QUATERNİON SECURİTY USİNG MODİFYİNG VERNAM CİPHER WİTH İMAGE STEGANOGRAPHY

Huda H.Al.ghuraify[1], Dr.Ali A.Al-bakry[2], Dr. Ahmad T. Al-jayashi[3]

[1]Engineering technical college, Al-Furat Al-Awsat University, Iraq
[2]Dean of engineering technical college, Al-Furat Al-Awsat University, Iraq
[3]Assistance dean of engineering technical college, Al-Furat Al-Awsat University, Iraq

ABSTRACT

The Internet is the essential wellspring of data in the present life where it offers the trade of data to the clients.The exchange of such data prompts an incredible security danger. Cryptography and steganography are two issues in security systems.Cryptography jumbles the message to be incomprehensible While Steganography shroud the message To be invisible. Therefore, Encryption any private data before concealing in the cover object will provide twofold security. This paper presents a technique for disguise message with four levels of security where the message first encrypt using modifying vernam cipher, in which the initial key originate automatically from random pixel of camouflage cover and alter continuously along message length then embedded cipher message in grayscale cover image, after that encrypt this cover using modifying vernam cipher also then embedded it in RGB color cover image. The simulation consequence illustrates that the scheme provides better protection.

KEYWORDS

Image steganography , modifying vernam cipher , message security, dual cryptography , spatial domain

1. INTRODUCTİON

In the current movement of the universe, the technologies have innovative so much that numerous of the persons favor utilizing the internet as the fundamental media to transfer data from one zone to another. There are various feasible methods to transmit information utilizing the internet such as chats, e-mails, etc. The information transfer is accomplished extremely simple, quick and accurate utilizing the internet. However, one of the foremost conundrum with dispatch data over the internet is the security menace where the private data can be hooked in several ways. Therefore, it becomes significant to take information security as one of the most important factors that require care during the information transmitting[1].

Cryptography and steganography are intimately associated procedure where the objective of these techniques is supplied information security and secure communicating[2].The aim of cryptography is to supply safe communications by altering the information into a fashion that cannot be comprehended[3].Essentially, it comprises a layout of protocols being founded on the realm of mathematics, computer scientific discipline, and electrical engineering to cipher and decode data in the state of information and images[4].

Cryptography algorithms categorize into Symmetric cryptography that utilizes private key, and asymmetric cryptography that utilizes private and public keys together[5].One of the restrictions of cryptography lies in the fact that the encoded information can generally be noticed during the transmitting which may allure malicious clients to perform progress examination which may

DOI:10.5121/ijma.2019.11301

guide to its harm or modification[6].Figure 1. demonstrate a common form of Cryptographic System.

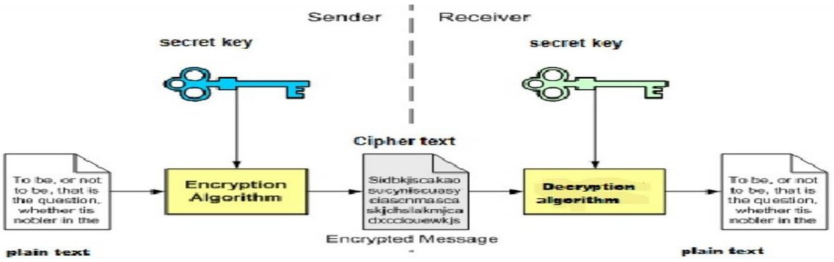


Figure 1. common form of Cryptographic System[7]

On the other hand, Steganography is a prominent branch of data disguise, where private contents are hiding in carrier file such image to hide its existence without deformation in a carrier.The term steganography is a derivation from Greek and denotes"covered, or hidden writing"[8].Basically, steganography mechanisms classify into six types: text, video, image, protocol, audio, and DNA steganography technique [9].

images could be vigorous host to conceal data because of the capacious spaces that it presents. Furthermore, vary in images are commonly imperceptible to an exposed eye[2].numerous researchers utilize the Least Significant Bits algorithms (LSB) to diminish the distortion into the stego-image[10].Figure.2 illustrates common Principle of Image Steganography System where The sender aims to transmit a private message to the recipient, therefore select a cover file (c) to hide the private message (m). The stego file (s) which necessary be indistinguishable from the cover file (c) where The stego file (s) correspond to the cover file (c) with the private message (m) which is concealed inside it. In order to intensify the security of the sender, the stego key (k) is utilized[11].

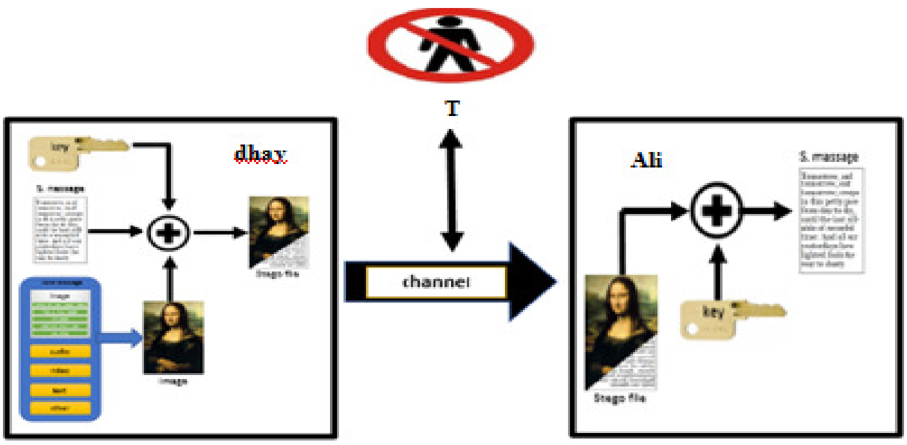


Figure 2. common Principle of Image Steganography System[11]

The incorporating of cryptography with steganography is quite prominent to preserve the balance of data occupies in the image where Steganography goal to deceive someone's outlook of particular data. But if the outlook is inferred existence the information, cryptography will arrogate to preserve data security [12].

in this paper ,a new method for security of message using modifying vernam cipher with image steganographyis proposed Where the secret message encrypted first using modifying vernam in which the initial key originate automatically from most significant bit (MSB) of a random pixel of camouflage cover image and alter continuously along message length then embedded cipher message in hybrid cover, first grayscale cover and then after encrypting it with modifying vernam cipher embedded it in RGB color cover thus provide four levels of security to the embedded private message.

The other sections of the paper are formed as pursue: In Section 2 demonstratesThe literature survey.Section 3 explains vernam cipher. Section 4 describes the measurements of appraising the performance of steganography technique. Section 5describes the measurements for evaluating the performance of encryption quality.Section 6 illustrated The Proposed algorithm. The Simulation results are demonstrated in Section 7. Section 8 explains performance comparison and Finally, Section 9clarify the conclusions follow the pertinent references.

2. LİTERATURE SURVEY

A. Setyono, et. al.[5]proposes a technique for Secure Image Transmission utilizing two cryptography algorithms that are RSA and Vernam algorithms. The Vernam cipher is accomplished after RSA cipher because of the idea that Vernam cipher can make the image random better than RSA . the proposed technique necessitates three inputs as follows : image , the key of RSA algorithms and the key of Vernam algorithms. the results that obtained demonstrate that the proposed techniques improved image security where the size of the original image is double after encryption.

W.Fitriani ,et .al.[12]Propose a method that combines the cryptography technique with steganography technique to embed a secret message in RGB color cover image. In this strategy, a series of characters of the secret message will be changed to byte code and then applying Vernam cipher to it with a secret key that allocate previously after that every byte of cipher message will be embedded at the end of the RGB color cover image at each channel where replace the byte of channel with byte from a secret data. The same key of encryption being repeated to encrypt the entire plain text and thus must exchange between the communicated party to extract the secret message exactly.

M.T.Sharabyan and H.Ghorbani[13]Propose a secure manner for the privacy information utilize the Imperialist Competitive with symmetric cryptography where first, cipher the secret information as the following depicts : The text is utilized as secret information where first transform it into characters array then to bits,and afterward encodes the information bits utilizing symmetric encryption key of 128-bit. The bit array of a secret text is separated into (64 bit) length then the two parts of (64 bit) length which is 128-bit, is accomplish XOR with an encryption key which is 128-bit , subsequent, take half of the encrypted part (64 bit) with the half of other part of an array (64 bit) and accomplish XOR with an encryption key(same key of 128 bit).This step continues until the encryption operation of the array is completed.Then utilize The Imperialist Competitive Algorithm as a key to conceal a secret data in the cover images of grayscale type based on the LSB method. The proposed scheme elevate the security of private information and promote the quality of the stego image and also give it immune to attacks.

V. Yadav and S.K.Sharma [14]utilize a new technique for implement steganography based on a cover image of HSI color with canny edge detection technique based on the threshold where conceal private message utilize 2-bit LSB substitution in the edges of the camouflaging cover. The amount of secret message that is concealed plays a significant job on the determination of edges where Based on the size of a secret message, the threshold can be adjusted. When the secret message is very long then select high threshold value to accommodate the message in edges in an effective manner where The value of high threshold parameter depicts that there are powerful edges present while low edge portrays that there is moderately low edges are available in an Image. The results demonstrate that the proposed technique efficaciously convert images into some other shape where the private message is camouflaged.

G.S.Charan ,et. al.[15]propose Novel approach based LSB With Multi-Level Encryption for image steganography where encrypting the plain text into two platforms, during the first platform it is encrypted utilize Ceaser cipher where each letter of plain text is supplanted by another letter at distance specify by given key and in the second platform it is encrypted utilizing chaos theory where the chaotic sequences created from various initial conditions that are free of one another and each part of secret data is encrypted with various initial conditions subsequently all parts are converged into cipher text then the cipher text embedding into a color image using 3, 3, 2 LSB where first 3 bits of ciphers are substitute with(3 LSB) bits of red channel, next 3 bits of ciphers are substitute with (3 LSB) bits of green channel, and last 2 bits of ciphers are substitute with (2 LSB) bits of blue channel.

M. Junejaand P. S. Sandhu[16]Propose a scheme that incorporates cryptography and random pixel conceal to achieve high resistance to attacks. The proposed algorithm integrating Hybrid feature detection technique that incorporates Canny and Hough transform for branched an image according to the edge and smooth region then utilize LSB Technique for concealing encrypted messages with AES in these regions.The procedure for implemented this method as the following depicted : Extraction of Edge and smooth areas from Input cover image by utilizing integrating Hybrid feature detection technique that incorporates Canny and Hough transform where using an enhanced of Hough transform algorithms by merging the classical with generalized of Hough transform for extract lines , circles and edge boundaries.the Secret text message is encrypted firstly utilizing AES then concealing the encrypted secret message randomly where using Two Component -based (LSB) Substitution Technique For edge areas and Adaptive (LSB) method For smooth areas.

D. Adiyan, et. al.[17]incorporate steganography with vigenere cipher to achieve Secure Steganography based on LSB algorithms .in proposed style utilize vigenere table to acquire encrypt text from plaintext where the character on the plaintext list into rows, and the character on the key list into columns Thus can get ciphertext from plaintext and a secret key by utilizing vigenere table then conceal encrypted text in the image using LSB algorithm. The secret message that encrypted with utilizing vigenere cipher in sending part need to processed again after extracted from the stego image in receiving part where utilize vigenere table again with a secret key to acquire the plaintext that represents a secret message.

P. Srilakshmi, et. al.[18]proposed image steganography technique in the spatial domain for text concealing where the text is embedded into the image based on reference according to the key, the retrieve of text is only attainable when the key is recognized. The proposed work is considered as the advancement of LSB method and Pixel Indexing method That utilize one of the color matrices as the key to point out where the secret message is concealed into the cover image. the result demonstrates that the proposed method is secured and complex to distinguish the data embedded into the image.

Table 1 describes the comparison of the proposed algorithm with other algorithms that utilize encryption for the secret message then concealing as explained it above.

Table 1. comparison of the proposed algorithm with otheralgorithmsin Literatures survey

ref	Type of secret data	Type of cover image	Embedding domain	algorithms	Type of security for secret data Before steganography	Comments on algorithms
[12]	Text message	RGB color	Spatial domain	embedded data at the end of the RGB color cover image	Vernam cipher with a secret key that allocates previously	The key that allocated repeated to encrypt the entire message
[13]	Text message	grayscale	Spatial domain	LSB algorithms with the Imperialist Competitive	symmetric encryption with a key of 128-bit	The key allocated previously
[15]	Text message	RGB Color	Spatial domain	3, 3, 2 LSB algorithms	utilize Ceaser cipher then encrypted utilize chaos theory	Require a secret key for Ceaser cipher and initial conditions for chaos theory
[17]	Text message	either RGB Color or grayscale	Spatial domain	LSB algorithms	vigenere cipher	Require utilizes vigenere table again with a secret key to acquire the plaintext at receiving side
Proposed method	Text message	Both RGB cover and grayscale cover	Spatial domain	LSB algorithms	Doul cryptography of Modifying Vernam cipher One for a secret message and other for grayscale cover	Create secret key based on the initial key that originates automatically from camouflage cover image

3. VERNAM CİPHER

Vernam cipher is an encryption manner that is performed by convert each bit individually with other bits utilize XOR manner where each bit from the private message will be XOR operation with another bit from the secret key. The decoding procedure of a secret message is realised by the task of XOR between the encoded message and the secret key [12].It can be the unsolved algorithm if it specifies the following express.first, the key span along the length of the message. second, the utilized key ought to be random and third should be utilized onlyone time[5].

4. MEASUREMENTS OF APPRAİSİNG THE PERFORMANCE OF A STEGANOGRAPHİC TECHNİQUE

For appraise the performance of stego image with regard to cover image, numerous parameters have been deliberated such asMSE,PSNR,Er and SSIM[19]as explained below:

4.1. Mean Square Error (Mse)

the average of the deviation between the cover image without private data and the cover image with private data.the lowest value of MSE is desired[20]. The MSE is given as follows in eq.(1)

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[Cover(i,j) - Stego(i,j)]^2 \quad \dots\dots\dots\dots\dots (1)$$

Where:

Cover(i,j) :stand for original image before embedded secret data;Stego(i,j) : stand for original image with embedded secret data ;M : represent number of rows; N:represent number of columns.

4.2. Peak Signal-To-Noise Ratio (PSNR)

PSNR describes the comparison between the greatest energy of a signal and the rumpus influence its characteristics. Great PSNR value commonly demonstrates great image characteristic, while lesser PSNR value demonstrates a lesser characteristic [21].PSNR will be computed utilizing the eq.(2)

$$PSNR = 10\log_{10}\frac{P^2}{MSE} \quad \dots\dots\dots\dots\dots (2)$$

Where:

p^2 is the greatest value of the pixel in an image.

4.3. Embedding Capacity

It is aprominent indicator to evaluate steganography method. It represents the amount of private data disguised in the cover image to the number of pixels belong to that cover. It denominates as embedding rate [22]and calculates as follows in eq .(3)

$$\frac{\mathrm{S}}{\mathrm{W} * \mathrm{H}}\,\mathrm{bpp} \quad \dots\dots\dots\dots\dots (3)$$

Where:

S: represent secret data embedded into the cover image ; W , H : represent the size of a cover image.

4.4. Structural Similarity İndex Metric (SSIM)

SSIM intend to appraise characteristic by comparing the closeness between images[23].A good stego image should be capable to produce a numerical quantity of SSIM that is approximately 1. the SSIM can be computed according to eq .(4) below

$$SSIM(C,S) = \frac{(2\mu_C\mu_S + c_1)(2\sigma_{CS} + c_2)}{({\mu_C}^2 + {\mu_S}^2 + c_1)({\sigma_C}^2 + {\sigma_S}^2 + c_2)} \quad \dots\dots\dots\dots\dots (4)$$

Where:

C and S: refer to reference and test image respectively .In this case reference image stand for cover image and test image stand for stego image ; σ_c and σ_s: refer to a standard deviation of C and S respectively ; $\mu_c$and μ_s: stand for mean value of C and Srespectively ; c_1 , c_2 : stand for stabilization constant ; σ_{cs} : indicate the correlation betweenC and S

5. Measurements For Evaluatİng The Performance Of Encryptİon Qualİty

The consequence of test encryption quality will be deliberated by utilizing entropy value , SSIM and histogram analysis [24].as explain below:

5.1. Entropy

In a system, The data entropy is characterized as locution the level of uncertainty of the system data.if the system is deliberate as an image, the data entropy is characterized as locution the level of the irregularity of the image data. Data entropy basically evaluates the distributing of the gray level of pixel values in an image. The data entropy estimation of an encoded image ought to be near the value 8[25] . the formula for depicting data entropy is as pursue in eq .(5)

$$E(n) = -\sum_{i=0}^{255} p(n_i)\, log_2\, p(n_i\,) \ldots\ldots\ldots\ldots\ldots\ldots (5)$$

n : the data source ; $p(n_i)$: the probability ofthe symbol n_i ; E(n) : the data entropy.

5.2. Histogram

The histogram represents the distributing of pixel quantities in an image. proper encryption consequence should produce the distributing of pixels comparatively alike [24].

5.3. Structural Similarity İndex Metric (SSIM)

SSIM can be utilized to gauge the nature of image encrypting. This numerical quantity is acquired by contrasting the reference image and the encoded image. The resultant value scope of SSIM is 0 to 1. A proper encrypting consequence ought to almost certainly produce an estimation of SSIM that is approximately 0, which implies that the encrypting consequence has no likeness to the reference image[24].The equation for computing the SSIM has demonstrated above in eq .(4).in this case, the reference image stands for the image before encryption and test image stand for the encrypted image.

6. The Proposed Algorİthms

6.1. Sending Part

The proposed scheme includes four stages, first of it utilizing modifying vernam cipher for private message to encrypt it, the second stage is concealing private message in a grayscale cover image to provide the second level of security and the third stage is utilizing modifying vernam cipher to encrypt a grayscale image then concealed it inside a color cover image of any size utilizing LSB algorithm in the spatial domain. Figure 3demonstrates the sketch that proposed for protection secret message at sending side.

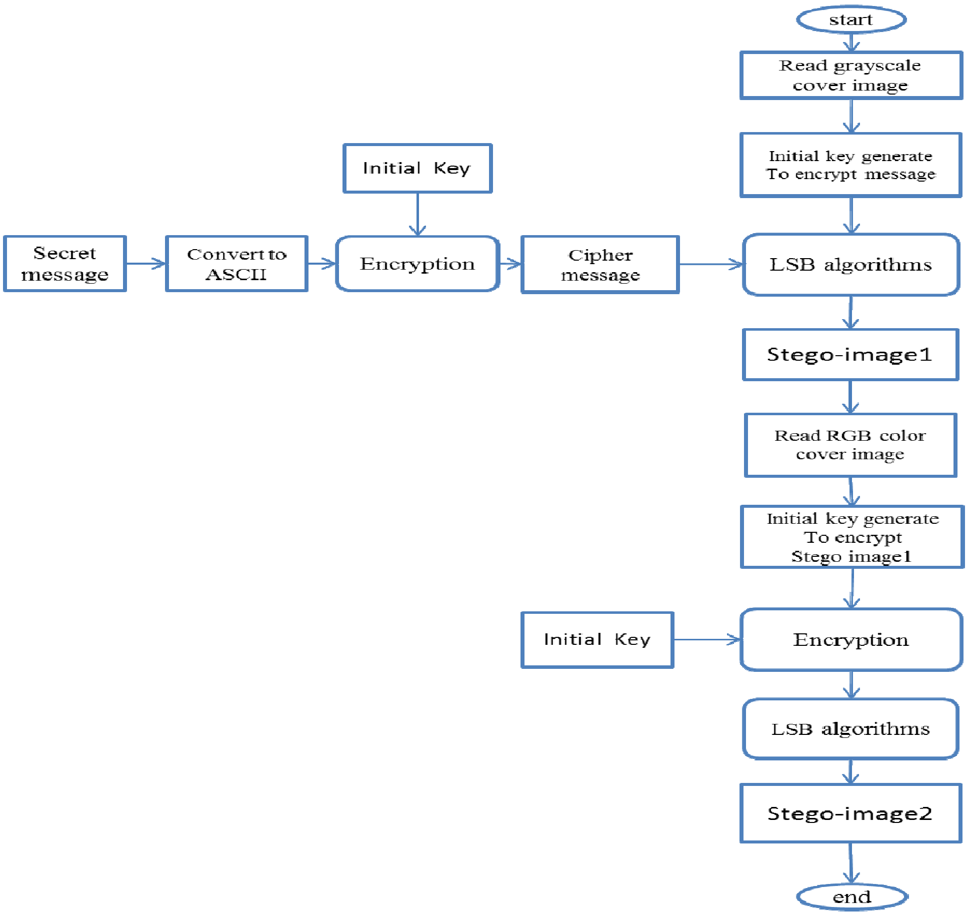


Figure 3. Block Diagram at sending side

6.1.1. The Steps that Accomplish at Sending Part

RGB cover image, grayscale cover image , and the private message are utilized here.
The steps of procedure:

1.Read the grayscale cover image.
2.Read the private message then convert it to ascii .
3.Generate an initial key for a secret message from the random pixel of a grayscale cover image using msb of that pixel as the illustration below:

a. Select a random pixel of the gray cover image then shift the msb of that pixel to right thus clear lsb of that pixel.
b. Return msb to the first position by shifting it to left then display the value of it to represent the initial key.
c. Apply circuit shift by one position to alter the value of initial key according to the length of the secret message and if the value of it reach initial key again increased it by one then this increased value represents second initial key and continue until reach value of 255 to reallocate another random initial key as explain below in figure 4:

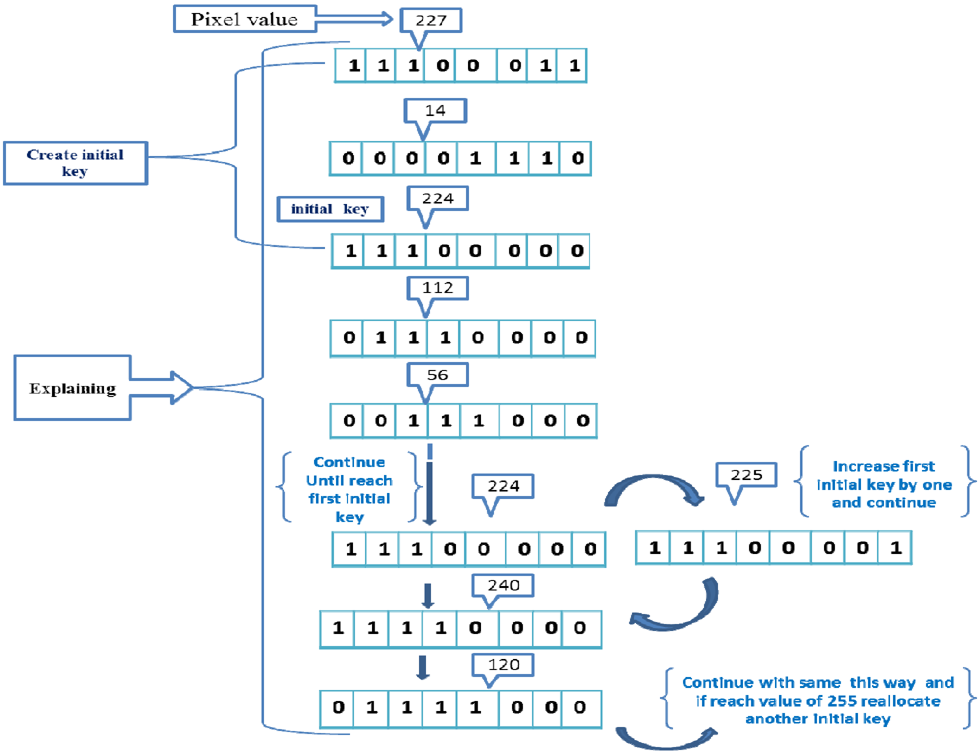


Figure 4. description of creating an encryption key

4.Convert the format of a gray cover image to a binary format to form (($r_{(\text{row of gray cover})}$ ×$c_{(\text{column of gray cover})}$) x 8).
5.Convert private message to binary format to form (($r_{(\text{row private})}$ * $c_{(\text{column private})}$)* 8).
6.Apply encryption to a private message of the binary format by utilizing modifying vernam cipher with a secret key that generates initially from grayscale cover image and extends along message length.
7.Each bit of encrypted private message will be concealed in a gray cover image utilizing LSB algorithms to form stego image 1.
8.Read RGB cover image then converts it to a binary format.
9.Separate channel then generate an initial key for encrypting stego image 1 from the random pixel of one channel by using MSB of that pixel as explaining it above.
10.Each bit of encrypted stego image1 will be concealed in an RGB cover image utilizing LSB algorithms in the spatial domain where utilize LSB of two channel of RGB color cover.
11.Write RGB stego-image 2 to the selected location utilizing BMP format.

6.2. Receiving Part

The RGB stego image 2 is utilized as the origin for the extraction stage to extract the private message without the need for an RGB cover image. Only the following data are necessitated in order to extract the private message exactly:

a.the size of the grayscale cover image.
b. the length of the private message.

Figure 5. Demonstrates the sketch that proposed for the extraction of a secret message at the receiving side.

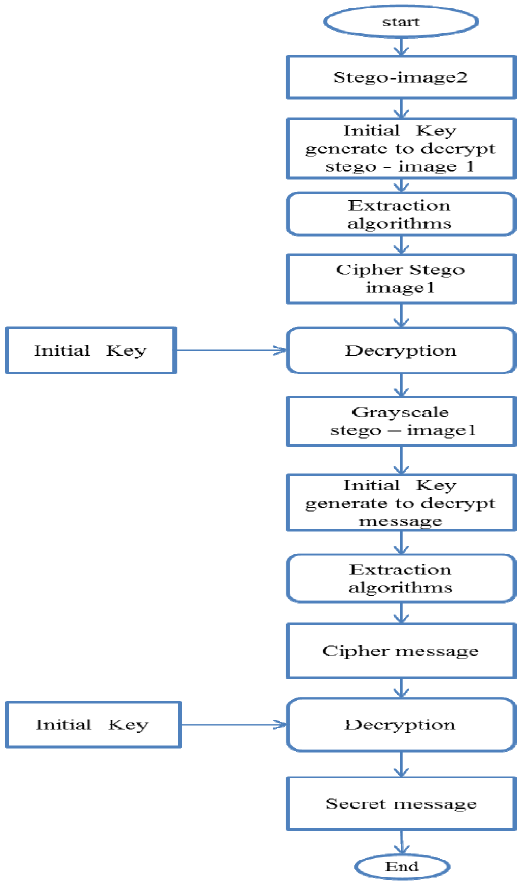


Figure 5. Block Diagram at receiving side

6.2.1. The Steps That Accomplish At Receiving Part

1. Enter the stego image2 to read it.
2. Convert the format of the stego image2 to binary shape.
3. Firstly , Separate channel then generates an initial key from the same random pixel of one channel as that utilizing at sending side.
4. According to the hidden algorithm retrieve the least significant bits from 1 to ((r * c) *8) bits for stego image 1.
5. The retrieved data form according to $((r * c)_{retrieved}/8)$ rows and (8) columns.
6. Converted binary bits form to decimal fashion according to (r, c) .
7. reshape image to form an entire stego-image1.
8. decrypt stego image1 utilizing the initial key that generates and extend along with image size as depicting the procedure of it at the sending side.
9. Generate an initial key from the same random pixel of decrypted stego image 1 that utilize at the sending side to decrypt the secret message .
10. According to the hidden algorithm , the least significant from 1 to the length of message bits retrieve for a secret message then decrypt the secret message using the initial key that generates and extend along with message size as depicting in sending side then convert it to a character.
11. Write a private message to a text file.

7. SIMULATION

7.1. Setup

The proposed algorithm was implemented utilizing MATLAB Version (R2017a) with a PC of description that exhibits as pursues:

Table 2.description of pc

PC description	detail
Processor portray of PC	Core(TM) i7-2630QM CPU @ 2.00GHz and RAM-6Gbytes

7.2. Dataset

Table 3. dataset for test proposed algorithms

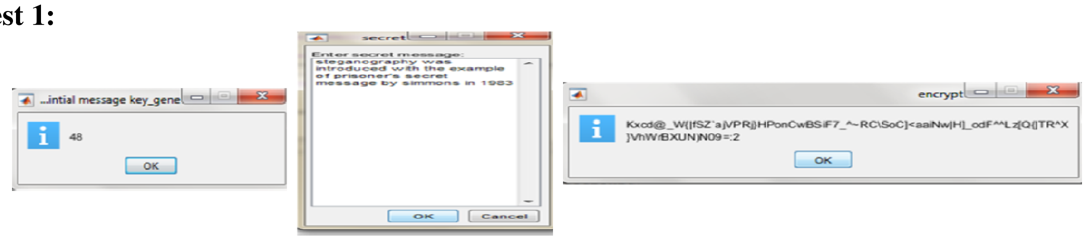
data	type	Details
Cover image2	RGB color	Test 1 : size 800×600×3 and of .jpg format [26] Test 2: size 1024×768×3 and of .jpg format[27]
Cover image 1	Grayscale	Test 1 : size 284×177 and of .jpg format[28] Test 2 : size 292×173 and of .jpg format [29]
Private message	"Steganography was introduced with the example of Prisoner's secret message by Simmons in 1983"[30]	

7.3. The Resultsand Discussion

7.3.1. Sending Part

As depicted from the visual quality of cover image 2 of RGB color type and stego image 2 of RGB color type can surmise that the achievement of the steganography scheme for disguising private data can't be recognized where cover image 2 and stego image 2 comparable at sending side. Figure 6 and Figure 7 Exhibit Sending part utilizing both RGB and grayscale images as cover to shape stego image where the private data first encrypted utilize modifying vernam cipher with initial key that generated automatically from random pixel of grayscale cover image and then embedded it in that cover to form first stego image after that encrypted this stego image 1 utilizing modifying vernam cipher also with initial key that generated automatically from second cover image of RGB color type then embedded cipher form of stego image 1 in that cover to form stego image 2 as demonstrated below:

Test 1:



a.secret message before and after encryption it

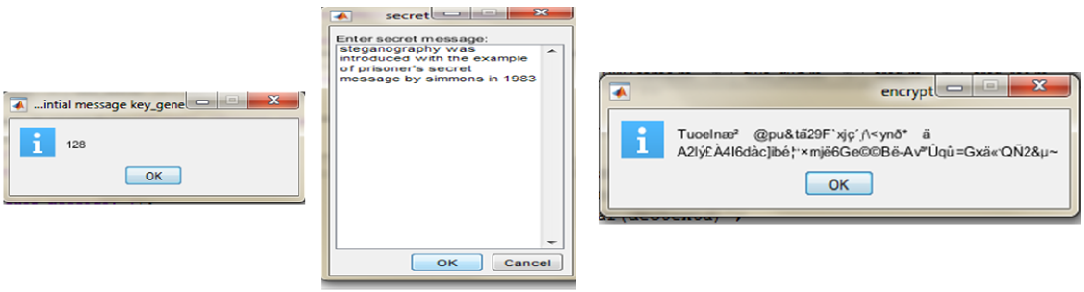
b.grayscale stego image1 before and after encryption it

c.dual cover image to hide a secret message with stego image2

figure 6.Steps of shape stego image2 using RGB and grayscale images as cover

According to figure 6, the data encrypted with two symmetric encryption key one of them for a secret message and other for a stego image 1 without necessitate exchanging encryption keys between communicating party for retrieve a secret message precisely where the encryption key create automatically depend on the initial key and This procedure is extremely significant in cryptography systematic where if the sender need to alter the encryption key don't require to exchange the new key to receiver side thus get rid of pilfer key by attacker and also consume the time that necessitate to reciprocation the secret key.on the other hand, the length of key a long data length provide preferable robustness to a secret data.

Test 2:



a. secret message before and after encryption it

b. grayscale stego image1 before and after encryption it

c.dual cover image to hide a secret message with stegoimage 2

figure 7.steps of shape stego image 2 using RGB and grayscale images as cover

According to the consequence of the encrypted data in test 2 deduce that each time change the initial key of cryptographic algorithms result in alter the entire encryption key and this exhibit clearly in result of cipher message where the same message utilizes in two test but the cipher of it be different from one test to another where when initial key be 48 in test 1 lead to cipher message differ from the cipher that acquire when initial key 128 in test 2 and this proves that each secret message can encrypt it with different cryptographic key dependent on initial key thus can create a new key for each secret message utilizing different grayscale cover image with a new initial key. The same approach is applicable for stego image 1 where can create a new key for each stego image 1 using different RGB color cover image with a new initial key.

Table 4 demonstrates the performance of proposed algorithms according to steganography system measurement as depicted below :

Table 4.performance investigation according to steganography system measurement

RGB color cover size	Grayscale cover size	Message length	Test	MSE	SSIM	PSNR/db	Elapsed time At sending part	Elapsed time At receiving part
800*600 (24bpp)	284*177 (8bpp)	94 * 1 char	Test 1	0.14046	0.9999	56.6553	22.501194 seconds	20.664334 seconds
1024*768 (24bpp)	292*173 (8bpp)	94 * 1 char	Test 2	0.086175	0.99994	58.777	28.990121 seconds	24.970278 seconds

According to table 4 deduce that value of PSNR value magnifies and value of MSE diminish as enlarge the size of RGB cover image and this explicitly appear in test 2 when increasing the size of RGB color cover image and test the performance according to steganography system measurement.

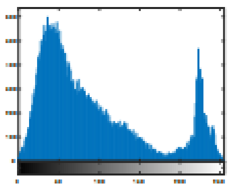
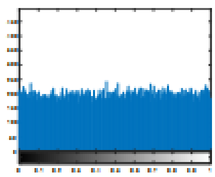
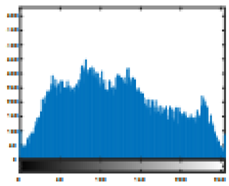
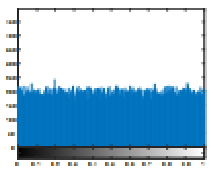
Table 5 and Table 6 evaluating the performance of the encryption algorithm of grayscale stego image 1 as depicted below :

Table 5. performance investigation according to the encryption quality of stego image1

Grayscale cover size	Test	SSIM	Entropy	Initial key
284*177 (8bpp)	Test 1	0.0064238	7.9963	160
292*173 (8bpp)	Test 2	0.007761	7.9972	224

According to table 5, the encrypting consequence has better execution where entropy value near 8 and SSIM value is near 0 and thus demonstrated that the cipher image doesn't supply any data about the precisely original image.

Table 6. The histogram of a grayscale stego image 1 before and after encryption

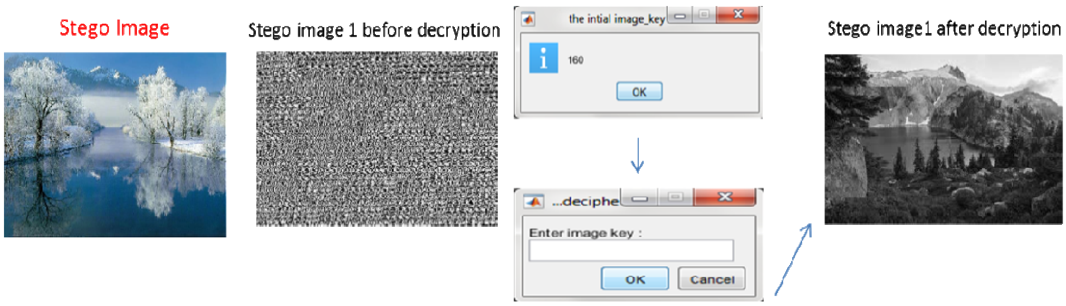
Grayscale cover size	Test	Histogram of image	Histogram of encrypting image
284*177 (8bpp)	Test 1		
292*173 (8bpp)	Test 2		

According to table 6, the histogram that created after the encryption process dissimilar with the histogram of an image before the encryption and yields the distributing of pixels value are approximately uniform level, thus dependent on the histogram conclude proper encrypting quality.

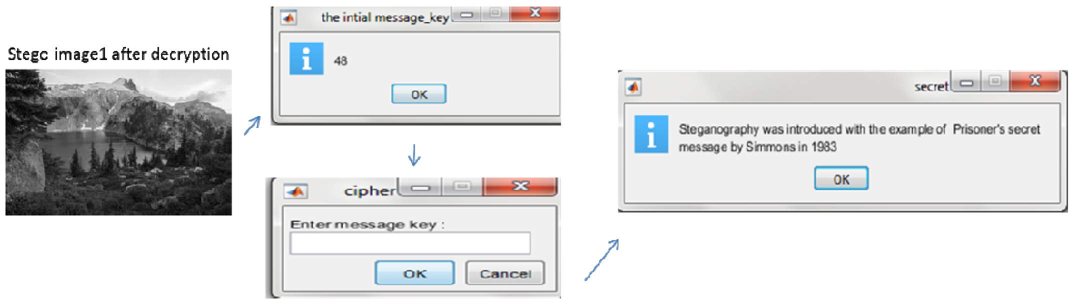
7.3.2. Receiving Part

The nature of the recovered information displays that private information and the recovered information indistinguishable. Figure 8 and Figure 9 exhibit receiving part where first,extract grayscale stego image then decode it utilizes modifying vernam cipher with the same initial key that generates automatically from RGB color cover image to shape first grayscale stego image after that extract mystery message from that image then decode it utilizes modifying vernam cipher with same initial key that originates automatically from grayscale cover image.

Test 1:



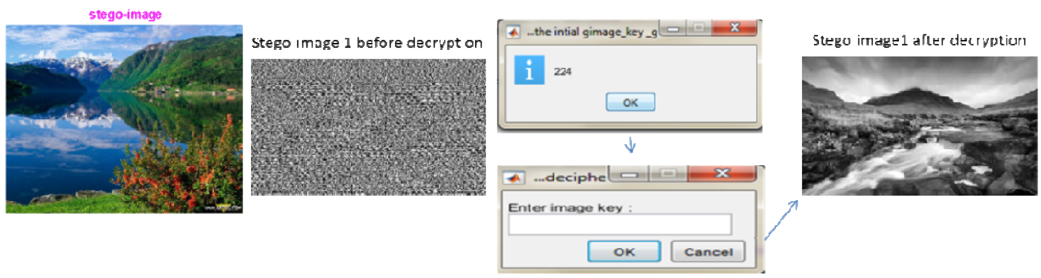
(a).Stego image2 with extract a grayscale stego image1



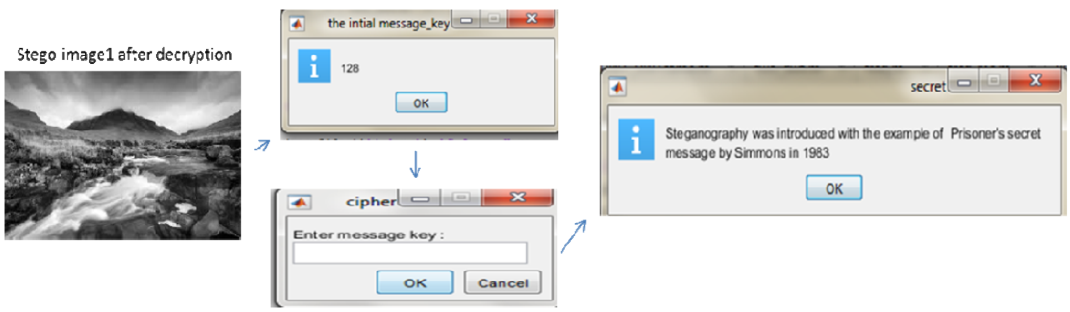
(b).Grayscale stego image1with extract a secret message

Figure 8.Steps to extract a secret message from stego image 2 of test 1

Test 2:



(a).Stego image2 with extract grayscale stego image



(b).Grayscale stego image1with extract secret message
figure 9. Steps to extract a secret message from stego image 2 of test 2

According to figure 8 and figure 9 deduce that the encryption shape of stego image 1 and a secret message respectively decrypted with a decryption key that created based on initial key identical as that utilize at sending side where it originates automatically from MSB of a random pixel of camouflage image without the need to receive decryption key from sender part.

Table 7 exhibit the time that necessitates for implemented an encryption algorithm of secret data at sending part and a decryption algorithm of same data after extracted it at the receiver part.

Table 7. The elapsed time that utilizes for encryption and decryption

Test 1	Encryption time	Decryption time
Stego-image of size(284*177)	3.565391second	3.564936seconds
Secret Message	0.020259 seconds	0.035698 seconds
Test 2	Encryption time	Decryption time
Stego-image1 of size(292*173)	3.598676seconds	3.598117 seconds
Secret Message	0.021036 seconds	0.029035 seconds

According to table 7 infer the time that required to encrypt and decrypt secret data either a secret message or stego image 1 is low, thus depict the better performance of the encryption algorithms.

Figure 10 and figure 11 demonstrate the Relation between magnifying message size and the steganography system measurement (PSNR value and MSE value).

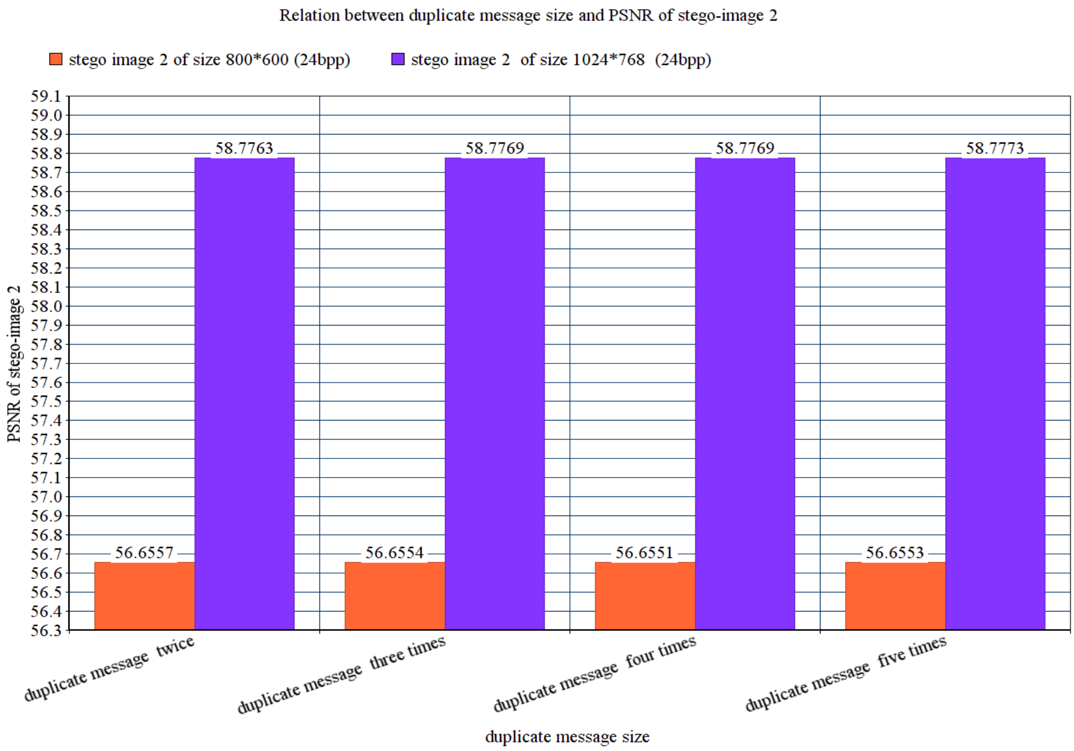


Figure10.The relation between magnify message size and $PSNR_{db}$ of stego image 2

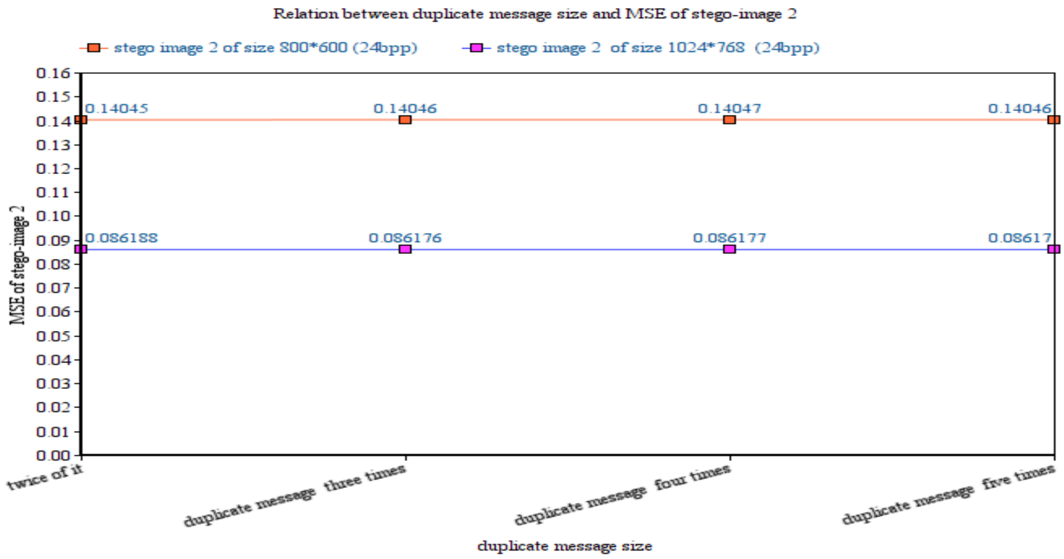


Figure 11 . The relation between magnify message size and MSEof stego image 2

According to figure 10 and figure 11 deduce that increase size of a message doesn't yield effect in term of steganography system measurement of stego-image 2 as illustrated above where the PSNR value and MSE value endure approximately intact unless altering the size of stego image1

8. PERFORMANCE COMPARİSON

Table 8.demonstrate the comparison of appraisal performance of the steganography measurement with another algorithm that explained it in section 2 as follows:

Table 8. Comparison of performance investigation according to steganography measurement

	Image name	method	PSNR	MSE	details of cover image
Text size Length 500	baboon[31]	Method in [15]	56.1872	0.1564	Standard RGB Cover of size (512 * 512)
		Proposed method	56.3464	0.15081	Standard RGB Cover of Size (512*512) grayscale cover of size (172*171)

Figure 12 demonstrates the comparison of appraisal performance of the encryption algorithm with another algorithm that explained it in section 2 where we utilize the entropy as a measure to test the performance of encryption algorithms :

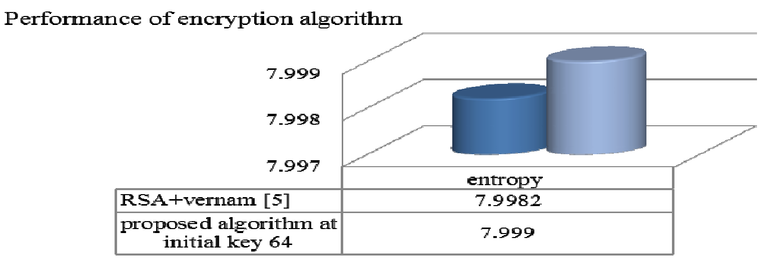


Figure 12 .show the performance investigation of the implemented encryption algorithm

Where :
Test image Mandrill (baboon)[31] which is standard image of grayscale type and size (256* 256)
.

9. CONCLUSİON

In this paper, a technique for veiling message with four levels of security is proposed where utilize two levels of steganography with two levels of cryptography. In each level of cryptography utilize Modifying Vernam cipher with the initial key that originates automatically from a random pixel of camouflage cover. The utilize of Modifying Vernam cipher in cryptography provide three feature as follows, first The initial key is created automatically from the camouflage cover image thus don't need to exchange encryption key. Second Comparable letters in a message are mapped to various symbols where each letter has a diverse key to encrypt it and third It is too difficult to be broken where utilize large random key size along data length. The proposed scheme create better camouflage to evade interloper attention and realize better performance in term of steganographic system measurement as clarifying according to an analysis of performance.

REFERENCES

[1] I. Nehra & R. Sharma, (2015) "Review Paper On Image Based Steganography," International Journal of Scientific & Engineering Research, pp. 1580-1583.

[2] S. D. M. Satar , N. A. Hamid, F.Ghazali, R. Muda,M. Mamat& Pang Kok ,(2016)"Secure Image Steganography Using Encryption Algorithm," Annual Int'l Conference on Intelligent Computing, Computer Science & Information Systems, pp. 43-46.

[3] K.Thakre, N. Chitaliya, (2014)"Dual Image Steganography for Communicating High Security Information," International Journal of Soft Computing and Engineering , vol. 4, no. 3, pp. 7-12.

[4] S.Mukherjee,S.Chakrabarti,S.Sinha&T.Mukhopadhyay,(2017)"A meticulous implementation of RSA Algorithm using MATLAB for Image Encryption," 1st International Conference on Electronics, Materials Engineering and Nano-Technology,IEEE, pp.1-6.

[5] A. Setyono, D. R.I. M.Setiadi & Muljono,(2018) "Dual encryption techniques for secure image transmission," Journal of Telecommunication, Electronic and Computer Engineering, Vols.10, no. 3-2,pp. 41-46.

[6] P.l Maniriho & Tohari Ahmad, (2019) "Digital Image Information Hiding Methods for Protecting Transmitted Data : A Survey," Journal of Communications , vol. 14, no. 1, pp. 9-16.

[7] A. R. Krishna1, A. S. N. Chakravarthy & A. S. C. S. Sastry ,(2016)"A hybrid cryptographic system for secured device to device communication," International Journal of Electrical and Computer Engineering, vol. 6, no. 6, pp. 2962-2970.

[8] P.Khare, J. Singh& M. Tiwari, (2011)"DIGITAL IMAGE STEGANOGRAPH," Journal of Engineering Research and Studies, Vol.II no.III, pp. 101-104.

[9] M.M.Hashim, M. S. M. Rahim, F.A. Johi , M. S. Taha & H. S. Hamad, (2018)"Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats," International Journal of Engineering & Technology, vol. 7, no. 4, pp. 3505-3514.

[10] A. A.Qader & F.AlTamimi, (2017) "A NOVEL IMAGE STEGANOGRAPHY APPROACH USING MULTI-LAYERS DCT FEATURES BASED ON SUPPORT VECTOR MACHINE CLASSIFIER,"The International Journal of Multimedia & Its Applications, vol. 9, no. 1, pp. 1-10.

[11] R.Din , M. Mahmuddin & A. J.Qasim ,(2019)"Review on Steganography Methods in Multi-Media Domain," International Journal of Engineering & Technology Website, vol. 8, pp. 288-292.

[12] W.Fitriani1, R. Rahim , B. Oktaviana & A. P. U.Siahaan, (2017)"Vernam Encypted Text in End of File Hiding Steganography Technique Vernam Encypted Text in End of File Hiding Steganography Technique," International Journal of Recent Trends in Engineering & Research, pp. 214-219.

[13] M.T.Sharabyan & H. Ghorbani , (2018)"A NEW COMBINED METHOD WITH HIGH SECURITY FOR DIGITAL IMAGES STEGANOGRAPHY BASED ON IMPERIALIST COMPETITIVE ALGORITHM AND SYMMETRIC ENCRYPTION ALGORITHM ," INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS , vol. 6, no. 1, pp. 1-12.

[14] V.Yadav& S. K. Sharma, (2017)"A New Approach for Image Steganography Using Edge Detection Method for Hiding Text in Color Images Using HSI Color Model," IJSRSET, vol. 3, no. 2, pp. 833-845.

[15] G. S.Charanl,N. Kumar , Karthikeyan ,Vaithiyanathan & D. Lakshm ,(2015) "A Novel LSB Based Image Steganography With Multi-Level Encryption," In 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS) , IEEE pp .1-5.

[16] M. Juneja1 & P.S.Sandhu ,(2014)"Improved LSB based Steganography Techniques for Color Images in Spatial Domain," International Journal of Network Security, vol. 16, no. 6, pp. 452-462.

[17] D. Adiyan , T. W. Purboyo& R.A. Nugrahaeni ,(2018) "Implementation of Secure Steganography on Jpeg Image Using LSB Method," International Journal of Applied Engineering Research, vol. 13, no. 1, pp. 442-448.

[18] P. Srilakshmi1,Ch. Himabindu ,N. Chaitanya ,S.V. Muralidhar , M.V. Sumanth & K. Vinay,(2018) "Text embedding using image steganography in spatial domain," International Journal of Engineering & Technology, vol. 7, no . 3.6 pp. 1-4.

[19] H.H.Al.Ghuraify , A.A.Al-Bakry & A. T. Al-Jayashi, (2019) "DUAL SECURITY USING IMAGE STEGANOGRAPHY BASED MATRIX PARTITION," International Journal of Network Security & Its Applications (IJNSA), vol. 11, no. 2, pp. 13-31.

[20] Ö.ÇATALTA&K.TÜTÜNCÜ, (2017)"Comparison of LSB Image Steganography Technique in Different Color Spaces," International Artificial Intelligence and Data Processing Symposium (IDAP) , IEEE ,pp. 1-6.

[21] B. Rexha, P.Rama, B.Krasniqi &G. Seferi, (2018) "Efficiency of LSB and PVD Algorithms Used in Steganography Applications," International Journal of Computer Engineering and Information Technology (IJCEIT), vol. 10, no. 2, pp. 20-29.

[22] C-F. Lee, C-C. Chang, X. Xie, K. Mao& R-H. Shi, (2018). "An Adaptive High-Fidelity Steganographic Scheme Using Edge Detection and Hybrid Hamming Codes," Displays, pp. 1-28.

[23] K.Silpa & S.A. Mastani , (2012)"COMPARISON OF IMAGE QUALITY METRICS," International Journal of Engineering Research & Technology (IJERT), vol. 1, no. 4, pp. 1-5,

[24] D.R. I.s M. Setiadi,E. H.R.mawanto,C.A.Sari,A.Susanto&M.Doheir, (2018) "A Comparative Study of Image Cryptographic Method," International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), pp. 336-341.

[25] S. Namasudra &G. C.Deka, (2018) Advances of DNA Computing in Cryptography, CRC Press.

[26] "https://women-girls.org/wp-content/uploads/2016/10/20161007-232.jpg".

[27] "http://photos49.blogspot.com/2011/01/blog-post_9090.html".

[28] "https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQXUtjHubn_JKAauZU5l7N4k8JnyaRCmruryR-4_OHcJULpyK8y".

[29] "https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSSWU5fh_XPXx2rE1U_jWczsmj16HAACC2YwetHnNyaDxxz3PHI".

[30] A. S. Ansari, (2019)"A Comparative Study of Recent Steganography Techniques for Multiple Image Formats," I. J. Computer Network and Information Security, vo. 1, pp. 11-25.

[31] "https://homepages.cae.wisc.edu/~ece533/images/ ".

AUTHORS

Huda .H. Al.ghuraify received her bachelor degree in communication engineering from Engineering technical college , najaf , Iraq in 2010.she is currently pursuing The MSC degree at Engineering technical college , AL-Furat AL Awsat University . Her Research interests include communication security and image steganography.

Dr .Ali A .Al-bakry was born in Babyloon /Iraq on June 3, 1959. He receivedhis B.Scand M.Sc.in electrical engineering department, college of engineering,university of Baghdad, Baghdad, Iraq, in 1982 and in 1994 respectively and his PhD degrees in electrical engineering from University of Technology (UoT) Baghdad, Iraq, in 2006.Since 2004 he is electrical engineering professor anda Dean of Al-Najaf Engineering Technical College, Al-Furat Al-Awsat TechnicalUniversity.His current research interests include high voltage engineeringTechniques, electrical power system stabilityand intelligent optimization,electric machine drive, renewable energy, intelligent control techniques, smartand adaptive control in electric power system.

Dr. Ahmad T. Al-jayashi received his bachelor in electrical engineering fromTikret university. received his MSC in electrical engineering from university of baghdad and phd from electrical and computer department of michigan state university.he has more than 29 papers published in different valuable journals and conferences. He is currently working as assistance dean of al najaf engineering technical collegeAL-Furat AL-AwsatUniversity. his interested control theory,advance image processing ,security of communicationsystem,robotics mainpulation systems.he had been chosen as a reviewer formany journals and conferences.