DUAL SECURITY USING IMAGE STEGANOGRAPHY BASED MATRIX PARTITION

Huda H.Al.Ghuraify[1], Dr. Ali A.Al-Bakry[2] and Dr. Ahmad T. Al-Jayashi[3]

[1]Engineering technical college,al-furat al-awsat university,al-najaf
[2]Dean of engineering technical college,al-furat al-awsat university,al-najaf
[3]Assistance deanof engineering technical college,al-furat al-awsat university,al-najaf

ABSTRACT

Recently, the mode of living became more complicated without computer systems. The techniques of camouflage information have acquired a vital role with the requirement of intensifying trade of multimedia content. Steganography is the technique that utilizes disguise in a way that prohibits unauthorized access from suspicion of the existence of confidential information exchanged during communication channels between the connected parties. In this paper, an integrated image steganographic system is designed to conceal images, messages or together where the mainly deliberate the improvement of embedding capacity through embedding text with image simultaneously. For that purpose, used matrix partition to partition the secret image then embedded each partition separately after scrambling each pixel by replacing msb instead of lsb to provide the second level of security furthermore to steganography. The simulation results clarify the better performance of the proposed algorithms.

KEYWORDS

Image steganography, Spatial domain , Matrix partition, Least Significant Bit

1. INTRODUCTION

In this contemporary age, computers and the internet are greater communicating media that join varied portions of the globe. Therefore, people can easily transfer data. Consequently, the safety and security stay an important question. The requirement to answer this question has guided to the improving of steganography system [1].

The name Steganography is formed from a Greek expression, “Steganos” denote "covered " and “Graptos” denote "writing ", which denote concealed communicating. In this technique, the existence of a message is camouflage[2] .

Steganography is closely associated with cryptography[3]. Cryptography is the most significant realm in computer security. Actually, it is a technique for exchanging private data through an open system correspondence, with the goal that as it were the recipient who has the mystery key can peruse the encoded messages, which may be reports, telephone discussions, images, or different types of information[4].Unlike cryptography where communicating is observable, but the content is kept private, steganography is the scientific discipline that hiding data within some data media [3].There are five primary class of cover which can be utilize for steganography technique [5].

Figure 1.demonstrate the kind of media that utilized as a cover for steganography technique.

The Image steganography deals with the information that is concealed in the image and can be performed in two domains [6]. The spatial domain where the private data is concealed by

DOI: 10.5121/ijnsa.2019.11202

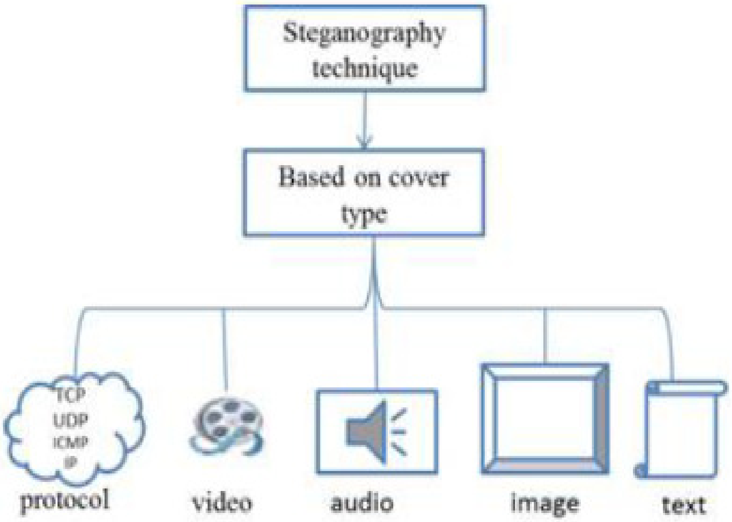


Figure 1. Type of steganography technique according to cover kind

modifying the intensity of pixel values into a cover image within concealing data directly [5] and Frequency domain where private information is concealed into carrier after converting it into frequency domain [6]. This technique utilizes a transform coefficient to conceal private information. By altering the transform coefficient, private information is to be concealed. This is broadly utilized as a result of its independence over image formatting. This procedure is progressively powerful to various sorts of assaults [7].figure 2. illustrates the sort of image steganography techniques indicated by the embedding domain.

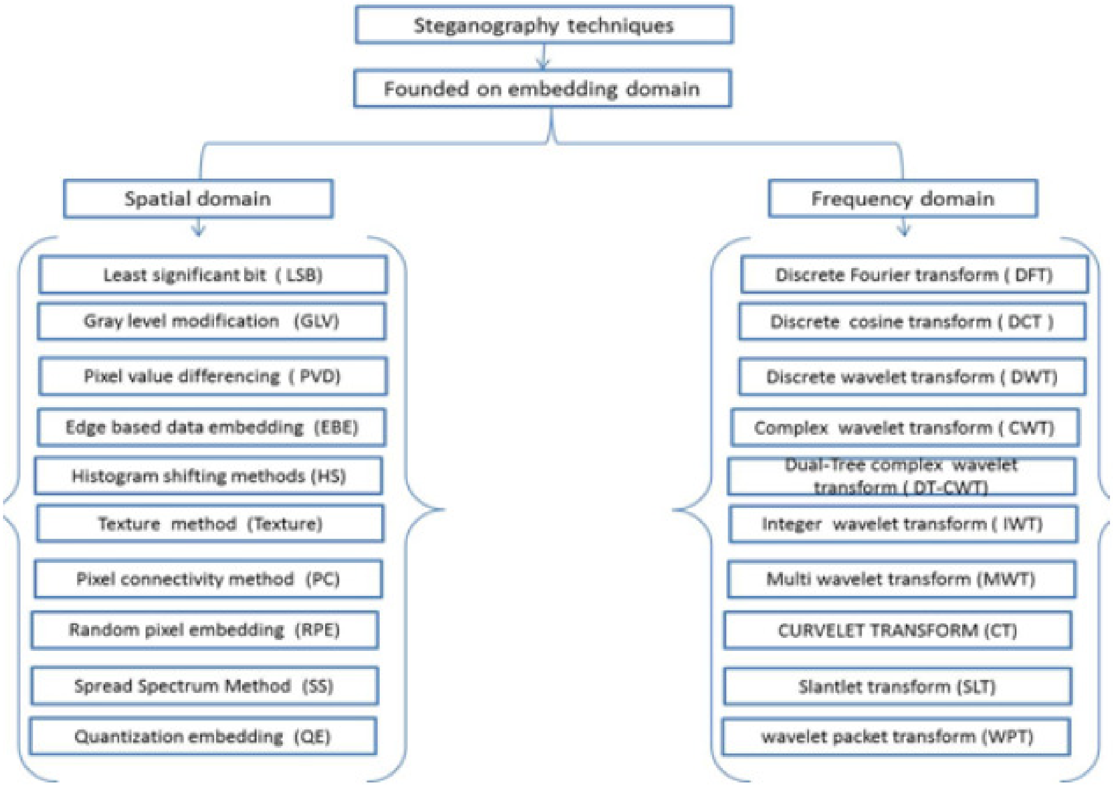

Steganography techniques
Founded on embedding domain
Spatial domain
Least significant bit (LSB)
Gray level modification (GLV)
Pixel value differencing (PVD)
Edge based data embedding (EBE)
Histogram shifting methods (HS)
Texture method (Texture)
Pixel connectivity method (PC)
Random pixel embedding (RPE)
Spread Spectrum Method (SS)
Quantization embedding (QE)
Frequency domain
Discrete Fourier transform (DFT)
Discrete cosine transform (DCT)
Discrete wavelet transform (DWT)
Complex wavelet transform (CWT)
Dual-Tree complex wavelet transform (DT-CWT)
Integer wavelet transform (IWT)
Multi wavelet transform (MWT)
CURVELET TRANSFORM (CT)
Slantlet transform (SLT)
wavelet packet transform (WPT)

Figure 2. Classification of image steganography technique according to the embedding domain

Despite the fact that the aim of the cryptography and steganography system are similar, which is to supply guard end to end data communicating, their meanings of robustness to the offense are dissimilar. A cryptography framework is considered as crack when the outsider acquire accesses to decrypt information, while the steganography framework is considered as crack when the outsider acquires the appearance of mystery information[8].

Steganography used in broad of applications such as military constitution for protecting the transmission of private information, intelligence service, in intelligent identity cards where particular details are hidden in the picture of a person for copyright restrain, medical imaging where patient's information is concealed within image give security of information and decrease transmitting time[9].

In this paper, we present a new partition steganography techniques utilized LSB algorithm in spatial domain to hide images, messages or together using RGB color and grayscale as cover images. The remains section of the paper is organized as listed below:

Section 2 shows The literature review. Section 3 explains Model of image Steganography system with measurement. Section 4 shows the proposed approach. The results are illustrated in section 5, and the conclusions demonstrated in Section 6 pursue the pertinent references.

2. LITERATURE REVIEW

S. Ali, et. al. [10] proposes a spatial domain LSB replacement method for grayscale image concealed and Arnold transform is applied to ensure security. The proposed system is verified against a series of standard images and it has features of imperceptibility and security but the limitation of the method is being slow in extracting algorithm when utilizing large size image greater than 160*160. Also, it employs images of the same dimensions.

Kh. A. Al-Afandyi, et al. [11] propose a data hiding scheme based on cropping a color image and separate The private message into section identical image crops and Each section is concealed into an image crop according to private sequence utilize the LSB. The proposed approach provides higher security for the private message.

Y. Parti, et al.[12] propose a steganographic approach for grayscale image hidden based on spatial domains which utilize three times the XOR operation and utilizes three MSB bits 8th, 7th, and 6th as keys to cipher the private message earlier and then concealed it utilizes the LSB algorithm. The proposed methods provide another level of security with a simple operation.

S. Mahdie [13] suggests a method based on Selected Least Significant Bit to hide data into color images utilize magic square. The proposed algorithm has two strong points; the private text is dispersed among the image using magic square order, which raises the complexity of the algorithm, and the secret bits are altered by their Xor with the corresponding Selected Least Significant Bit value but the Mean Square Error approach 10.81.

Kh. F. Rafat, et al.[14] propose Secure image Steganography where the secret information is dispersed irregular into cover image utilize Stego key dependent position where the attacker may not definite whether the image holds some hidden data . The proposed scheme is difficult to detect but limited capacity when applied to color image because of used the only blue channel.

V.Shahuse.[15] suggest Sparse Matrix for Steganography in the spatial domain to encode data such as the key and message which support the security of the algorithm and the proposed is better in time of execution but lacks cover image size to analyze performance.

K. Joshi, et al.[16] propose a method of image steganography using gray images as cover and combine it with cryptography in a spatial domain. In the proposed scheme, the private message is ciphered employ Vernam cipher and then the cipher is hidden into an image utilizes LSB with Shifting. The proposed method enhances the security of concealed information but doesn't determine exactly the number of a bit from LSB that used for data hidden to recognize the total capacity that available to conceal the private message.

3. IMAGE STEGANOGRAPHY SYSTEM

3.1 MODEL OF IMAGE STEGANOGRAPHY SYSTEM

The entire steganography system is constituent of cover media, stego media, concealing algorithm, extraction algorithm, secret data, and in some model a stego key used where Data concealing manner is achieved at the sender part while the data extraction is achieved at the receiver part. Steganography systems suppose the private transmitting of the information only know for sender and receiver [17]. The steganography system that utilizes images as the cover media is known as an image steganography where conceal private information into images is the common employ manner as it can gather benefit of the confined power that associate with the human visual system and an enormous amount of superfluous data of images that can be exploited to conceal private information [18]. Figure 3 shows the model of an image steganography system structure. Initially, the cover image here can be considered in different sizes and secret data can be either image or message or both.

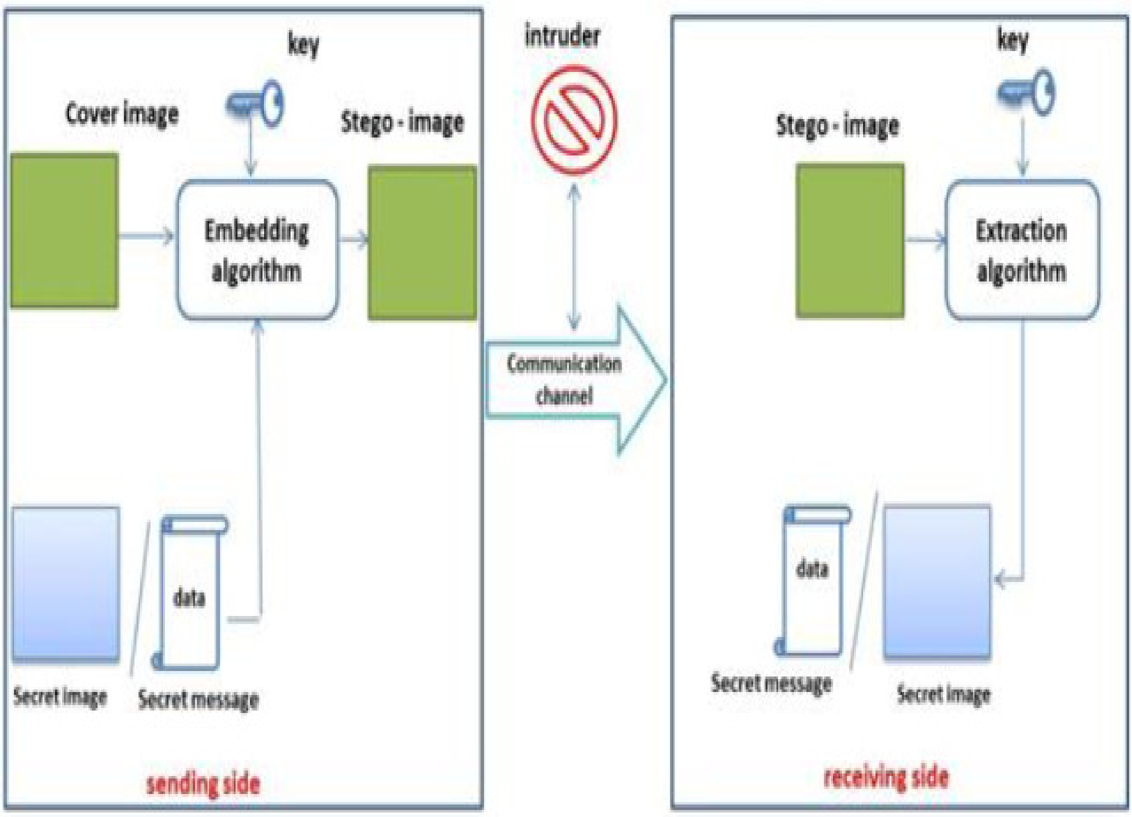


Figure 3.Simple model of image Steganography System

3.2 STEGANOGRAPHY MEASUREMENT

There are many factors which can be considered for the steganography measurement but the most effective parametric quantity that examines the effectiveness of a steganographic scheme is: imperceptibility, which is able to be unnoticed by the human eye. The capacity is explained by how many bits can be concealed in a cover medium and robustness that define the quantity of change the stego media can resist before an opponent can devastate the concealed data [19]. Figure 4 shows the requisite for any steganography system measurements.

Robustness
Capacity
Imperceptibility

Figure 4. Fundamental properties of steganographic system[19]

4. THE PROPOSED PROCEDURE

4.1

The proposed work in this paper comprises three stages, first of it using matrix partition for private image to increase capacity, second stage is scrambling the secret data by make MSB instead of LSB to provide an additional level of security and third stage is Steganography, to conceal either a grayscale image or message or together inside a grayscale cover-image of any size and also conceal either a color image or message or together inside a color cover-image of any size using LSB algorithm in spatial domain. Figure 5and figure 6 illustrates the diagram proposed at sending and receiving part respectively.

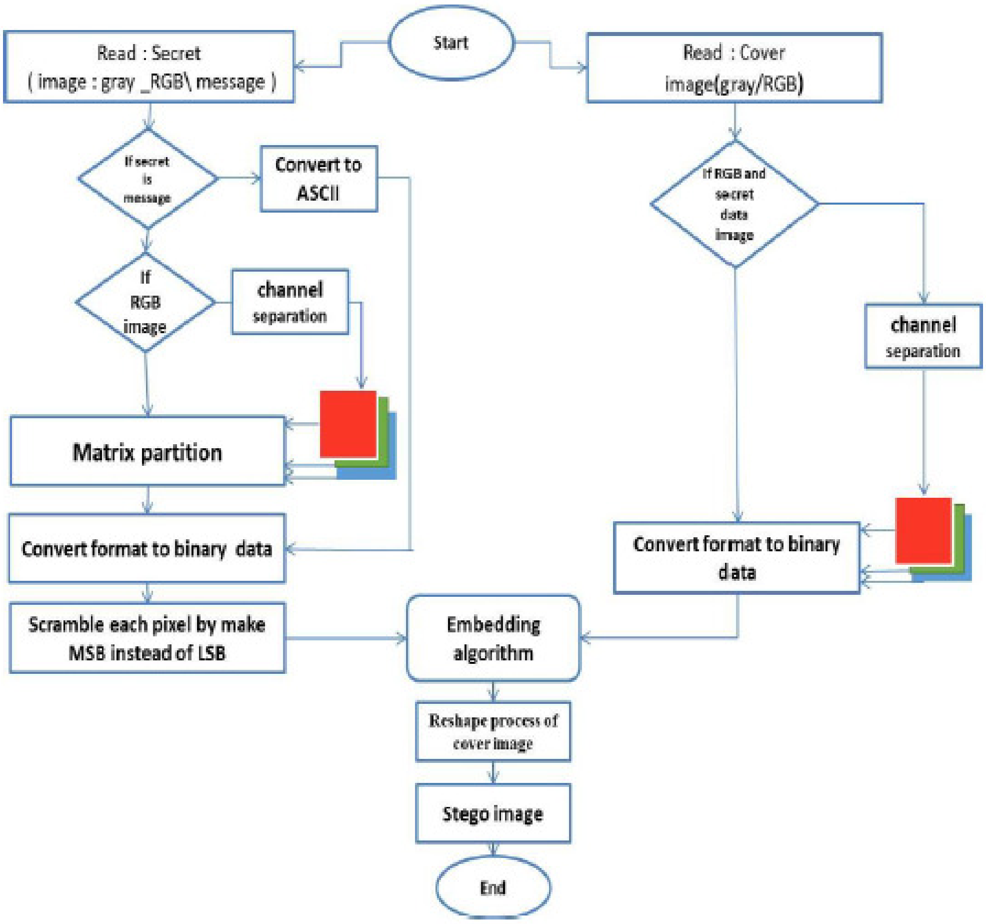


Figure 5. Block Diagram that proposed at sending side

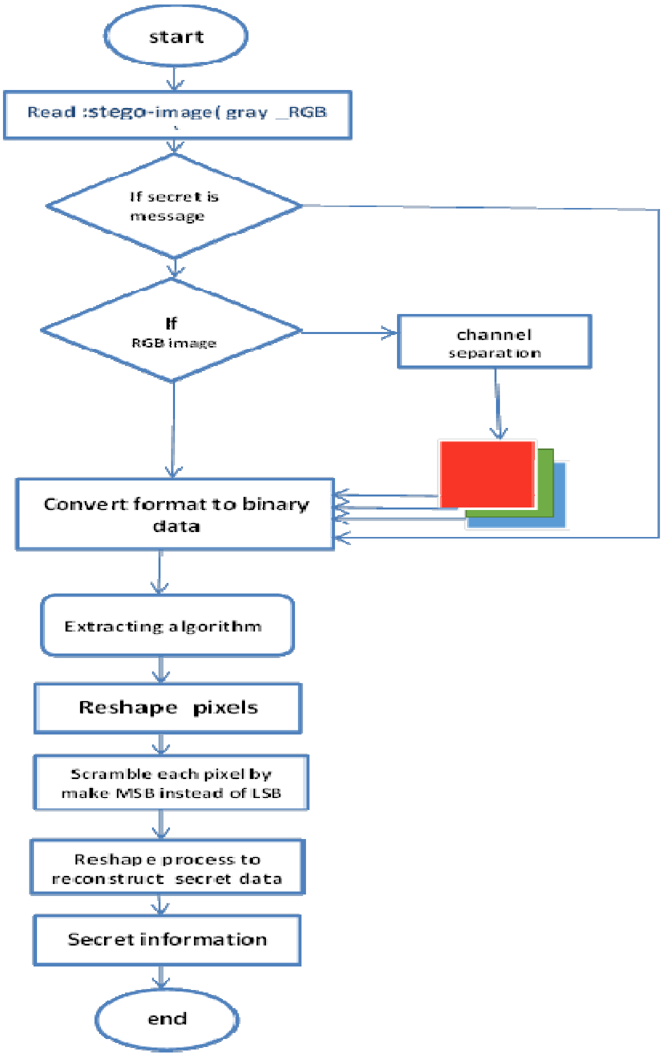

start
Read :stego-image(gray _RGB
If secret is message
If RGB image
channel separation
Convert format to binary data
Extracting algorithm
Reshape pixels
Scramble each pixel by make MSB instead of LSB
Reshape process to reconstruct secret data
Secret information
end

Figure 6. Block Diagram that proposed at receiving side

4.1.1. Embedding Procedure at Sending Side

Cover image and the private information are used here.

Steps:

1. Read Cover image and Secret data (image/message/imagewith a message).
2. Apply matrix partition to a secret image if the hidden data is image or image with a message example:-
a- if a secret image is grayscale and size (256*256) then after apply matrix partition obtain two matrices (128*256)and(128*256).
b-if a secret image is RGB and size (256*256) first separate channels and then apply matrix partition to each channel then obtain six matrices each of size(128*256).
3-convert cover image to binary format. The result data will be
((R(rowcover)*C(columncover)) x 8).
4- convert secret data to binary format. The result data will be
((R(rowsecret)*C(columnsecret)) x 8).
5- Apply scrambling to secret data of binary format by making MSB bits instead of LSB bits.

6-Each bit of scramble private information will be concealed in a cover image using LSB method where each scramble matrix partition bits conceal separately.
7-reshape cover image according to size to create stego image.
8-write stego-image to the selected location using BMP format .

4 .1.2. Extraction Procedure at Receiver Side

The Stego image is utilized as the source for the Extraction stage to extract the private information without the need for a cover image. the following keys are necessitated In order to extract the private data exactly:

a-The size of one image partition (R partition,C partition) if secret information is an image.
b- The length of the message if secret information is a message.
c- combine a and b if secret information together.

Steps:

1. Enter the Stego image and then read it.
2. Convert format of it to binary form.
3. The least significant bits(according to the hidden algorithm) from 1 to (R partition* C partition*8) bits of every partition are retrieved for secret image and from 1 to the length of message bits are retrieved for a secret message Where the type of confidential data is clarify depending on the name of the stego- image .
4. The retrieved information shape to ((R partition * C partition)retrieved/8) rows and (8) columns.
5.scramble each binary bits that shaped by making MSB bits instead of LSB bits.
6-converted scramble binary bits to decimal form.
7- shape decimal form according to (R partition,C partition) for secret image partition and transpose decimal form then convert to a character for a secret message.
8- reshape partition to form an entire secret image if private information contains an image.
9-write secret image to the current directory using .bmp format if private data contain an image and write a secret message to a text file if private data contain a message.

5. SIMULATION

5.1. SIMULATION SETUP

The proposed algorithm was implemented in MATLAB Version (R2017a) with a computer of the specifications that demonstrate as follows:

Processor depict : Core(TM) i7-2630QM CPU @ 2.00GHz and RAM- 6Gbytes

5.2. SIMULATION PARAMETERS

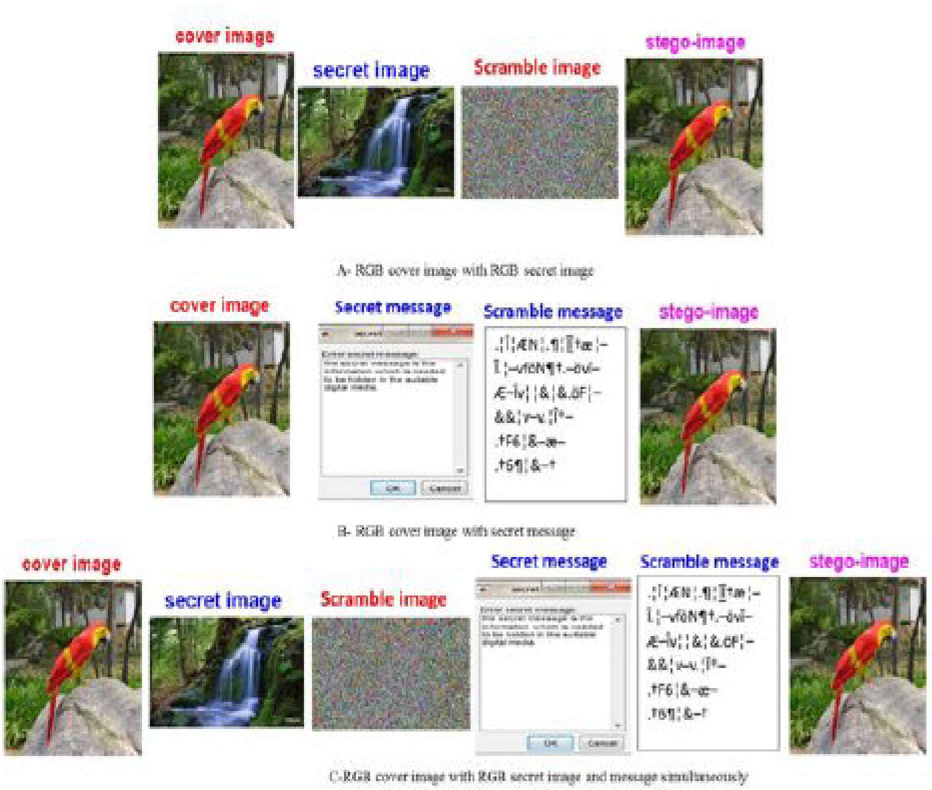
Table 1. Parameters Of Simulation That Utilized To Examine Execution Of The Proposed Algorithm

Information	Type	Details
Cover image	RGB image	size 640×640×3 and of .jpg format [20].
	Grayscale image	size 900×800 and of .jpg format [21].
Secret data	RGB image	size 284×177 and of .jpg format [22].
	Grayscale image	of size 292×173 and of .jpg format [23].
	Message	“ The secret message is the information which is needed to be hidden in the suitable digital media ” [24].

5.3. SIMULATION RESULTS

5.3.1. Visual Quality at Sending Side

From visual quality infer that the employ of the steganography scheme for concealing private information cannot be distinguished where the cover image and stego-image similar at sending part .Figure 7 and Figure 8 Exhibit Sending part utilizing both RGB and grayscale image as cover to form stego image. where the mystery information first scramble by replacing MSB rather than LSB then embedded scramble information in the cover image according to the embedded algorithm.

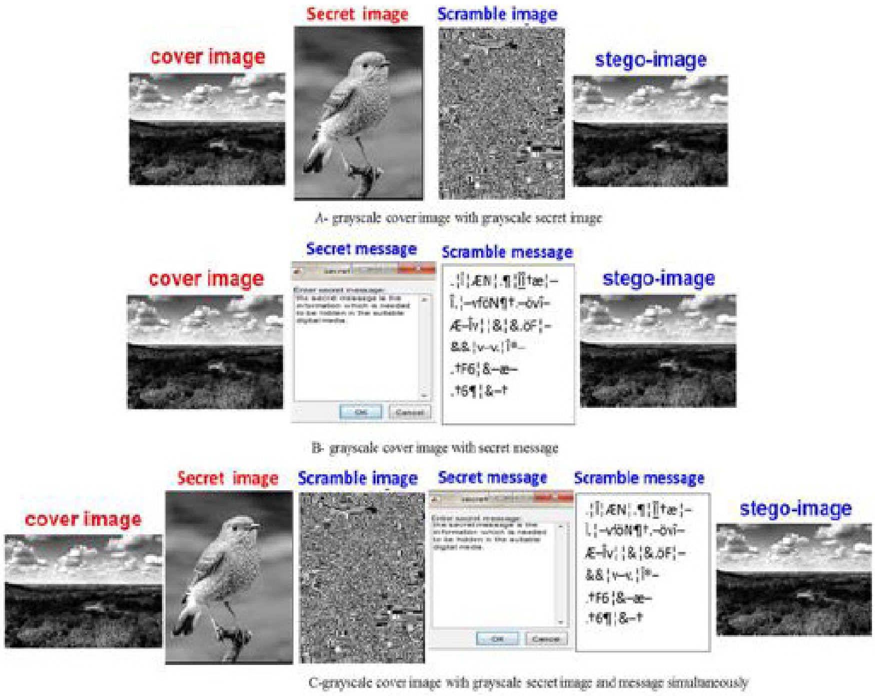


A- RGB cover image with RGB secret image

B- RGB cover image with secret message

C-RGB cover image with RGB secret image and message simultaneously

Figure 7. RGB cover image with secret data to form stego image at sending part



A- grayscale cover image with grayscale secret image

Enter secret message:
the secret message is the information which is needed to be hidden in the suitable digital media.

.¦¦¦ÆN¦.¶¦‖†æ¦–
Ĩ.¦–√fôN¶†.–ôvĩ–
Æ–Ĩv¦¦&¦&.ôF¦–
&&¦v–v.¦Ĩª–
.†F6¦&–æ–
.†6¶¦&–†

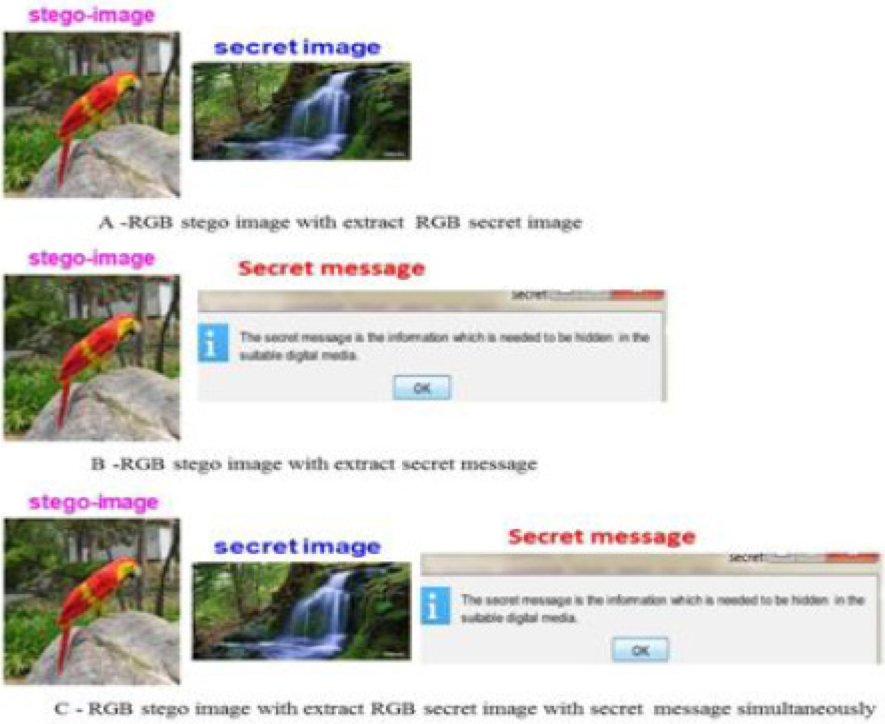
B- grayscale cover image with secret message

C-grayscale cover image with grayscale secret image and message simultaneously

Figure 8. Grayscale cover image with secret data to form stego image at sending part

5.3.2. Visual Quality at receiving part

The quality of the retrieved data exhibits that private data and the retrieved data identical. The PSNR between the private image and retrieved image is (Inf) this signifies that two image identical. Figure 9 and Figure 10 demonstrate receiving part with extract secret information.



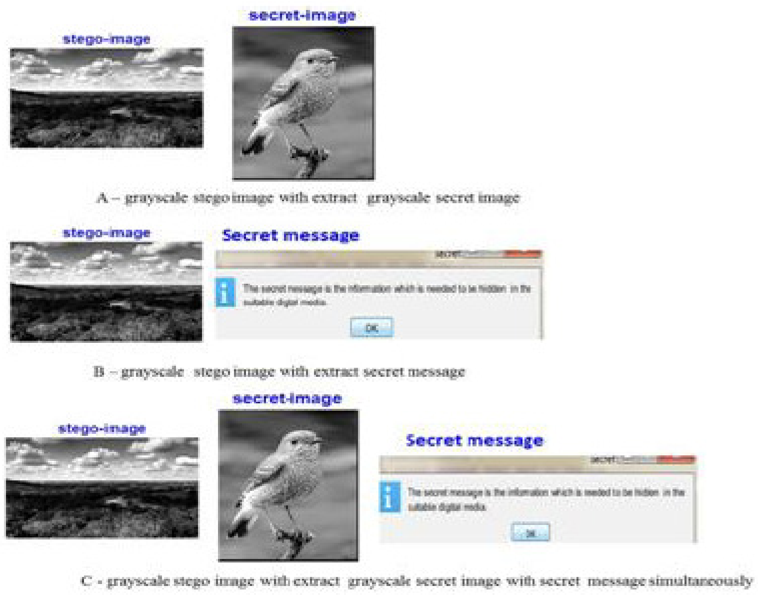
A -RGB stego image with extract RGB secret image

The secret message is the information which is needed to be hidden in the suitable digital media.

B -RGB stego image with extract secret message

C - RGB stego image with extract RGB secret image with secret message simultaneously

Figure 9. RGB stego image with extract secret data at receiver part



The secret message is the information which is needed to be hidden in the suitable digital media.

A – grayscale stego image with extract grayscale secret image

B – grayscale stego image with extract secret message

C - grayscale stego image with extract grayscale secret image with secret message simultaneously

Figure 10. Grayscale stego image with extract secret data at receiver part

5.4. Performance Measure

For measure stego image performance with respect to cover image, several parameters have been regarded such as:

5.4.1. Mean Square Error (Mse)

The square of the mistake between the image without secret data and the image with secret data. Value of MSE determine The distortion in the image [25].MSE is computed utilizing eq.(1)

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[C(i,j) - S(i,j)]^2 \dots\dots\dots (1)$$

Where:
C(i,j) : cover image without secret data.
S(i,j) : stego-image with secret data.
m: number of row for image.
n: number of columns for image.

5.4.2. Peak Signal To Noise Ratio (Psnr)

The ratio between the extreme attainable power of a signal to the power of clatter that influence the correctness of its representation. The greatest value of PSNR demonstrates the better quality of the stego image[26].PSNR is computed as follows in eq. (2)

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

Where:

I^2 is the maximum possible pixel value of the images.

5.4.3.Structural Similarity Index Metric (SSIM)

Is utilized for comparing the similarity between two images[27].the SSIM index can be calculated according to eq.(3)

$$SSIM(X,Y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x{}^2 + \mu_y{}^2 + C_1)(\sigma_x{}^2 + \sigma_y{}^2 + C_2)} \ldots\ldots\ldots (3)$$

Where :

X: reference image
Y: test image.
σx: standard deviation of X
σy: standard deviation of Y
µx : the mean value of X
µy : the mean valueof Y
C1 and C2 : the stabilization constant.
σxy : the correlation between X and Y.

5.4.4.Embedding Rate (Er)

Represent the ratio of the embedded private bits into the entire pixels of the carrier image. According to the embedding payload rating, an enormous value of ER refer that the steganographic system has better functioning, that is, a pixel in the cover image can hold more private bits. On the contrary, a tiny value of ER refers to a worse functioning[28]. The ER is defined as in eq.(4)

$$\frac{H}{M * N}\text{bpp} \quad \ldots\ldots\ldots (4)$$

H :the entire numeral of the embedded private data.
M*N : the size of the carrier image

Table 2.Performance Measure of proposed algorithms utilizing RGB color as cover image

Cover	Secret information	MSE	PSNR db	Capacity available to hide/byte	Used capacity byte	ER% For used	SSIM	Elapsed time/hide seconds	Elapsed time/extract seconds
RGB color Cover image (640*640) (24 bpp)	RGB color secret image (284*177)(24bpp)	1.2811	47.0549	307200	150804	12.27%	0.99816	12.008376	0.542885
	Message	0.000318	83.1038	153600	97	0.007%	1	12.230383	0.250372
	Message with RGB color secret image simultaneous (284*177)(24bpp)	1.2864	47.037	358400	150901	12.28%	0.99815	12.629328	0.573567

Table 3.Performance Measure of proposed algorithms utilizing Grayscale as cover image

Cover	Secret information	MSE	PSNR db	Capacity available to hide/byte	Used capacity byte	ER% For used	SSIM	Elapsed time/hide seconds	Elapsed time/extract seconds
Gray scale Cover image (900*600) (8bpp)	Gray scale secret image (194*259)(8bpp)	0.92758	48.4573	135000	50246	9.30%	0.99523	1.400487	0.310399
	Message	0.000744	79.4125	67500	97	0.017%	1	1.143407	0.113008
	Message with gray secret image simultaneous (194*259)(8bpp)	0.93875	48.4053	202500	50343	9.32%	0.99516	2.175494	0.358758

Where the capacity available to hide = (rowcover*columncover* L)

L represents the number of LSB in the entire cover that can be utilized for hiding secret data according to embedded algorithms.

And used capacity represents the entire numeral of the actual embedded secret data into an available cover image.

According to table 2 and table 3 the Performance analysis signify that the deviation of stego-image quality is less and an onlooker cannot identify any distinction between the cover image and stego image where The closer the SSIM to one is regarded as that the stego image more comparable to the cover image, the PSNR has value above 40 dB and the MSE has value less than 1.5.

Enlarge the size of cover image provide better performance in term of steganography system measurement where The capacity that available to conceal private information increase with reduced MSE and increase of PSNR while retaining the same secret information as shown in Figure11,Figure 12and Figure 13 .

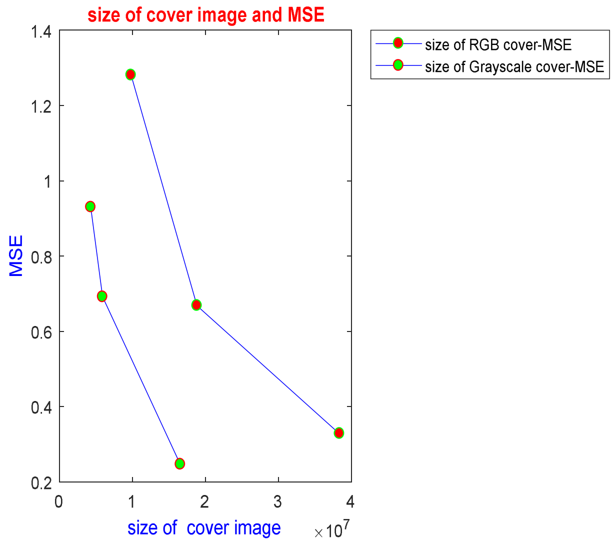


Figure 11. Relation between size of cover image and MSE

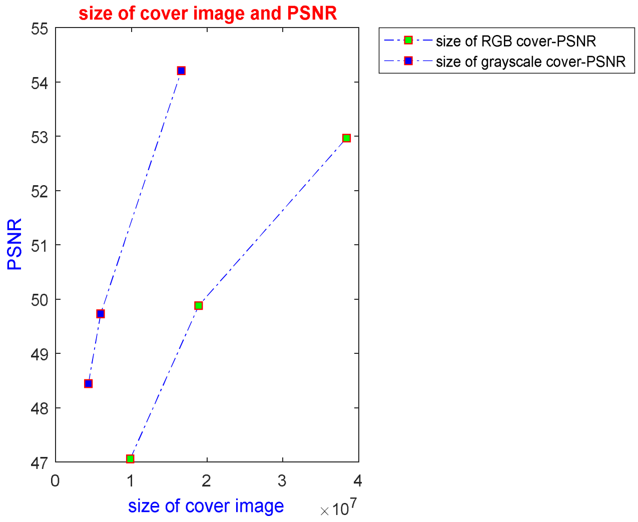


Figure 12. Relation between size of cover image and PSNR

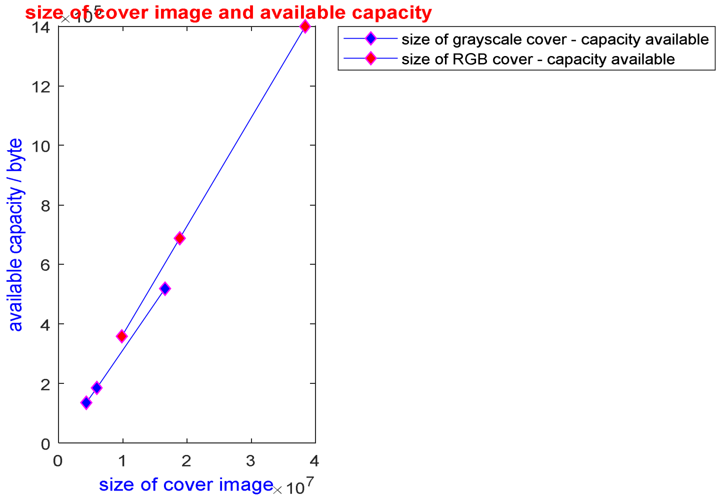
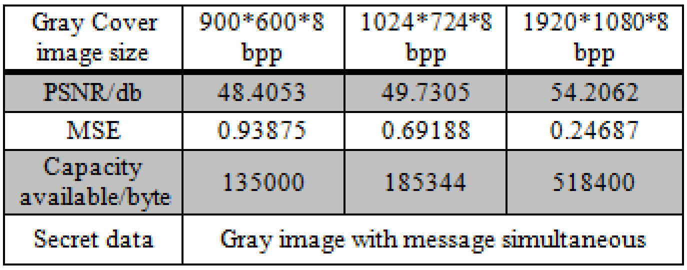


Figure 13. Relation between size of cover image and capacity

Table 4. Performance Analysis Of utilize different size of RGB cover image with retain secret data

RGB Cover image size	640*640*24 bpp	1024*768*24 bpp	1000*1600*24 bpp
PSNR /db	47.037	49.8805	52.966
MSE	1.2864	0.66839	0.32846
Capacity available/ byte	358400	688128	1400000
Secret data	RGB image with message simultaneous		

Table 5. Performance Analysis of utilize different size of grayscale cover image with retain secret data



Gray Cover image size	900*600*8 bpp	1024*724*8 bpp	1920*1080*8 bpp
PSNR/db	48.4053	49.7305	54.2062
MSE	0.93875	0.69188	0.24687
Capacity available/byte	135000	185344	518400
Secret data	Gray image with message simultaneous		

The Performance measure in table 4 and table 5 denote that the PSNR value and the capacity available for hiding secret data enlarge as the cover image size enlarge and the MSE value decline as the size of the cover image magnify. The proposed system hides the size of any secret image within the capacity available for camouflage in the cover image while maintaining better performance in term of a requirement for the steganographic system as shown in figure14:

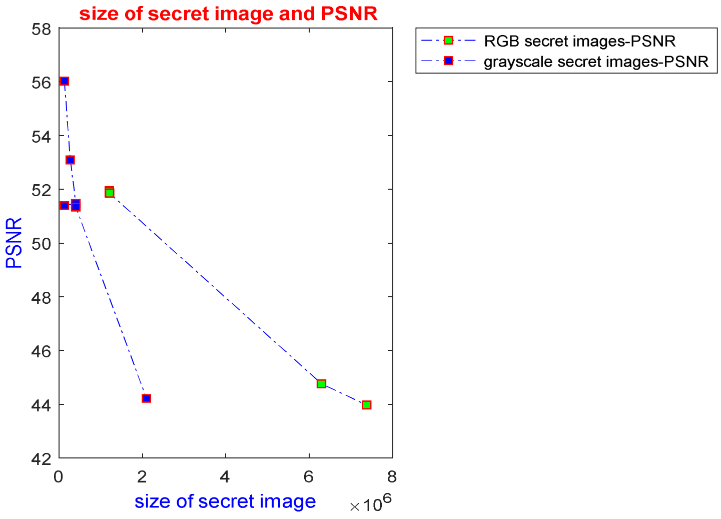


Figure 14. Relation between size of secret images and PSNR(db)

Table 6.Performance investigation Of test proposed algorithm with different size of secret RGB color image while maintain size of cover RGB image

RGB cover image of size 1280* 960*24bpp						
Capacity available for hide/byte to this cover:- 921600 byte						
Secret image type	RGB image					
RGB secret image size	194*259 *24 bpp	284*177*24 bpp	193*261*24 bpp	225*225*24 bpp	512*512*24 bpp	640*480*24 bpp
PSNR /db	51.9521	51.9197	51.8620	51.8482	44.7650	43.9739
Capacity used to hide/ byte	150738 byte	150804 byte	151119 byte	151875 byte	786432 byte	921600
ER %	4.0890%	4.0908%	4.0994%	4.1199%	21.3333%	25.0000%

Table 7.Performance investigation of test proposed algorithm with different size of secret grayscale image while maintain size of cover grayscale image

Grayscale cover image of size 1280* 848*8 bpp						
Capacity available for hide/byte to this cover:- 271360 byte						
Secret image type	Grayscale image					
secret image size	128*128 *8 bpp	182*186*8 bpp	194*259*8 bpp	292*173*8 bpp	225*225*8 bpp	512*512*8 bpp
PSNR /db	56.0194	53.0890	51.4690	51.3917	51.3333	44.2201
Capacity used to hide/ byte	16384 byte	33852 byte	50246 byte	50516 byte	50625 byte	262144 byte
ER %	1.5094 %	3.1187%	4.6291%	4.6540%	4.6640%	24.1509%

Table 6 and table 7 exhibit that the proposed algorithm can utilize various size of secret data until the utilized capacity of secret data equal the capacity that available to hide into cover image with better value of PSNR as shown in table 6 when the size of secret data (640 * 480 * 24 bpp) the value of PSNR above 40 dB while the capacity used equally to available capacity into cover image this indicate better performance of the algorithms.

6. CONCLUSION

In this paper, an integrated image steganographic system based matrix partition utilize RGB color and grayscale carrier images is proposed to hide text, image, or both, where hiding text with the image simultaneously in the proposed algorithms provide three features, The first feature seize the attacker's attention to the amount of data thus supply more protection for private message. The second feature, offer details about secret image with append secret message embedded in the cover image simultaneously thus exploit time that consumes when sent them separately and the third feature uses matrix partition to private image that increase the concealed capacity of the algorithm. Also, present better performance in terms of speed of execution and extraction. The simulation results exhibit that our proposed algorithm realize better embedding capacity with the excellent visual quality of both stego image and extract private image with providing additional security by using scramble of each pixel furthermore to steganography. The limitation of the proposed algorithms that stego image loss secret data if exposed to lossy compression because the algorithm accomplishes in spatial domain using LSB algorithms. As a future work, the proposed method may be utilized with the encryption algorithms to provide three levels of security and the proposed method may be also applied in transform domain rather than spatial domain to provide robustness against attack.

REFERENCES:

[1] N. Hamid, A. Yahya, R. B. Ahmad, and O. M. Al-Qershi, (2018) “Image in image Steganography Technique based on Arnold Transform and LSB Algorithms,” Int. J. Comput. Sci. Secur., vol. 6, no. 3, pp. 32–39.

[2] A. Sharma, M. Poriye, and V. Kumar, (2017) “A Secure Steganography Technique Using MSB,” Int. J. Emerg. Res. Manag. &Technology, vol. 6, no. 6, pp. 208–214.

[3] J. M. ud din lone Amit Chaturvedi, (2018) “An Analysis on LSB Image Steganography with Colour Image as Cover,” Int. J. Comput. Appl., vol. 182, no. 4, pp. 23–28.

[4] H. N. Kamel, M. A. Alia, A. Saeq, and E. A. Maria, (2017) "A S ECURE E- M EDICAL E XEMPTION S YSTEM (E-MES): J ORDAN C ASE," Int. J. Netw. Secur. Its Appl., vol. 9, no. 2, pp. 13–19.

[5] M. M. Hashim, M. Shafry, and M. Rahim,(2018) "A REVIEW AND OPEN ISSUES OF MULTIFARIOUS IMAGE," J. Theor. Appl. Inf. Technol., vol. 96, no. 4, pp. 956–977.

[6] D. L. K. Gunda Sai Charan , Nithin Kumar S S V , Karthikeyan B , Vaithiyanathan V, (2015) "A Novel LSB Based Image Steganography With Multi-Level Encryption," IEEE Spons. 2nd Int. Conf. Innov. Inf. Embed. Commun. Syst. ICIIECS'15.

[7] S. C. Dinde and S. B. Patil, (2014) "DWT Domain Data Encryption with Asymmetric key Cryptography," vol. 3, no. 8, pp. 7744-7747.

[8] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, (2018) "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," Neurocomputing.

[9] F. M. Shelke, A. A. Dongre, and P. D. Soni, (2014) "Comparison of different techniques for Steganography in images," Int. J. Appl. or Innov. Eng. Manag., vol. 3, no. 2, pp. 171–176.

[10] S. A. Al-taweel, M. H. Al-hada, and A. M. Nasser, (2018) "Image in image Steganography Technique based on Arnold Transform and LSB Algorithms," Int. J. Comput. Appl., vol. 181, no. 10, pp. 32–39.

[11] K. A. Al-afandy, O. S. Faragallah, and A. Elmhalawy, (2016) "High Security Data Hiding Using Image Cropping and LSB Least Significant Bit Steganography," IEEE, pp. 400–404.

[12] Y. P. Astuti, D. R. I. M. Setiadi, E. H. Rachmawanto, and C. A. Sari, (2018) "Simple and secure image steganography using LSB and triple XOR operation on MSB," in International Conference on Information and Communications Technology (ICOIACT) Simple, pp. 191–195.

[13] S. M. Klim, (2017) "SELECTED LEAST SIGNIFICANT BIT APPROACH FOR HIDING INFORMATION INSIDE COLOR IMAGE STEGANOGRAPHY BY" J. Eng. Sustain. Dev., vol. 21, no. 01, pp. 74–88.

[14] M. J. Hussain,(2016) "Secure Steganography for Digital Images," Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 6, pp. 45–59.

[15] V. Shah, (2017)"Sparse Encoded Matrix based Steganography algorithm Vipul Shah," Int. Res. J. Eng. Technol., vol. 4, no. 4, pp. 1996–1998.

[16] K. Joshi and R. Yadav, (2015) "A new LSB-S image steganography method blend with Cryptography for secret communication," Proc. 3rd Int. Conf. Image Inf. Process. ICIIP, pp. 86–90.

[17] N. K. Jumaa, (2017) "Image Steganography : Review and Comparison," ResearchGate".

[18] vidhu kiran dutt Shikha, (2014) "Steganography: The Art of Hiding Text in Image using Matlab," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 4, no. 9, pp. 822–828.

[19] D. A. A. Sabri and M. J. Mohsin, (2015) "A New Algorithm for a Steganography System," Eng. &Tech.Journal, vol. 33, no. 8, pp. 1955–1970.

[20] "https://ae01.alicdn.com/kf/HTB12Cu7NpXXXXaBaXXXq6xXFXXXX/40.jpg_640x640.jpg." .

[21] "https://jefflynchdev.files.wordpress.com/2008/12/hill_country_landscape_large.jpg." .

[22] “https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRMmv9KbtAnusL1uh2GlGVat_7mesvJ15Amlr_khloLa3el0IgA.” .

[23] “https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSCdBurtIFUQj7lB12ep57INLBTbDc9BkqmogJM2G6L541EeZHb.” .

[24] A. M. Al-shatnawi, (2012) “A New Method in Image Steganography with Improved Image Quality,” Appl. Math. Sci., vol. 6, no. 79, pp. 3907–3915.

[25] M. C. Pallavi Das, Satish Chandra Kushwaha, (2015) “MULTIPLE EMBEDDING SECRET KEY IMAGE STEGANOGRAPHY USING LSB SUBSTITUTION AND ARNOLD TRANSFORM,” IEEE Spons. 2ND Int. Conf. Electron. Commun. Syst., pp. 845–849.

[26] P. Mathur and S. Adhikari, (2017) “DATA HIDING IN DIGITAL IMAGES USING STAGNOGRAPHY PARADIGM : STATE OF THE ART,” Int. J. Adv. Electron. Comput. Sci., vol. 4, no. 2, pp. 98–102.

[27] K. Silpa and S. A. Mastani,(2012) “COMPARISON OF IMAGE QUALITY METRICS,” Int. J. Eng. Res. Technol., vol. 1, no. 4, pp. 1–6.

[28] Y. Zhang, J. Jiang, Y. Zha, H. Zhang, and S. Zhao, (2013) “Research on Embedding Capacity and Efficiency of Information Hiding Based on Digital Images,” Int. J. Intell. Sci., no. 3, pp. 77–85.

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 Baby loon /Iraq on June 3, 1959. He received his B.Sc and 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 and a Dean of Al-Najaf Engineering Technical College, Al-Furat Al-Awsat Technical University. His current research interests include high voltage engineering Techniques, electrical power system stability and intelligent optimization, electric machine drive, renewable energy, intelligent control techniques, smart and adaptive control in electric power system.

Dr. Ahmad T. Al-jayashi received his bachelor in electrical engineering from Tikret 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 communication system,robotics mainpulation systems.he had been chosen as a reviewer for many journals and conferences.