RESEARCH ARTICLE OPEN ACCESS

Image Security Enhancement With Vigenere Knight's Tour And Advanced Encryption Standard Technique

S.Jagadeesan M.Sc(CS)., MCA., M.Phil(CS)., ME(CSE).,*, R.Indhumathi**
* Assistant Professor, Department of MCA, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India.
Email: jagadeesan12398@gmail.com
** Final MCA, Department of MCA, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India.
Email: suryaindhu8056@gmail.com

****

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 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 reinforce 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.

Keywords — **Cryptography, Stegnography, Exploiting modification direction, Knight tour, Vigenere cipher, Huffman coding**

****

I. 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; Tahaet 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.

II. THE SUGGESTED METHOD

One important issue is that the got to establish mystery systems for sending and receiving the information. To achieve this, a new method is proposed to hide the information by combining cryptog raphy 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 tactic within the face of electronic attacks. These factors are the challenges that face the method 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 specific pixel within it to increase the robustness of the suggested scheme. Following that,
the EMD method is employed for embedding the compressed encrypted mystery message within the duvet image and extracting it. The steps of the proposed scheme include:

- 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 therefore the groups used for embedding.
  b. EMD method for embedding the compressed encrypted mystery message within the cover image.
  c. Extraction process: the compressed encrypted mystery message is extracted from the stego image using:
- Knight tour algorithm and arbitrary function of determining the blocks and the groups that have a message within a particular pixel.
- EMD method for extracting the compressed encrypted mystery message from the stego image
- Uncompressing process: the compressed encrypted mystery message is uncompressed using Huffman dictionary table.
- Decryption process: the encrypted mystery message is decrypted by using a Vigenere cipher algorithm.

A. The process of encrypting

Initially, the mystery message is written as a clear text using the English alphabet. To intensify the security, Vigenere algorithm then is employed 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 counting 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 attenuate the size of the message and to form it harder to get 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.

[1] Vigenere cipher algorithm

Substitution cipher schemes suffer from weakness in the fre quency 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 precise 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 counting on its place within the message and on the secret key, which may be 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 harder and increases the safety ofthe message. Eq. (1) is used for encrypting the secret message

$$ek(\rho i) = (\rho i + kx_{(i \bmod m)} \ )\text{mod}1 \qquad (1)$$

where l represents the alphabet length which is employed for writing the mystery message and that i is that the length of the mystery message while m represents the key length, and Pi 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

[2] Compressing the crypto secret message using Huffman coding algorithm

After the key message is encrypted using the Vigenere cipher method, Huffman coding algorithm is applied to compress this crypto message to rework it into mystery digits (Nag et al.,2009; Jayaraman et al., 2009). during this scheme, each letter of this message is compressed and transferred into a stream of bits to reduce the dimensions of the crypto message and to extend the payload of data that's inserted inside the duvet 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:** consistent with their occurrences, the are letters number of sorted in an ascending order.
- **Step 4:** add the primary two occurrences within the table, then resort the table another time .
- **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 employed to rewrite the cipher text letters.
- **Step 8:** create Huffman dictionary table which incorporates each letter of crypto secret message with their mystery digits

B. The method of embedding

In this process, the duvet image is segmented into blocks of size (w*h) groups for every block where, the groups are generated by dividing the block within the cover image; each group has (n)

pixels to embed the mystery digits within a selected pixel within the group.The number of blocks (b) within the cover image equals the image size divided by ((w*h) * n). Then, the knight tour algorithm and arbitrary function are wont to select the blocks and therefore the groups randomly which features a particular pixel to embed the knowledge within it to overtake the weakness of the normal EMD scheme which uses the sequential option to enhance the suggested scheme's robustness because the way of choosing the blocks and the groups is unknown for unauthorized persons. then , the mystery digits are embedded within the duvet image using EMD method.

[1] Knight tour algorithm

The traditional EMD method uses a sequential selection of the groups used for embedding the knowledge within it. This is often considered one among the weaknesses because the hacker can simply extract the key message from the image. Hence, it's essential to discover methods that utilize an arbitrary selection like Knight tour algorithm and arbitrary function. After dividing the duvet image into blocks, 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's difficult to spot the blocks and therefore the groups that have the knowledge within it just in case an unauthorized person receives it. this system is employed to reinforce the suggested scheme's robustness and to avoid the normal 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 embed ding the knowledge .
- **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 within the cover image and n represents the amount of pixels within the group and w represents the amount of groups in the row while, h represents the amount of groups within the column.

- **Step 2:** the duvet image is represented as a chessboard of size (p*q) blocks where, p represents the amount of blocks within the row and q stands for the amount of blocks within 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 subsequent block that has the groups used for

embedding as: if the present block (b(i,j)) subsequent block is selected throw the direction of movement as:

- If b (i + 1, j + 2) didn't practice in embedding the information within the groups and that i + 1 < p ; j + 2 < q then b(i + 1 , j+ 2) is selected; i = i + 1 , j + 2.
- else if b(i + 1 , j-2) didn't practice in embedding the information within the groups and that 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) didn't 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) didn't 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) didn't 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
- **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 chosen blocks are finished

[2] EMD method

In this method, (2n + 1)-ary encoding system is used to represent the mystery digits that are embedded within the duvet 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

$$ek(\rho i) = (\rho i + kx_{(i \bmod m)} \text{)mod1} \quad (2)$$

where, (g1, g2, ..., gn) represents the values of the pixels inside the group; while, (n) represents the amount of pixels in each group. Following that, compare the worth of (f) and therefore the value of the mystery digit (d). it's not necessary to vary the worth of pixel if f = d because the worth of the mystery digit is like the estimation of the first pixel otherwise the worth of image indi cator (s) is computed using Eq. (3) (Zhang and Wang, 2006):

S=d-f.mod(2n+1) (3)

Later, if the estimation of (s) is fewer than or like (n) then the pixel value (gs) is increased by one alternatively decrease the worth of (g2ns) 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 amount of pixels within 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 (gi _ i) mod (2n + 1)
  end loop i
- **Step 5:** if f – d then s = d _ f mod (2n + 1)
- **Step 6:** if s _ n then gs increased by 1 else g(2n+1-s) decreased by1.
- **Step 7:** m = m +1
- **Step 8:** end loop m

[3] 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).

$$f = f(g1, g2, \ldots gn) = [\sum_{i=1}^{n}(gi \quad \times i]) \text{mod1(2n+1)}$$

where ci 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
- **Step 3:** determine the blocks and therefore the groups using Knight tour and arbitrary function using an equivalent steps utilized in the embed ding process.
- **Step 4:** for i = 1 to n
  d = sum (g0i 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 attend 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 let ter by using Huffman coding
- **Step 13:** Vigenere cipher is employed to decrypt the message and achieve the plain text

III. RESULT

The major goal behind this study is to hide an outsized quantity of information with a high security and preserve the image quality at an equivalent time. MATLAB 2013a was utilized as a programming language and 6 images of size 512*512 pixels were taken from USC-SIPI Data Base (USC-SIPI) and wont to evaluate the suggested scheme as has been widely employed by researchers within the field of information hiding and giving accurate leads to terms of quality. Fig. 1 shows the pictures which were utilized in this study.

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

Assume that the mystery message to be encoded written using
the characters of English alphabet is (university of mosul) and the keyword is (vector). Here, the length of the alphabet is adequate to 26 and every character has 26 possible replacement characters according to its position within the message and therefore the key. Following that, determine the vectors of key as integers where key = (21, 4, 2, 19, 14, 17) and therefore the length of the key's adequate to 6. Here, the vectors of key are repeated until they match the length of the mystery message.

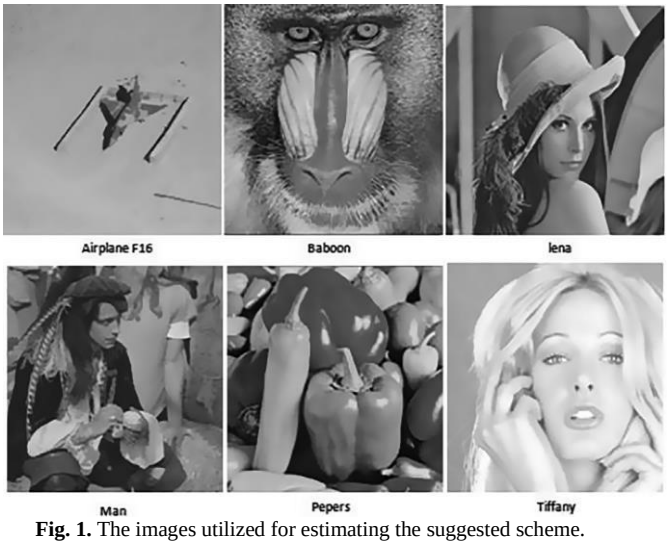


Fig. 1. The images utilized for estimating the suggested scheme.

To encode the mystery message using the key and depending on Eq. (1), the primary character u within 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 within the encrypted

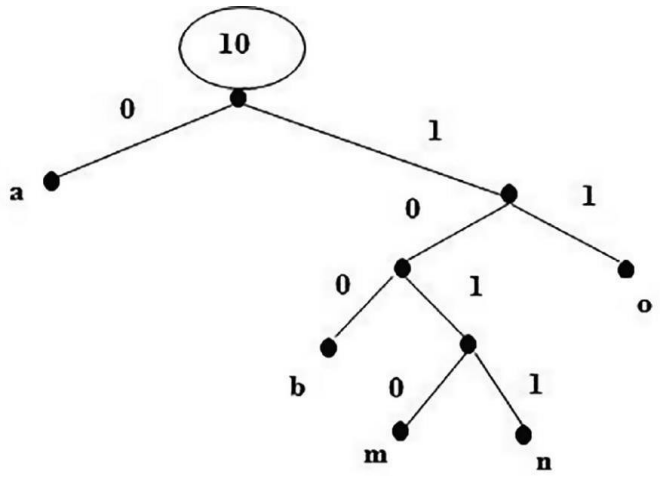
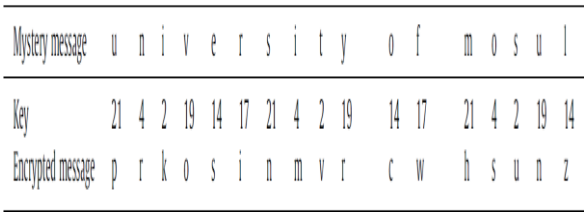


Fig. 2. Huffman tree.

As a result of the encryption process, the mystery message (universityof 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:

- Step1: input the encrypted message (aboamanabo)



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 stegnoimage hose value is calculated by utilizing

$$MSE= \sum_{I=1}^{M*N}(GI - GI)^{2}/(M*N) \quad (6)$$

where gi is a pixel value before inserting the information within the image and g0 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

TABLE I

HUFFMAN DICTIONARY TABLE.

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

.

TABLE II

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
32,768 byte	37.5	6144

$$PSNR=10log_{10}\frac{max}{MSE} \quad (7)$$

where, max signifies the maximum value of pixels in the image.Structural Similarity Index Metric (SSIM) is utilized to evaluatethe likeness among the cover image and the stego-image (Wanget 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):

where, mx and my are mean values of cover image (x) and stegoimage(y) and rx and ry are standard deviation values of the cover image and stego image while, rxy means the covariance of both two images. c1 and c2 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:

$$ER = \frac{P}{M*N} \quad (9)$$

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

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

Payload	Images dataset		
	Measures	Lena	Baboon
52,400 byte	PSNR	55.69	55.70
	MSE	0.20	0.20
	SSIM	0.91	0.91
49,152 byte	PSNR	55.96	55.98
	MSE	0.17	0.17
	SSIM	0.94	0.94
32,768 byte	PSNR	57.77	57.76
	MSE	0.11	0.11
	SSIM	0.97	0.97
16,384 byte	PSNR	60.74	60.81
	MSE	0.06	0.06
	SSIM	0.98	0.99

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.

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

Methods	Payload	Embedding rate (bpp)	PSNR value	
			Lena	Baboon
Proposed Method	52,400 byte	1.59	55.69	55.70
Opt EMD			overflow	
EMD			overflow	
LSB			overflow	
Proposed Method	49,152 byte	1.5	55.96	55.98
Opt EMD			52.11	52.11
EMD			52.11	52.11
LSB			45.91	45.92
Proposed Method	32,768 byte	1.0	57.77	57.76
Opt EMD			54.67	54.66
EMD			53.86	53.87
LSB			51.14	51.14
Proposed Method	16,384 byte	0.5	60.74	60.81
Opt EMD			58.37	58.38
EMD			56.88	56.89

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. 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.

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.3-6show the comparison by using the method of x2 on the original image (lina), and on the same image after embedding

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

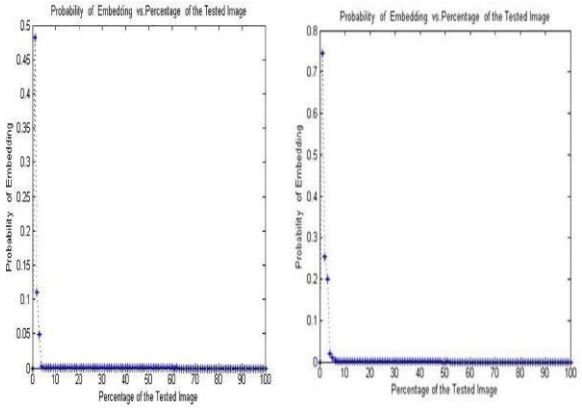


Fig. 4. The result of generating x2 method on LINA image before and after embedding process using the suggested scheme.

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 (lina) 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.

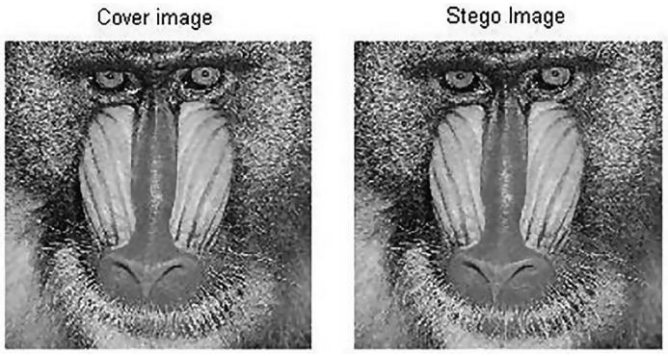


Fig. 5. Baboon image before and after embedding process.

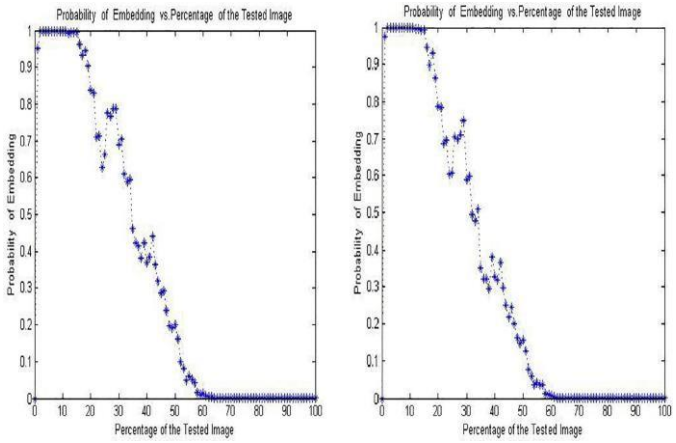


Fig. 6. The result of generating x2 method on Baboon image before and after embedding process using the suggested scheme.

III. CONCLUSIONS

The major goal of steganography schemes is to hide an outside amount of data within picture without affecting the image quality. Additionally, the robustness and the security of those schemes provide protection against electronic attacks. In this study, a completely unique scheme has been suggested to cover the information within images by merging cryptography and steganography methods using four techniques. Firstly, the key message contents are encrypted using Vigenere cipher so as to guard data and to increase the saftty of the suggested scheme. Then, the encrypted message is compacted using Huffman Coding methods to attenuate the message size and to extend 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, x2 method is used for evaluating the robustness of the suggested scheme against electronic attacks. The empirical results show that the standard 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 check the tactic through generating other electronic attacks and also, it is possible to use other methods for random selection.

REFERENCES

[1] Afrakhteh, M., Ibrahim, S., 2010. Enhanced least significant bit scheme robust

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

[3] Chan, C., Cheng, L., 2004. Hiding data in images by simple LSB substitution. Pattern

[4] Recogn. 37, 469–474. https://doi.org/10.1016/j.patcog.2003.08.007.

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

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

[7] Habibi, M., Karimi, R., Nosrati, M., 2013. Using SFLA and LSB for text message

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

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] Ranjani, J., 2017. Data hiding using pseudo magic squares for embedding high payload in digital images.

[17] 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.

[18] 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.

[19] 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.

[20] 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.