Journal of King Saud University – Computer and Information Sciences xxx (xxxx) xxx

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

Image steganography using exploiting modification direction for compressed encrypted data

Zeyad Safaa Younus [a,*], Mohammed Khaire Hussain [b]

[a] Faculty of Computer Sciences and Mathematics, University of Mosul, Mosul, Iraq
[b] Northern Technical University, Mosul Technical Institute, Mosul, Iraq

ARTICLE INFO

Article history:
Received 11 December 2018
Revised 9 April 2019
Accepted 12 April 2019
Available online xxxx

Keywords:
Steganography
Cryptography
Exploiting modification direction
Knight tour
Vigenere cipher
Huffman coding

ABSTRACT

Building a balanced relation between image quality and the payload, the robustness of the method in facing electronic attacks and securing data, all the mentioned processes represent the main challenge in steganography. Here, a novel approach to steganography is suggested using Vigenere Cipher and Huffman Coding methods to encrypt and compress the mystery message content. This approach will raise the security and ensure the message content cannot be extracted without earlier knowledge of decrypting rules and the Huffman Dictionary Table. Later, the image is segmented into blocks, size ($w*h$) groups for each block and with each group having n pixels. Subsequently, the knight tour algorithm and arbitrary function are utilized to select which blocks and groups can be used to conceal the mystery digit within a specific pixel in the group randomly. This is to address the weakness of the Exploiting Modification Direction (EMD) technique that uses a serial selection to enhance the robustness of the suggested scheme. The EMD technique is then utilized to insert the mystery digits inside a specific pixel. Later, the chi-square method is employed to apply statistical attacks on the stego-image to estimate the suggested scheme robustness. The empirical outcomes show that the suggested scheme is more efficient compared to the old Steganography schemes with respect to Imperceptibility by PSNR of 55.71 dB, the Payload of 52,400 bytes and the robustness.

1. Introduction

In recent years, data protection has become a highly important issue as a result of the enormous progress of information and communication technology and the huge increase in internet usage through sending and receiving data. Therefore, researchers have focused on creating schemes for data protection and studies have been conducted to develop old techniques and launch new ones to protect data from hackers (Morkel et al., 2005). Cryptography is a method utilized to protect a mystery data by encrypting the data in a manner that no one can read it except those who have the mystery key. It is also one way to guarantee that the data are not changed during the transmission process. Many methods have been developed for encrypting and decrypting data to protect them, but these methods have become inefficient following the advent of the internet. Therefore, new techniques have been required to address this issue, and this has led to the emergence of the Steganography concept (Rehman et al., 2013; Kumar and Kumar, 2017; Younus and Younus, 2019). Steganography is the knowledge and skill of hiding the information or any communication about network users between the dispatcher and the receiver of the mystery data through a digital media holding the information (Habibi et al., 2013; Tejeshwar, 2014; Ranjani, 2017; Taha et al., 2018). The term (steganography) is of Greek origin and derived from (steganos) meaning (concealed) and (graph) meaning (script) which refers to (concealed script) (Kalra and Singh, 2014; Hashim and Rahim, 2017). The main purpose of cryptography and steganography techniques is to protect data from being accessed by unauthorized persons. The difference between these techniques is that encryption protects the contents of the message by rewriting it, but it stays visible because of being written in plain text. On the other hand, steganography keeps the message invisible by hiding it within digital media (Wang and Wang, 2004; Wanget al., 2010). Combining cryptography and steganography

* Corresponding author.
E-mail addresses: zeyad.saffawi@uomosul.edu.iq (Z.S. Younus), mohammed.khaire@ntu.edu.iq (M.K. Hussain).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2019.04.008
1319-1578/

Please cite this article as: Z. S. Younus and M. K. Hussain, Image steganography using exploiting modification direction for compressed encrypted data, Journal of King Saud University –Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.04.008

schemes is more efficient for the purpose of obtaining the security and data protection (Sahu et al., 2018; Younus and Younus, 2019). Image steganography is a technique which uses the images as a carrier for a mystery message because the Internet accommodates a large amount of digital images and also offers ease in dealing with images (Kuo et al., 2015; Saha et al., 2018; Shet et al., 2019).

2. Related works

The main challenge of data hiding schemes is in embedding the largest amount of information in the image by retaining the quality as well as the security and the strength of the method in facing electronic attacks by hackers. Many schemes and systems have been suggested to conceal data in images because of the huge amount of digital images on the web and also the simplicity of dealing with images in a hiding process (Chang et al., 2007; Cheddad et al., 2010; Maniriho and Ahmad, 2018). Towards this end, researchers have attempted to find modern techniques to cope with the rapid development in hiding techniques to achieve accurate results. Recently, researchers have focused on improving the hiding process in images by using different methods like LSB and EMD.

Least Significant Bit (LSB) scheme is very popular for concealing data within images. This scheme directly deals with the image by changing the least significant bit value to embed the mystery information and to make the changing process in the image very difficult to recognize with the human eye. Therefore, this is a good scheme to embed secret information by making invisible changes in the image, but it is a weak scheme to face the electronic attacks by using the chi-square (x^2) method (Chan and Cheng, 2004; Shjul and Kulkarni, 2011).

Zhang and Wang (2006) suggested the Exploiting Modification Direction (EMD) technique in which the image is partitioned into several groups containing n pixels to insert the mystery digit in $(2n + 1)$-ary encoding system. During the inserting process, the rate of a certain pixel inside a group is increased or reduced by 1. The drawback of this scheme is the low image quality because the size of the group has two pixels. Lee et al. (2007) presented a scheme to improve the EMD method called (IEMD). This method achieves a large amount of data compared with the traditional EMD method without affecting the image quality. In this method, the mystery message is transformed into mystery digit in 8-ary encoding System and each mystery digit is inserted into a group containing two pixels.

Jung and Yoo (2009) introduced a method to improve the traditional EMD method using every pixel in the image to embed one mystery digit in each pixel. In this method, the embedded information in the image is doubled compared to the traditional method. Using this method overcomes the negatives of the EMD method and embeds the largest amount of data while retaining the quality of the image.

Lin et al. (2010) suggested an Opt EMD scheme in which the relationship between the quantity of pixels (n) in each group and the quantity of payload that is embedded within the image is found to reduce the distortion of the image. This scheme achieves high quality, but it is affected by the payload amount.

Mohsin (2013) introduced a scheme utilizing Huffman encoding, affine cipher and Knight Tour methods. In this scheme, the mystery message is encoded and compressed using affine cipher and Huffman coding, and then the mystery message is embedded within an image using LSB and Knight tour algorithm. Here, the image is transformed to YCbCr color space and the mystery message is embedded within Cb component.

Ahmed et al. (2014) presented a method using improved EMD and Huffman coding methods. In this method, the mystery message is compacted utilizing Huffman coding, and then the mystery code is embedded within an image using EMD method, where the group of pixels used for embedding is segmented into two subgroups containing 2 and 3 pixels sequentially to increase the payload without affecting the image quality.

Lee et al. (2015) introduced a scheme of data hiding to multiply the quantity of information embedded in the image using EMD method. In this scheme, the mystery digits are represented using (c^n-ary). Then, the group of (n) pixels is used to insert the mystery digits within it by using C of different methods to modify its value. Alsaffawi (2016) suggested a scheme using LZW method to reduce the size of the mystery data and to increase the amount of payload and using Knight tour method and EMD scheme for inserting the mystery information within the cover image. Saha et al. (2018) presented a method to improve the EMD method. In this scheme, the image is divided into n pixels that are used to embed $2kn$-ary numbers in the main row.

In this paper, Image Steganography scheme is suggested by merging the cryptography and steganography methods. Firstly, Vigenere cipher and Huffman coding are utilized to encrypt and compress the mystery message. This is to protect the data and to reduce the mystery message size for insertion within the image using EMD technique. It is then enhanced utilizing Knight tour scheme and arbitrary function to rise the robustness and the security by choosing the blocks and the groups that are utilized to insert the mystery digit within a specific pixel. This is also to preserve the stego-image quality and make it closer to the cover image.

3. The suggested method

One important issue is the need to establish mystery systems for sending and receiving the information. To achieve this, a new method is proposed to hide the information by combining cryptography and steganography techniques to conceal a large amount of data and considering the stego-image quality after inserting the information within the image. This produces high secrecy in concealing the information within the cover image and increasing the strength of the method in the face of electronic attacks. These factors are the challenges that face the process of hiding data within images. Here, the Vigenere cipher algorithm is used for encoding and decoding the mystery message to enhance the suggested scheme security. Then, the Huffman coding scheme is employed to compress and uncompress the encrypted mystery message to reduce its size. The knight tour algorithm and arbitrary function are then used for arbitrary selection of the blocks and groups of the cover image used for embedding the compressed encrypted mystery message within a particular pixel within it to increase the robustness of the suggested scheme. Following that, the EMD method is used for embedding the compressed encrypted mystery message within the cover image and extracting it. The steps of the proposed scheme include:

1. Encryption process: the mystery message is encoded utilizing a Vigenere cipher algorithm.
2. Compression process: the encrypted mystery message is compressed using Huffman coding method.
3. Embedding process: the compressed encrypted mystery message is embedded within a cover image by using:
   a. Knight tour algorithm and arbitrary function for arbitrary selection of the blocks and the groups used for embedding.
   b. EMD method for embedding the compressed encrypted mystery message within the cover image.
4. Extraction process: the compressed encrypted mystery message is extracted from the stego image using:

Please cite this article as: Z. S. Younus and M. K. Hussain, Image steganography using exploiting modification direction for compressed encrypted data, Journal of King Saud University –Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.04.008

a. Knight tour algorithm and arbitrary function of determining the blocks and the groups that have a message within a particular pixel.
b. EMD method for extracting the compressed encrypted mystery message from the stego image

5. Uncompressing process: the compressed encrypted mystery message is uncompressed using Huffman dictionary table.
6. Decryption process: the encrypted mystery message is decrypted by using a Vigenere cipher algorithm.

3.1. The process of encrypting

Initially, the mystery message is written as a plain text using the English alphabet. To intensify the security, Vigenere algorithm then is utilized to encrypt the mystery message characters because it is a complex and asymmetric scheme. As such, the specific input character is replaced by several output characters depending on its position in the mystery message. The keyword is used for encryption, where each character has (l) possible replacement characters, and where (l) represents the length of the alphabet which is used for writing the mystery message. This makes the decoded process more complex when the unauthorized person discovers the presence of the mystery message. The encrypted mystery message then is compressed using Huffman coding algorithm to minimize the size of the message and to make it harder to discover the message in the image after the embedding process. This is because it is a lossless compression method and it gives high confidence, by generating Huffman dictionary table that includes each character of the encrypted mystery message with their mystery digits which will be sent to the receiver to be utilized during the extraction process.

3.1.1. Vigenere cipher algorithm

Substitution cipher schemes suffer from weakness in the frequency analysis where the largest message can certainly be broken by determining the frequency of characters. To solve this problem Polyalphabetic substitution methods have emerged, by utilizing more than one character to encode the specific input character in the message. A vigenere cipher algorithm is one of the most complicated Polyalphabetic substitution methods (Trappe and Washington, 2006; Dennie, 2007). In this scheme, every character is encrypted depending on its place in the message and on the secret key, which is a vector (Bharti and Kumar, 2014) i.e. the character in the secret message is replaced by several characters in the encrypted message depending on its place. This makes the decrypting process more difficult and increases the security of the message. Eq. (1) is used for encrypting the secret message (Mawengkang et al., 2018).

$$e_k(p_i) = (p_i + k_{(i \bmod m)}) \bmod l \quad (1)$$

where l represents the alphabet length which is used for writing the mystery message and i is the length of the mystery message while m represents the key length, and P_i is the i-th characters of the mystery message while, k represents a vector of keys that are used to encrypt the letters of the message.

3.1.2. Compressing the crypto secret message using Huffman coding algorithm

After the secret message is encrypted using the Vigenere cipher method, Huffman coding algorithm is applied to compress this crypto message to transform it into mystery digits (Nag et al., 2009; Jayaraman et al., 2009). In this scheme, each letter of this message is compressed and transferred into a stream of bits to reduce the size of the crypto message and to increase the payload of data that is inserted inside the cover image. Following this, each bits stream is converted into mystery digits by utilizing Huffman dictionary table. The steps for this method are explained as:

- **Input**: encrypted mystery message.
- **Output**: mystery digits.
- **Step 1:** read the cipher text.
- **Step 2**: create a table which contains letters of cipher text and the number of its occurrences.
- **Step 3**: according to their number of occurrences, the letters are sorted in an ascending order.
- **Step 4**: add the first two occurrences in the table, then resort the table once more.
- **Step 5**: repeat step 4 till unique occurrence number is completed.
- **Step 6**: build tree of Huffman by appointing every twosome of branches by (0,1).
- **Step 7**: tree of Huffman is used to rewrite the cipher text letters.
- **Step 8**: create Huffman dictionary table which includes each letter of crypto secret message with their mystery digits.

3.2. The process of embedding

In this process, the cover image is segmented into blocks of size (w^*h) groups for each block where, the groups are generated by dividing the block in the cover image; each group has (n) pixels to embed the mystery digits within a specific pixel in the group. The number of blocks (b) in the cover image equals the image size divided by ((w^*h) * n). Then, the knight tour algorithm and arbitrary function are used to select the blocks and the groups randomly which has a particular pixel to embed the information within it to overtake the weakness of the traditional EMD scheme which uses the sequential choice to enhance the suggested scheme's robustness because the way of selecting the blocks and the groups is unknown for unauthorized persons. After that, the mystery digits are embedded within the cover image using EMD method.

3.2.1. Knight tour algorithm

The traditional EMD method uses a sequential selection of the groups used for embedding the information within it. This is considered one of the weaknesses because the hacker can simply extract the secret message from the image. Hence, it is essential to discover methods that utilize an arbitrary selection like Knight tour algorithm and arbitrary function. After dividing the cover image into blocks, based on the Knight tour algorithm the cover image is signified as a chessboard and as per the direction of the knight in the chess in various directions similar to the shape of the character (L) in English (Ganzfried, 2004). This is for the purpose of selecting the blocks that are used for inserting the information within the groups randomly. Then, the groups are randomly selected by utilizing mystery key and arbitrary function. Through this method, the groups are randomly selected relying upon mystery key identified by the dispatcher and recipient with a more complicated way and it is difficult to identify the blocks and the groups that have the information within it in case an unauthorized person receives it. This technique is used to enhance the suggested scheme's robustness and to avoid the traditional EMD scheme negatives which utilize the sequential selection of the groups. The algorithm steps include:

- **Input:** cover image size (M^*N).
- **Output:** selected groups within blocks that are used for embedding the information.
- **Step 1:** dividing the image into blocks in size (w^*h) groups for each block as: $b = M^*N / (w^* h)^* n$; where, b represents the number of blocks in the cover image and n represents the number of

Please cite this article as: Z. S. Younus and M. K. Hussain, Image steganography using exploiting modification direction for compressed encrypted data, Journal of King Saud University –Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.04.008

pixels in the group and w represents the number of groups in the row while, h represents the number of groups in the column.

- **Step 2:** the cover image is represented as a chessboard of size (p*q) blocks where, p represents the number of blocks in the row and q stands for the number of blocks in the column.
- **Step 3:** $i = 1$; $j = 1$, k = 1, $v = 1$.
- **Step 4:** for $k = 1$ to b.
- **Step 5:** for $i = 1$ to p ; for $j = 1$ to q.
- **Step 6:** select the next block that has the groups used for embedding as: if the current block (b(i,j)) the next block is selected throw the direction of movement as:
  - If *b (i + 1, j + 2)* did not practice in embedding the information within the groups and *i + 1 < p ; j + 2 < q then b(i + 1 , j + 2) is selected; i = i + 1 , j = j + 2.*
  - else if *b(i + 1 , j-2)* did not practice in embedding the information within the groups and *i + 1 < p j-2>= 1 then b(i + 1 , j-2) is selected; i = i + 1 , j = j-2*;
  - else if *b(i-1, j + 2)* did not practice in embedding the information within the groups and *i-1>=1 ; j + 2 < q then b(i-1, j + 2) is selected; i = i-1 , j = j + 2*;
  - else if *b(i-1, j-2)* did not practice in embedding the information within the groups and *i-1>=1 ; j-2>=1 then b(i-1, j-2) is selected; i = i-1 , j = j-2*;
  - else if *b(i + 2, j + 1)* did not practice in embedding the information within the groups and *i + 2 < p , j + 1 < q then b(i + 2, j + 1) is selected; i = i + 2 j = j + 1*;
  - else if *b(i + 2, j-1)* did not practice in embedding the information within the groups and *i + 2 < p , j-1>=1 then b(i + 2, j-1) is selected; i = i + 2 , j = j-1*;
  - else if *b(i-2, j + 1)* did not practice in embedding the information within the groups and *i-2>=1 , j + 1 < q then b(i-2, j + 1) is selected; i = i-2 , j = j + 1*;
  - else if *b(i-2, j-1)* did not practice in embedding the information within the groups and *i-2>=1 , j-1>=1 then b(i-2, j-1) is selected ; i = i-2 , j = j-1.*
- **Step 7:** gr = *(w*h)*n* divided by n where, *(gr)* represents the number of groups within blocks.
- **Step 8:** for x = 1 to w.
- **Step 9:** for y = 1 to h.
- **Step 10:** if v <= *gr*.
- **Step 11:** x = arbitrary numbers between 1 and gr
- **Step 12:** $w = w + 1$, $h = h + 1$, $v = v + 1$
- **Step 13**: repeat step 6 until the selected blocks are finished.

3.2.2. EMD method

In this method, (*2n + 1*)-ary encoding system is employed to represent the mystery digits that are embedded within the cover image after selecting the groups randomly; where, the mystery digits obtained from the Huffman coding method are embedded within the group by adding or subtracting 1 from the certain pixel inside the group. Eq. (2) represents the extraction function (f) as (Zhang and Wang, 2006):

$$f = f(g_1, g_2, \ldots g_n) = \left[\sum_{i=1}^{n} (g_i \times i)\right] \; mod \; (2n+1) \tag{2}$$

where, (g_1, g_2, …, g_n) represents the values of the pixels inside the group; while, (n) represents the number of pixels in each group.

Following that, compare the value of (f) and the value of the mystery digit (d). It is not necessary to change the value of pixel if $f = d$ because the value of the mystery digit is equivalent to the estimation of the original pixel otherwise the value of image indicator (s) is computed using Eq. (3) (Zhang and Wang, 2006):

$$s = d - f.mod(2n+1) \tag{3}$$

Later, if the estimation of (s) is fewer than or like (n) then the pixel value (g_s) is increased by one or else decrease the value of (g_{2n+1-s}) by one. The steps of this algorithm include:

- **Input:** mystery digit (d), cover image (M*N), selected groups.
- **Output:** stego-image
- **Step 1:** n represents the number of pixels in the group; $m = 1$; l represents the message length.
- **Step 2:** while $m <= l$
- **Step 3:** random selection of the blocks and the groups using Knight Tour algorithm and arbitrary function.
- **Step 4:** for i = 1 to n
  - f = sum ($g_i \times i$) mod (2n + 1)
  - end loop i
- **Step 5:** if $f \neq d$ then $s = d - f \; mod \; (2n + 1)$
- **Step 6:** if $s \leq n$ then g_s increased by 1 else $g_{(2n+1-s)}$ decreased by 1.
- **Step 7:** $m = m + 1$
- **Step 8:** end loop m

3.3. The process of extraction

In this step, when the embedding process is accomplished, the stego-image is sent by the dispatcher to the receiver. The extraction process is performed using the same steps that are used in the embedding process but in reverse order. Firstly, the stego image is configured by splitting it into blocks of size (w*l) groups and each group has n pixels. Then, determine the blocks that contain the groups using Knight tour scheme. After that, appoint the groups that have the information inside a specific pixel within it by using arbitrary function and apply the same procedures that were used in the embedding process. Then, use the EMD scheme to extract the mystery digits using Eq. (4) (Zhang and Wang, 2006):

$$d = f(g'_1, g'_2, \ldots, g'_n) = \left[\sum_{i=1}^{n} (g'_i \times i)\right] \; mod \; (2n+1) \tag{4}$$

where, d represents the mystery digit value extracted from the group within stego image, n is the number of pixels in each group, while (g'_1, g'_2, …, g'_n) are the pixels value of the group that has the mystery digit.

3.4. The process of decrypting

In this process, after the mystery digits are extracted from the stego-image using EMD scheme, the mystery digits are transferred into a stream of bits. Next, this stream is converted into decimal numbers to get the mystery code. After that, the mystery codes are transferred into the encrypted letters using Huffman dictionary table. Finally, Vigenere cipher is used to decrypt the letters of the secret message and to get the plain text using the same keyword (k) that was used for the encrypting process. Eq. (5) is utilized to decode the encrypted mystery message and extract the original message (Mawengkang et al., 2018).

$$d_k(c_i) = \left(c_i - k_{(i \; mod \; m)}\right) \; mod \; l \tag{5}$$

where c_i are the *i-th* letters of the encrypted message. The extraction process and decrypting process steps include:

- **Input**: stego-image size (M*N).
- **Output**: plain text
- **Step 1:** n is the number of pixels in each group; $m = 1$; l represents the encrypted message length.
- **Step 2**: while $j <= l$

Please cite this article as: Z. S. Younus and M. K. Hussain, Image steganography using exploiting modification direction for compressed encrypted data, Journal of King Saud University –Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.04.008

- **Step 3**: determine the blocks and the groups using Knight tour and arbitrary function using the same steps used in the embedding process.
- **Step 4**: for $i = 1$ to n
  - d = sum $(g_i' \times i)$ mod $(2n + 1)$
  - end loop i
- **Step 5**: convert the mystery digits *d* into bits stream.
- **Step 6**: $m = m + 1$
- **Step 7**: if $m > l$ then go to step 13, otherwise
- **Step 8**: convert the bits stream into decimal mystery digits.
- **Step 9**: $j = j + 1$
- **Step 10**: repeat step 7
- **Step 11**: end loop *j*
- **Step 12**: convert the decimal mystery digits into the crypto letter by using Huffman coding
- **Step 13**: Vigenere cipher is used to decrypt the message and achieve the plain text.

4. Results

The major goal behind this study is to conceal a large quantity of information with a high security and preserve the image quality at the same time. MATLAB 2013a was utilized as a programming language and six images of size 512*512 pixels were taken from USC-SIPI Data Base (USC-SIPI) and used to evaluate the suggested scheme as has been widely used by researchers in the field of information hiding and giving accurate results in terms of quality. Fig. 1 shows the images which were used in this study.

Additionally, the mystery message was prepared and written using the English alphabet, following which the mystery message was encrypted by using a Vigenere cipher algorithm. The encrypting process of the mystery message is explained below:

Assume that the mystery message to be encoded written using the characters of the English alphabet is (***university of mosul***) and the keyword is (***vector***). Here, the length of the alphabet is equal to 26 and each character has 26 possible replacement characters according to its position in the message and the key. Following that, determine the vectors of key as integers where key = (21, 4, 2, 19, 14, 17) and the length of the key is equal to 6. Here, the vectors of key are repeated until they match the length of the mystery message. To encode the mystery message using the key and depending on Eq. (1), the first character *u* in the message is substituted by character *p*. Then substitute the second character *n* with the character *r*, and so on. Also, the characters (u, *i, s and o) in* the message are substituted by various characters in the encrypted

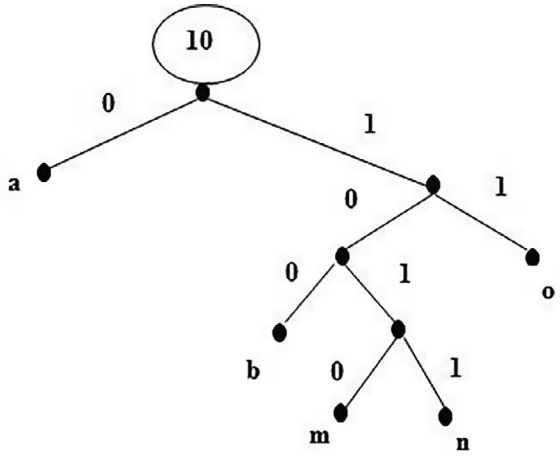

Fig. 2. Huffman tree.

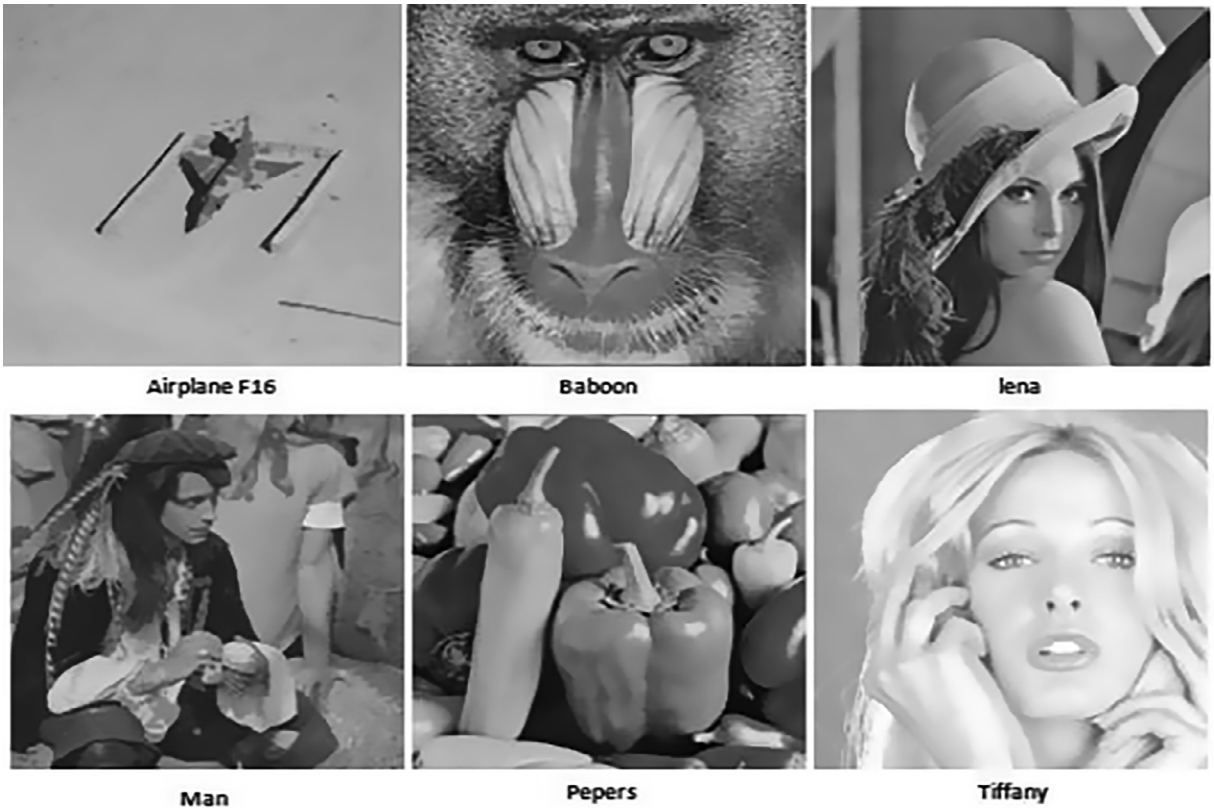

Fig. 1. The images utilized for estimating the suggested scheme.

Please cite this article as: Z. S. Younus and M. K. Hussain, Image steganography using exploiting modification direction for compressed encrypted data, Journal of King Saud University –Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.04.008

message depending on its position in the original message and the key as explained bellow.

Mystery message	u	n	i	v	e	r	s	i	t	y	o	f	m	o	s	u	l
Key	21	4	2	19	14	17	21	4	2	19	14	17	21	4	2	19	14
Encrypted message	p	r	k	o	s	i	n	m	v	r	c	w	h	s	u	n	z

As a result of the encryption process, the mystery message (***university of mosul***) is substituted by the encrypted mystery message (***Prkosinmvr cw Hsunz***) to achieve the security where no one can understand the message except the person who has the key vector and its length.

Later, the Huffman coding algorithm is used for compressing the encrypted mystery message and converting it into a stream of bits. After that, the Huffman dictionary table is used to convert each bit stream into the mystery digits. For example, let the encrypted mystery message be (***aboamanabo***). Firstly create a table that has the characters and their occurrences. Following that, the characters are sorted in ascending order depending on their occurrence. Later, add the first two occurrences and resort the table. Then, repeat this step until unique occurrence number is completed. The steps which are used according to the Huffman coding algorithm are explained below:

Step 1: input the encrypted message (***aboamanabo***)

Step2		Step3		Step4 1st repetition		Step4 2nd repetition	
Character	Occurrence	Character	Occurrence	Character	Occurrence	Character	Occurrence
a	4	m	1	m,n	2	o	2
b	2	n	1	b	2	b,m,n	4
o	2	b	2	o	2	a	4
m	1	o	2	a	4		
n	1	a	4				

Step4 3rd repetition		Step4 4th repetition	
Character	Occurrence	Character	Occurrence
a	4	a,b,m,n,o	10
b,m,n,o	6		

Following that, the Huffman tree is generated, where the left side of the branches in the tree is assigned to 0 and the right side of the branches is assigned to 1 as explained in Fig. 2 below:

The Huffman tree is used to rewrite the characters as a bits stream. Then, each bits stream is converted into the mystery digits using Huffman dictionary table as shown in Table 1 below:

From the table above, notice the characters that have more occurrences denoted as fewer bits than the fewer occurrence characters.

Table 2 shows the results of compressing different sizes of the encoded mystery message. Here, the message size is reduced after compressing it using Huffman coding algorithm while preserving the contents of the message from loss.

The image quality and the payload of data that are inserted within the image and the robustness of the scheme to face the electronic assaults and the security are the most important factors to evaluate the methods of steganography.

Mean Square Error (MSE) is utilized to quantify the average of mean square mistake among pixels of the cover image and stego-image whose value is calculated by utilizing Eq. (6) (Younus and Younus, 2019).

$$MSE = \sum_{i=1}^{M*N} (g_i - g_i')^2 / (M * N) \quad (6)$$

where g_i is a pixel value before inserting the information within the image and g_i' is a pixel value after inserting the information within the image, while, M^*N denotes the size of image. The lower value of MSE means better quality of image.

Peak Signal to Noise Ratio (PSNR) is utilized to calculate the quality of stego-image by relying on the standard value of the Human Visual System (HSV) with a value of (30 dB) (Shen et al., 2017). If the PSNR value is greater than 30, this implies that the inserted data inside the image is invisible to the human eye (Jung and Yoo, 2009; Kuo et al., 2015). Eq. (7) is used to calculate the value of PSNR (Alsaffawi, 2016):

Table 1
Huffman dictionary table.

Characters	Bits stream	Mystery digit (d)
a	0	0
b	100	4
m	1010	10
n	1011	11
o	11	3

Please cite this article as: Z. S. Younus and M. K. Hussain, Image steganography using exploiting modification direction for compressed encrypted data, Journal of King Saud University –Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.04.008

Table 2
The result of compressing the mystery message.

Message size	Compression rate	Message size after Compression
52,400 byte	37.5	36,091
49,152 byte	37.5	18,432
32,768 byte	37.5	12,288
16,384 byte	37.5	6144

$$\text{PSNR} = 10\log_{10}\frac{\max^2}{\text{MSE}} \tag{7}$$

where, max signifies the maximum value of pixels in the image.

Structural Similarity Index Metric (SSIM) is utilized to evaluate the likeness among the cover image and the stego-image (Wang et al., 2004). The yield of SSIM value is limited in the range between 0 and 1. If the SSIM value is close to 1 that indicates the stego-image is alike the cover image and it has high quality. Eq. (8) is used to calculate the value of SSIM (Wang et al., 2004):

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2\mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{8}$$

where, μ_x and μ_y are mean values of cover image (x) and stego-image (y) and σ_x and σ_y are standard deviation values of the cover image and stego image while, σ_{xy} means the covariance of both two images. c_1 and c_2 are constants to stabilize the division.

Embedding rate (ER) is utilized to measure the bits number that can be inserted per pixel of the cover image (bpp) (Zhang et al., 2013). Eq. (9) is used to calculate the value of ER:

$$ER = \frac{p}{M * N} \tag{9}$$

where, P is the total number of bits inserted within a cover image while, M and N represent the size of the cover image. The performance of the suggested scheme is better when the value of embedding rate is high.

Table 3 displays the values of PSNR, MSE and SSIM on various images which are used in this study by using a variety of payloads of the embedded data within the stego image. Here, notice that the PSNR value is greater than 30 and the MSE value is very small which means the proposed method is good in hiding the information inside the stego image by embedding a large amount of information within it and preserving the image quality. Moreover, the value of SSIM is nearer to 1 that means the stego-image is alike the original image with a good quality.

Following that, the suggested scheme is compared with the old schemes using the same payload of data. This is achieved by using four images (Lena, Baboon, Airplane F16, Tiffany) which were used to test the old schemes. Table 4 depicts the results of a comparison between the suggested scheme and the former schemes. The PSNR value of the suggested scheme is 55.71 dB when using the full size of data which is 52400byte and the embedding rate equals 1.59bpp compared to its values of the methods of EMD (Zhang and Wang, 2006), Opt EMD (Lin et al., 2010) and LSB overflow because the size of data exceed the allowed limits for those methods which are 49,152 byte (1.5 bpp). When the sizes of embedded data are 49,152 byte (1.5 bpp), 32,768 byte (1 bpp) and 16,384 byte (0.5 bpp), the values of PSNR are 55. 98 dB, 57.53 dB, 60. 79 dB respectively for the proposed scheme. According to the empirical results, the PSNR value of the suggested scheme is more efficient than the previous schemes with the capacity to insert the maximum size of mystery information within the image without affecting the image quality.

Table 5 displays the results of a comparison between the suggested scheme and (Mohsin, 2013) scheme. Here, the suggested scheme is compared with the (Mohsin, 2013) scheme using four images (Lena, Baboon, Airplane F16, Peppers) which were used to test the (Mohsin, 2013) scheme and using the same payload of data. Here, notice that the PSNR value of the suggested scheme is better than (Mohsin, 2013) scheme with the capacity to insert the mystery information within the image without affecting the image quality.

Chi-square attack (x^2) method is a potential electronic attack method used to recognize the robustness and security of the suggested scheme to face electronic attacks through its ability to statistically analyze the image instead of the physical test to find out whether the image contains secret message or not (Lee et al., 2009; Zanganeh and Ibrahim, 2011). In this method, the frequency distribution expected of the cover image is compared with the frequency distribution of the stego image after embedding data to find out whether there is a change in the image or not (Nissar and Mir, 2010). If the value of the frequency distribution is about zero, this means that the frequency distribution is as the original frequency distribution of the image and there is no secret message within it. However, if the distribution is about one, this means that there is a secret message within the image. Figs. 3–10 show the use of the method of x^2 on the original images (Tiffany, Peppers, Baboon and Lina) and on the same images after embedding the mystery message within it using the suggested scheme.

The figures above show the possibility of frequency distribution of the stego images after embedding the information within it by using the proposed scheme which is very close to the possibility of the normal frequency distribution of the original image which means the mystery message cannot be discovered by the hacker. Figs. 11–13 show the comparison by using the method of x^2 on the original image (Man), and on the same image after embedding

Table 3
PSNR, MSE and SISM values of the suggested scheme.

Payload	Images dataset						
	Measures	Lena	Baboon	Airplane F16	Tiffany	Pepers	Man
52,400 byte	PSNR	55.69	55.70	55.73	55.72	55.76	55.72
	MSE	0.20	0.20	0.21	0.20	0.20	0.20
	SSIM	0.91	0.91	0.92	0.92	0.92	0.92
49,152 byte	PSNR	55.96	55.98	56.02	55.95	55.91	55.95
	MSE	0.17	0.17	0.17	0.17	0.17	0.17
	SSIM	0.94	0.94	0.95	0.94	0.93	0.94
32,768 byte	PSNR	57.77	57.76	56.81	57.79	57.70	57.72
	MSE	0.11	0.11	0.11	0.11	0.11	0.11
	SSIM	0.97	0.97	0.96	0.97	0.96	0.96
16,384 byte	PSNR	60.74	60.81	60.76	60.84	60.80	60.81
	MSE	0.06	0.06	0.06	0.06	0.06	0.06
	SSIM	0.98	0.99	0.99	0.99	0.99	0.99

Please cite this article as: Z. S. Younus and M. K. Hussain, Image steganography using exploiting modification direction for compressed encrypted data, Journal of King Saud University –Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.04.008

Table 4
A comparison between the suggested method and the old methods.

Methods	Payload	Embedding rate (bpp)	PSNR value				Average of PSNR
			Lena	Baboon	Airplane F16	Tiffany	
Proposed Method	52,400 byte	1.59	55.69	55.70	55.73	55.72	55.71
Opt EMD			overflow				
EMD			overflow				
LSB			overflow				
Proposed Method	49,152 byte	1.5	55.96	55.98	56.02	55.95	55.98
Opt EMD			52.11	52.11	52.10	52.11	52.11
EMD			52.11	52.11	52.10	52.11	52.11
LSB			45.91	45.92	45.63	45.94	45.85
Proposed Method	32,768 byte	1.0	57.77	57.76	56.81	57.79	57.53
Opt EMD			54.67	54.66	54.67	54.66	54.66
EMD			53.86	53.87	53.87	53.86	53.87
LSB			51.14	51.14	51.16	51.14	51.14
Proposed Method	16,384 byte	0.5	60.74	60.81	60.76	60.84	60.79
Opt EMD			58.37	58.38	58.36	58.36	58.37
EMD			56.88	56.89	56.89	56.88	58.89
LSB			54.16	54.15	54.16	54.15	54.16

Table 5
A comparison between the suggested method and (Mohsin, 2013) scheme.

Methods	Payload	PSNR value				Average of PSNR
		Lena	Baboon	Airplane F16	Peppers	
Proposed Method	32,768 byte	57.77	57.76	56.81	57.70	57.51
(Mohsin, 2013) scheme		43.871	43.893	44.098	44.018	43.97
Proposed Method	20,480 byte	58.12	58.07	57.87	58.05	58.02
(Mohsin, 2013) scheme		45.928	45.936	46.261	46.076	46.05
Proposed Method	10,240 byte	62.32	62.29	61.92	62.22	62.19
(Mohsin, 2013) scheme		49.038	48.943	49.196	49.042	49.05
Proposed Method	5120 byte	64.17	64.08	63.88	64.06	64.04
(Mohsin, 2013) scheme		52.079	51.936	52.168	52.138	52.08
Proposed Method	1024 byte	70.75	70.74	69.52	70.46	70.36
(Mohsin, 2013) scheme		58.834	58.973	58.874	59.091	58.94

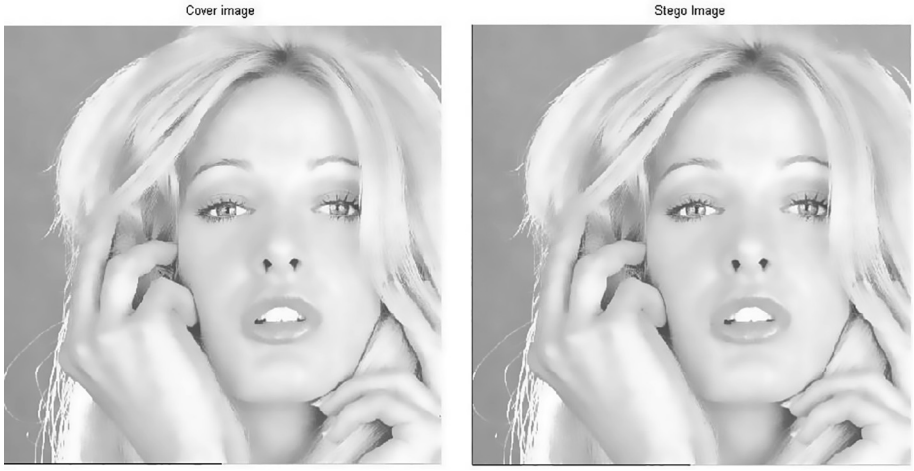

Fig. 3. Tiffany image before and after embedding process.

the mystery message within it by using the suggested scheme and the old schemes which are (traditional EMD scheme and simple LSB scheme).

Through comparison among the figures above, the possibility of frequency distribution of the stego image (Man) after embedding the information within it by using the suggested scheme which is highly close to the possibility of the normal frequency distribution of the original image. This means the mystery message cannot be discovered by the hacker, whereas in the traditional EMD scheme the possibility value of the frequency distribution is close to one at the beginning of the test while in the simple LSB scheme, the possibility value of the frequency distribution is close to one that the hacker will discover the secret message within the (Man) image. This displays the robustness of the suggested scheme in facing electronic attacks by keeping the security of the information.

Please cite this article as: Z. S. Younus and M. K. Hussain, Image steganography using exploiting modification direction for compressed encrypted data, Journal of King Saud University –Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.04.008

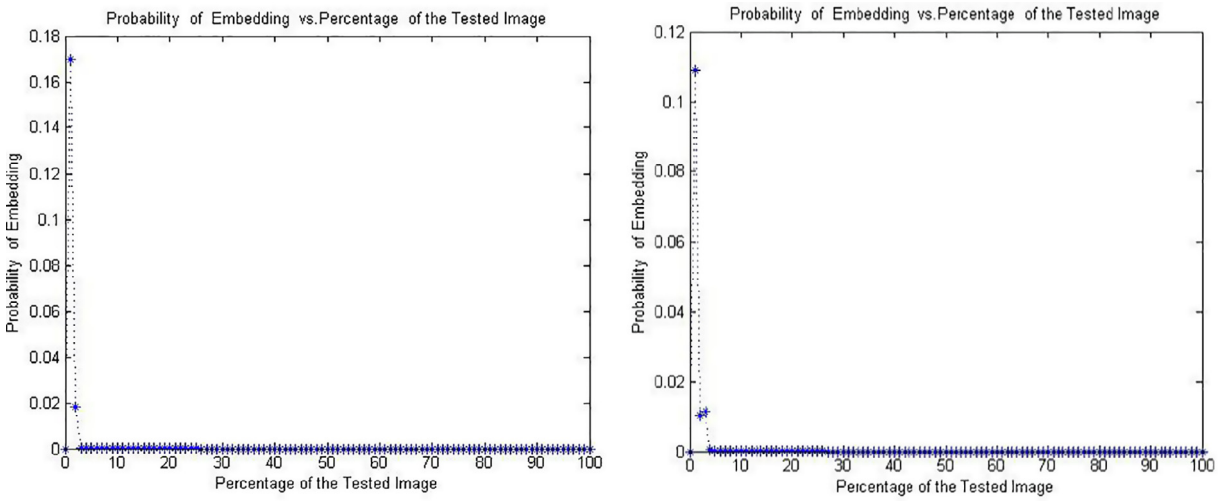

Fig. 4. The result of generating x^2 method on Tiffany image before and after embedding process using the suggested scheme.

Fig. 5. Peppers image before and after embedding process.

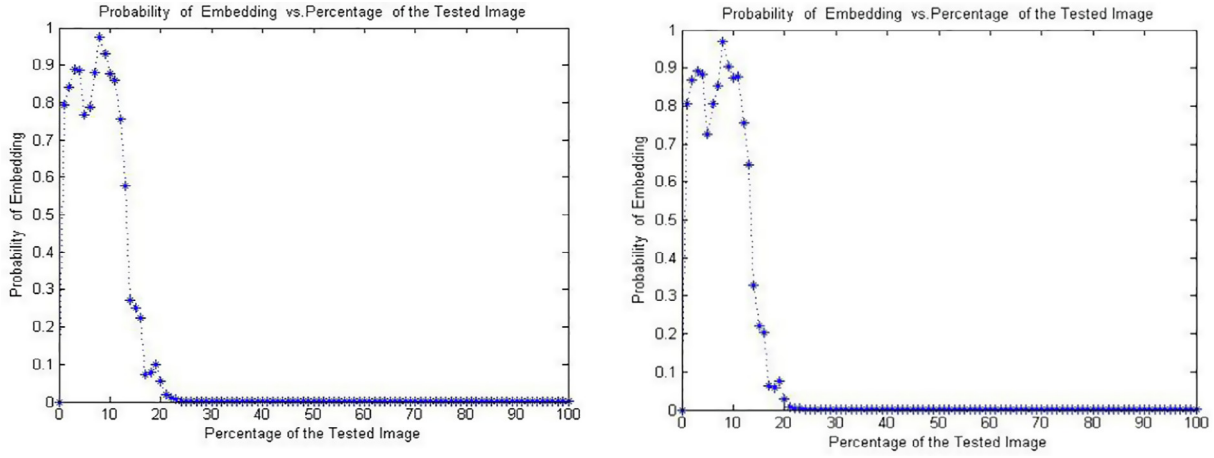

Fig. 6. The result of generating x^2 method on Peppers image before and after embedding process using the suggested scheme.

Please cite this article as: Z. S. Younus and M. K. Hussain, Image steganography using exploiting modification direction for compressed encrypted data, Journal of King Saud University –Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.04.008

Fig. 7. Baboon image before and after embedding process.

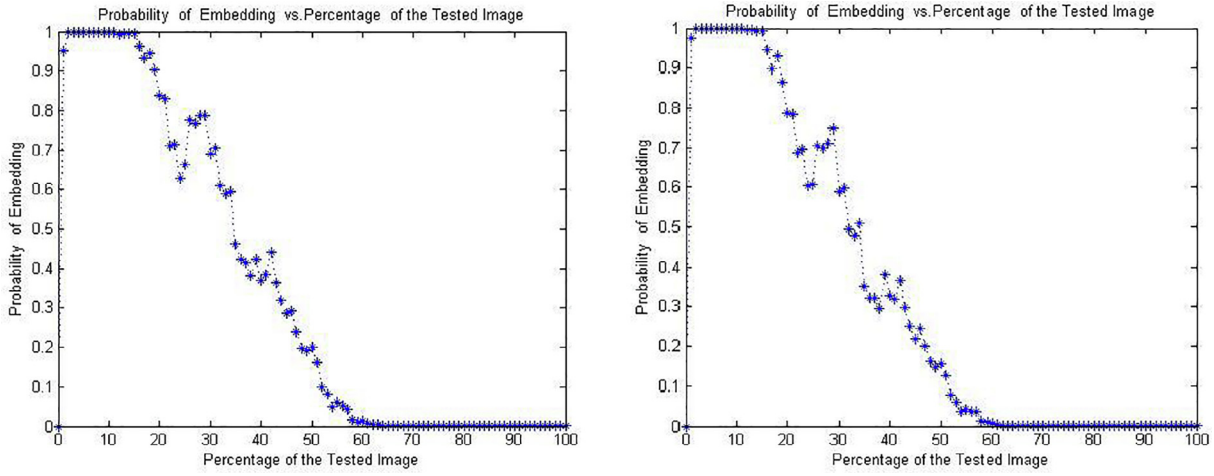

Fig. 8. The result of generating x^2 method on Baboon image before and after embedding process using the suggested scheme.

Fig. 9. Lina image before and after embedding process.

Please cite this article as: Z. S. Younus and M. K. Hussain, Image steganography using exploiting modification direction for compressed encrypted data, Journal of King Saud University –Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.04.008

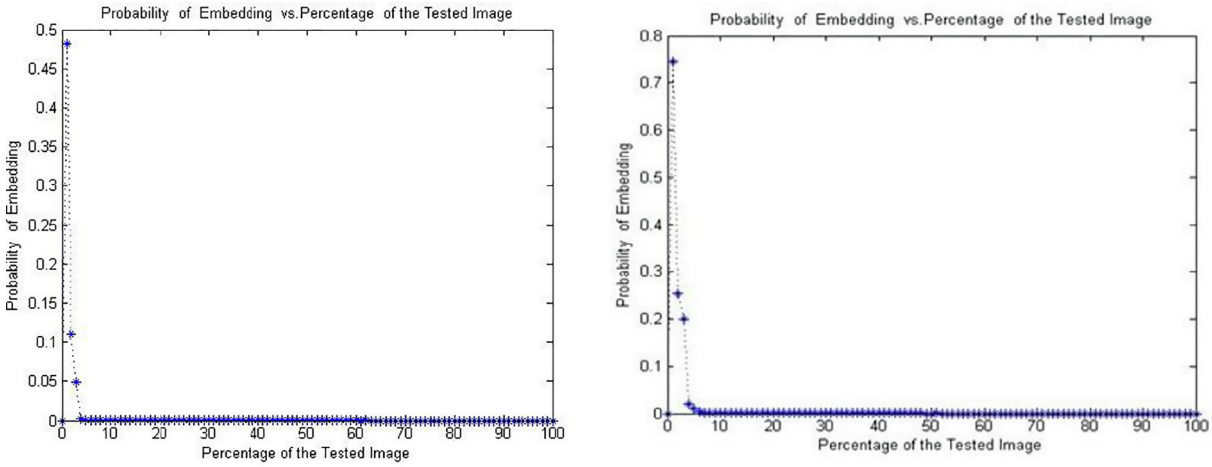

Fig. 10. The result of generating x^2 method on LINA image before and after embedding process using the suggested scheme.

Fig. 11. Man image before and after embedding process.

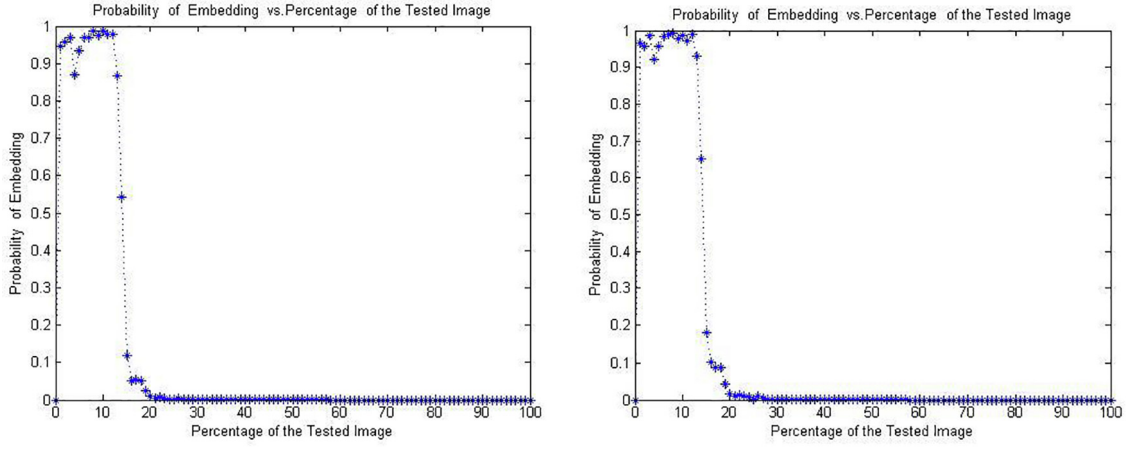

Fig. 12. The result of generating x^2 method on Man image before and after embedding process using the suggested scheme.

5. Conclusion

The major goal of steganography schemes is to conceal a large amount of information within an image without affecting the image quality. In addition, the robustness and the security of these schemes provide protection against electronic attacks. In this study, a novel scheme has been suggested to hide the information within images by merging cryptography and steganography methods using four techniques. Firstly, the secret message contents are encrypted using Vigenere cipher in order to protect data and to

Please cite this article as: Z. S. Younus and M. K. Hussain, Image steganography using exploiting modification direction for compressed encrypted data, Journal of King Saud University –Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.04.008

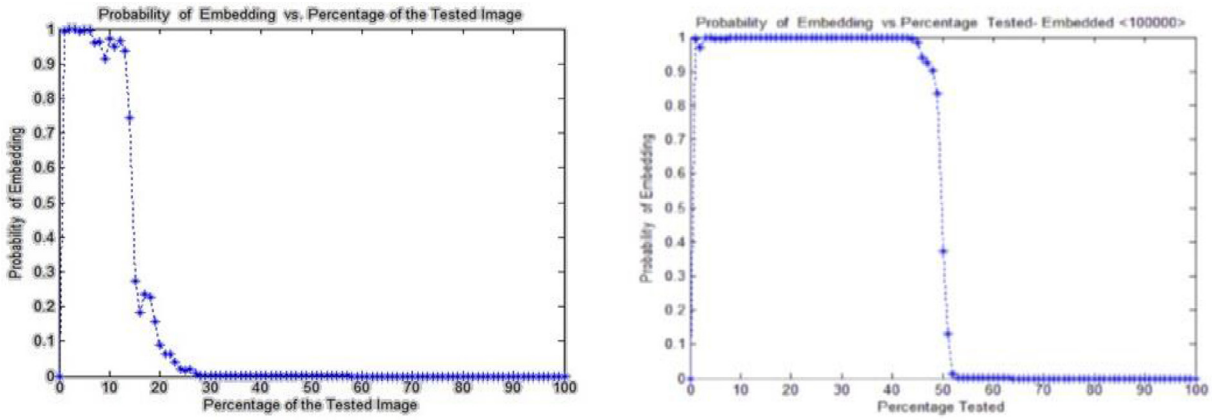

Fig. 13. The result of generating x^2 method on the Man image after embedding process using traditional EMD scheme and simple LSB scheme (Afrakhteh and Ibrahim, 2010).

increase the security of the suggested scheme. Then, the encrypted message is compacted using Huffman Coding methods to minimize the message size and to increase the payload. Subsequently, the compressed encoded message is inserted within the image by using a Knight tour scheme to select the blocks and by using an arbitrary function to select the groups used for inserting the information in a certain pixel within it randomly. This is to achieve a higher security for the suggested scheme and to improve the performance of the EMD method that uses a serial selection of the group. After that, the EMD technique is used to insert one mystery digit within the group by modifying one grayscale value for a specific pixel. The suggested scheme is evaluated by using PSNR, MSE and SSIM for evaluating the quality and by using the compression rate and the embedding rate for evaluating the payload. In addition, x^2 method is used for evaluating the robustness of the suggested scheme against electronic attacks. The empirical results show that the quality and the payload of the suggested scheme are better than the old schemes. In addition, the security and robustness of the suggested method are found to be adequate in facing electronic attacks. In future works, it is possible to test the method through generating other electronic attacks and also, it is possible to use other methods for random selection.

Conflict of interest

None.

Acknowledgment

The authors are grateful to the Ministry of Higher Education and Scientific Research (MOHESE), Iraq for supporting this scientific research.

References

Afrakhteh, M., Ibrahim, S., 2010. Enhanced least significant bit scheme robust against chi-squared attack. In: IEEE 2010 Fourth Asia International Conference on Mathematical/Analytical Modelling and Computer Simulation, Bornea, pp. 286–290. https://doi.org/10.1109/AMS.2010.64.

Ahmad, A., Sulong, G., Rehman, A., Alkawaz, M., Saba, T., 2014. Data hiding based on improved exploiting modification direction method and huffman coding. J. Intell. Syst. 23 (4), 451–459. https://doi.org/10.1515/jisys-2014-0007.

Alsaffawi, Z.S.Y., 2016. Image steganography by using exploiting modification direction and knight tour algorithm. J. Al-Qadissiya Comput. Sci. Math. 8 (1), 1–11.

Bharti, D., Kumar, A., arti and Kumar 2014. Enhanced steganography algorithm to improve security by using vigenere encryption and first component alteration technique. Int. J. Eng. Trends Technol. 13 (5).

Chan, C., Cheng, L., 2004. Hiding data in images by simple LSB substitution. Pattern Recogn. 37, 469–474. https://doi.org/10.1016/j.patcog.2003.08.007.

Chang, C., Tai, W., Chen, K., 2007. Improvements of EMD embedding for large payloads. In: Third International Conference on International Information Hiding and Multimedia Signal Processing (IIH-MSP 2007). ACM, pp. 473–476.

Cheddad, A., Condell, J., Curran, K., McKevitt, P., 2010. Digital image steganography: survey and analysis of current methods. Signal Process. 90, 727–752. https://doi.org/10.1016/j.sigpro.2009.08.010.

Dennie, V., 2007. Cryptographic techniques for computers: substitution methods. Inf. Storage Retrieval 6, 241–249.

Ganzfried, S., 2004. A new algorithm for knight's tours. REU Program in Mathematics at Oregon State University.

Habibi, M., Karimi, R., Nosrati, M., 2013. Using SFLA and LSB for text message steganography in 24-bit RGB color images. Int. J. Eng. 2 (3), 68–75.

Hashim, M., Rahim, M., 2017. Image steganography based on odd/even pixels distribution scheme and two parameters random function. J. Theor. Appl. Inf. Technol. 95 (22), 5977–5986.

Jayaraman, S., Esakkirajan, S., Veerakumar, T., 2009. Digital Image Processing. Tata McGraw Hill Education Private Limited, India.

Jung, K., Yoo, K., 2009. Improved exploiting modification direction method by modulus operation. Int. J. Signal Process. Image Process. Pattern. 2 (1), 79–87.

Kalra, M., Singh, P., 2014. EMD techniques of image steganography a comparative study. Int. J. Technol. Explor. Learn. 3 (2).

Kumar, V., Kumar, D., 2017. Performance evaluation of modified color image steganography using discrete wavelet transform. J. Intell. Syst. https://doi.org/10.1515/jisys-2017-0134.

Kuo, W., Wang, C., Huang, Y., 2015. Binary power data hiding scheme. Int. J. Electron. Commun. 69 (11), 1574–1582. https://doi.org/10.1016/j.aeue.2015.07.007.

Lee, C., Chang, C., Pai, P., Liu, C., 2015. Adjustment hiding method based on exploiting modification direction. Int. J. Netw. Security 17 (5), 607–618.

Lee, C., Wang, Y., Chang, C., 2007. A steganography method with high capacity by improving exploiting modification direction. In: IEEE Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP), pp. 497–500. https://doi.org/10.1109/IIH-MSP.2007.62.

Lee, Y., Bell, G., Huang, S., Wang, R., Shyu, S., 2009. An Advance Least-Significant-Bit Embedding Scheme for Steganographic Encoding. Advance in Image and Video Technology. Springer, Berlin Heidelberg, pp. 349–360.

Lin, K., Hong, W., Chen, J., Chen, T., Chiang, W., n et al. 2010. Data hiding by exploiting modification direction technique using optimal pixel grouping. In: IEEE 2010 2nd international Conference on Education Technology and Computer (ICETC). https://doi.org/10.1109/ICETC.2010.5529581.

Maniriho, P., Ahmad, T., 2018. Information hiding scheme for digital images using difference expansion and modulus function. J. King Saud Univ.-Comput. Inf. Sci. 1–13. https://doi.org/10.1016/j.jksuci.2018.01.011.

Mawengkang, H., Sitepu, I., Efendi, S., 2018. Security analysis in file with combinations One Time Pad Algorithm and Vigenere Algorithm. In: IOP Conf. Series: Materials Science and Engineering (2018) 2nd Nommensen International Conference on Technology and Engineering, pp. 21–29. https://doi.org/10.1088/1757-899X/420/1/012129.

Mohsin, A.T., 2013. A New Steganography Technique Using Knight's Tour Algorithm, Affine Cipher And Huffman Coding (Master Thesis). Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia.

Morkel, T., Eloff, J., Olivier, M., 2005. An overview of image steganography. Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005). Sandston, South Africa.

Nag, A., Biswas, A., Sarkar, D., Sarkar, P., 2009. A Novel technique for image steganography based on DWT and huffman encoding. Int. J. Comput. Sci. Security 4 (6), 561–570.

Nissar, A., Mir, A., 2010. Classification of steganalysis techniques: a study. Digital Signal Process. 20, 1758–1770. https://doi.org/10.1016/j.dsp.2010.02.003.

Ranjani, J., 2017. Data hiding using pseudo magic squares for embedding high payload in digital images. Multimedia Tools Appl. 76 (3), 3715–3729. https://doi.org/10.1007/s11042-016-3974-1.

Please cite this article as: Z. S. Younus and M. K. Hussain, Image steganography using exploiting modification direction for compressed encrypted data, Journal of King Saud University –Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.04.008

Rehman, A., Alqahtani, S., Altameem, A., Saba, T., 2013. Virtual machine security challenges: case studies. Int. J. Mach. Learn. Cybern. https://doi.org/10.1007/s13042-013-0166-4.

Saha, S., Ghosal, S., Chakraborty, A., Dhargupta, S., Sarkar, R., Mandal, J., 2018. Improved exploiting modification direction-based steganography using dynamic weightage array. Electron. Lett. 54 (8), 498–500. https://doi.org/10.1049/el.2017.3336.

Sahu, A., Swain, G., Babu, E., 2018. Digital image steganography using bit flipping. Cybern. Inf. Technol. 18 (1), 69–80. https://doi.org/10.2478/cait-2018-0006.

Shen, Y., Huang, L., Yu, S., 2017. A novel adaptive data hiding based on improved EMD and interpolation. Multimedia Tools Appl. 77 (1), 1–17. https://doi.org/10.1007/s11042-017-4905-5.

Shet, K., Aswath, A., Hanumantharaju, M., Gaw, X., 2019. Novel high-speed reconfigurable FPGA architectures for EMD-based image steganography. Multimedia Tools Appl. 1–30. https://doi.org/10.1007/s11042-019-7187-2.

Shjul, A., Kulkarni, U., 2011. A secure skin tone based steganography using wavelet transform. Int. J. Comput. Theory Eng. 3 (1), 16–22.

Taha, A., Hammad, A., Selim, M., 2018. A high capacity algorithm for information hiding in Arabic text. J. King Saud Univ., 1–8 https://doi.org/10.1016/j.jksuci.2018.07.007.

Tejeshwar, G., 2014. Colour image steganography using LZW compression and fisher-yates shuffle algorithm. Int. J. Innovative Res. Develop. 3 (6), 54–61.

Trappe, W., Washington, L., 2006. In: Introduction to Cryptography with Coding Theory. second ed. ACM Pears on Education International, pp. 14–15.

USC-SIPI Image Database. Available from: https://sipi.usc.edu/database/.

Wang, H., Wang, S., 2004. Cyber warfare: steganography vs. steganalysis. Commun. ACM 47, 10.

Wang, J., Sun, Y., Xu, H., Chen, K., Kim, H., Joo, S., 2010. An improved section-wise exploiting modification direction method. Signal Process. ACM 90 (11), 2954–2964. https://doi.org/10.1016/j.sigpro.2010.04.022.

Wang, Z., Bovik, A., Sheikh, H., Simoncelli, E., 2004. Image quality assessment: from error measurement to structural similarity. IEEE Trans. Image Process. 13 (1), 1–14.

Younus, Z.S., Younus, G.T., 2019. Video steganography using knight tour algorithm and LSB method for encrypted data. J. Intell. Syst. https://doi.org/10.1515/jisys-2018-0225.

Zanganeh, O., Ibrahim, S., 2011. Adaptive image steganography based on optimal embedding and robust against chi-square attack. Inf. Technol. J. 10 (7), 1285–1294. https://doi.org/10.3923/itj.2011.1285.1294.

Zhang, X., Wang, S., 2006. Efficient stenographic embedding by exploiting modification direction. IEEE Commun. Lett. 10 (11), 781–783. https://doi.org/10.1109/LCOMM.2006.060863.

Zhang, Y., Jiang, J., Zha, Y., Zhang, H., Zhao, S., 2013. Research on embedding capacity and efficiency of information hiding based on digital images. Int. J. Intell. Sci. 3 (2), 77–85. https://doi.org/10.4236/ijis.2013.32009.

Please cite this article as: Z. S. Younus and M. K. Hussain, Image steganography using exploiting modification direction for compressed encrypted data, Journal of King Saud University –Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.04.008