark smell optimization and genetic algorithm,” *International Journal of Advances in Intelligent Informatics*, vol. 6, no. 2, pp. 123-134, 2020.

[2] B. T. Ahmed, O. Y. Abdulhameed, “Fingerprint Authentication using Shark Smell Optimization Algorithm,” *UHD Journal of Science Technology*, vol. 4, no. 2, pp. 28-39, 2020.

[3] O. Shetye, C. Vanmali, M. Fernandes, P. Patil, “Survey on Different Techniques of Image Steganography,” *International Journal of Computer Applications*, vol. 138, no. 3, pp. 36-38, 2016.

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

[5] O. Y. Abdulhammed, “Strengthening Steganoghraphy by Using Crow Search Algorithm of Fingerprint Image,” *Eastern-European Journal of Enterprise Technologies*, vol. 2, no. 9, pp. 28-36, 2020.

[6] K. Bansal, A. Agrawal, N. Bansal, “A Survey on Steganography using Least Significant bit (LSB) Embedding Approach,” *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, 2020, pp. 64-69.

[7] P. Pareek, N. Monica, “An Overview Of Steganography: Data Hiding Technique,” *International Research Journal of Engineering and Technology (IRJET)*, vol. 7, no. 1, pp. 87-89, 2020.

[8] R. Hegde, S. Jagadeesha, “Design and Implementation of Image Steganography by using LSB Replacement Algorithm and Pseudo Random Encoding Technique,” *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 3, no. 7, pp. 4415-4420, 2015.

[9] A. Kumar, R. Sharma, “A secure image steganography based on RSA algorithm and hash-LSB technique,” *International Journal of Advanced Research in Computer Science Software Engineering*, vol. 3, no. 7, pp. 363-372, 2013.

[10] M. H. Sharma, M. Mithlesh Arya, M. D. Goyal, “Secure image hiding algorithm using cryptography and steganography,” *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN*, vol. 13, no. 5, pp. 1-6, 2013.

[11] J. K. Saini, H. K. Verma, “A hybrid approach for image security by combining encryption and steganography,” *2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013)*, 2013, pp. 607-611.

[12] A. Nag, J. P. Singh, S. Biswas, D. Sarkar, P. P. Sarkar, “A Huffman code based image steganography technique,” in *International Conference on Applied Algorithms*, 2014, pp. 257-265.

[13] S. Singh, A. Datar, “Improved hash based approach for secure color image steganography using canny edge detection method,” *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 15, no. 7, pp. 92-98, 2015.

[14] S. D. M. Satar, N. A. Hamid, F. Ghazali, R. Muda, M. Mamat, P. K. An, “Secure Image Steganography Using Encryption Algorithm*,” in Annual Int'l Conference on Intelligent Computing, Computer Science & Information Systems (ICCSIS-16)*, 2016.

[15] X. Zhou, W. Gong, W. Fu, L. Jin, “An improved method for LSB based color image steganography combined with cryptography,” *2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)*, 2016, pp. 1-4.

[16] V. K. Sharma, D. K. Srivastava, “Comprehensive data hiding technique for discrete wavelet transform-based image steganography using advance encryption standard,” in *Computing and Network Sustainability*, Springer, pp. 353-360, 2017.

[17] E. J. Kusuma, C. A. Sari, E. H. Rachmawanto, “A combination of inverted LSB, RSA, and Arnold Transformation to get secure and imperceptible image steganography,” *Journal of ICT Research Applications*, vol. 12, no. 2, pp. 103-122, 2018.

[18] A. Tauhid, M. Tasnim, S. A. Noor, N. Faruqui, M. A. Yousuf, “A Secure Image Steganography Using Advanced Encryption Standard and Discrete Cosine Transform,” *Journal of Information Security*, vol. 10, no. 3, pp. 117-129, 2019.

[19] A. Ahmed, A. Ahmed, “A Secure Image Steganography using LSB and Double XOR Operations,” *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 20, no. 5, p. 139-144, 2020.

[20] C. Y. Roy, M. K. Goel, “Review on Image Steganography,” *Indian Journal of Science and Technology*, vol. 9, no. 47, pp. 1-5, 2016.

[21] R. Poornima, R. Iswarya, “An overview of digital image steganography,” *International Journal of Computer Science and Engineering Survey*, vol. 4, no. 1, pp. 23-31, 2013.

[22] Image Steganography Block Diagram, 2021. [Online] Available: https://image.slidesharecdn.com/ppt-sreelekshmis-151109062026-lva1-app6892/95/image-steganography-using-lsb-6-638.jpg?cb=1447050147.

[23] S. Kundra, N. Madaan, “A comparative study of image steganography techniques,” *International Journal of Science and Research (IJSR)*, vol. 3, no. 4, pp. 293-297, 2014.

[24] A. Febryan, T. W. Purboyo, R. E. Saputra, “Steganography methods on text, audio, image and video: A survey,” *International Journal of Applied Engineering Research*, vol. 12, no. 21, pp. 10485-10490, 2017.

[25] F. M. Shelke, A. A. Dongre, P. D. Soni, “Comparison of different techniques for Steganography in images,” *International Journal of Application or Innovation in Engineering & Management*, vol. 3, no. 2, pp. 171-176, 2014.

[26] N. Menon, Vaithiyanathan, “A survey on image steganography,” *2017 International Conference on Technological Advancements in Power and Energy (TAP Energy)*, 2017, pp. 1-5.

[27] M. Hassaballah, M. A. Hameed, M. H. Alkinani, “Introduction to digital image steganography,” in *Digital Media Steganography: Elsevier*, pp. 1-15, 2020.

[28] N. Hamid, A. Yahya, R. B. Ahmad, O. M. Al-Qershi, “Image steganography techniques: an overview,” *International Journal of Computer Science and Security (IJCSS)*, vol. 6, no. 3, pp. 168-187, 2012.

[29] P. Joseph, S. Vishnukumar, “A study on steganographic techniques,” *2015 Global Conference on Communication Technologies (GCCT)*, 2015, pp. 206-210.

[30] S. S. Yadahalli, S. Rege, R. Sonkusare, “Implementation and analysis of image steganography using Least Significant Bit and Discrete Wavelet Transform techniques,” *5th International Conference on Communication and Electronics Systems (ICCES)*, 2020, pp. 1325-1330.

[31] M. K. Oudah, R. S. Khudhair, S. M. Kaleefah, A. N. Abed, “Improvement of Image Steganography Using Discrete Wavelet Transform,” *Engineering and Technology Journal*, vol. 38, no. 1A, pp. 83-87, 2020.

[32] S. Dhawan, R. Gupta, “Analysis of various data security techniques of steganography: A survey,” *Information Security Journal: A Global Perspective*, vol. 30, no. 2, pp. 63-87, 2020.

[33] R. Ruchi, U. Ghanekar, “A Brief Review on Image Steganography Techniques,” in *International Conference on Advances in Electronics, Electrical & Computational Intelligence (ICAEEC)*, 2019.

[34] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. Ho, K.-H. Jung, “Image steganography in spatial domain: A survey,” *Signal Processing: Image Communication*, vol. 65, pp. 46-66, 2018.

BIOGRAPHY OF AUTHOR

Bakhan Tofiq Ahmed received the B.Sc. in Software Engineering at Salahaddin University- Erbil- Kurdistan Region- Iraq, in 2010. She obtained the M.Sc. in IT at Sulaimani Polytechnic University- Sulaimani- Kurdistan Region- Iraq, in 2020. Her research interests are in information security, image processing, artificial intelligence, swarm intelligence algorithm, and Biometric system design. She published 5 research articles, 4 articles published in a reputed international journal, and 1 article in a national journal