

IMAGE STEGANOGRAPHY USING INHOMOGENEOUS IMAGES WITH MODYFING VERNAM SCHEME

Huda H.Al.ghuraify¹, Dr.Ali A.Al-bakry², Dr. Ahmad T. Al-jayashi³

¹Engineering technical college,Al-furat Al-awsat university, Iraq

²Dean of engineering technical college,Al-furat al-awsat university, Iraq

³Assistance dean of engineering technical college,Al-furat al-awsat university, Iraq

ABSTRACT

Nowadays, due to the rapid development of the internet, it is prominent to guard mystery data from cyberpunks through communicating. The steganography technique utilizes for trading mystery data in an approach to stay away from doubt. This paper accomplishes a manner for encryption each channel of RGB color image separately without the necessity to exchange an encryption key utilizing the principle of modifying vernam scheme then camouflage it into a grayscale cover image .On the other hand, encrypts a grayscale image without the necessity to exchange an encryption key utilizing the principle of modifying vernam scheme then camouflage it into a cover image of RGB color type . The simulation results revealed an offering of extremely security for the image transmission.

KEYWORDS

Image steganography, Inhomogeneous images, Mystery data, Vernam scheme, Image transmission

1. INTRODUCTION

Nowadays practically every one of the strategies for communicating has become computerized and for the trading of data , we are basically reliant on the internet. Through various zone over the globe, we can trade an assortment of data. These outcomes in secret information being utilized by someone else without assent which could guide perilous results [1].Steganography possesses an urgent role in trading sensitive information over the network. It can be depicted as an information camouflage technique in which private textual detail is disguised by showing the irrelevant media object [2].Communication media are digital files i.e. text ,image , DNA ,video, audio and network protocol [3]as depicted in Fig. 1.

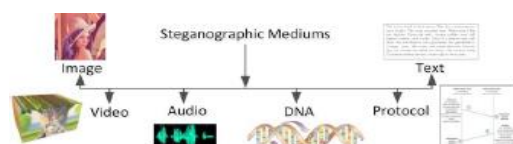


Fig.1.Steganographic mediums [3]

Steganography, acquired from Greek and literally denotes "covered writing"[4].Steganography varies from cryptography as in where cryptography centers around conserve the contents of a message mystery, steganography centers around conserve the manifestation of a message mystery [5].The performance of a steganography technique can be deliberate utilizing various

properties. The most vital property is the imperceptibility of the information, which demonstrates how hard it is to specify the presence of a concealed message. Other related appraise are the capacity of steganographic technique, which is the most extreme data that can securely conceal in a cover without having statistically distinguishable objects, and robustness, which refers to the ability of steganographic technique withstand the extraction of shrouded information[6]. Fig.2 depicts the common principle of steganographic technique .

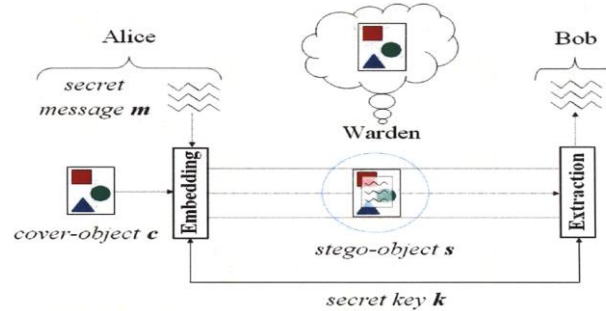


Fig.2.Common model of steganographic technique[7]

A steganography procedure that utilizes images as the cover media is called image steganography. Concealing mystery data in digital images is the most broadly utilized technique as it can exploit the restricted intensity of the human visual system and furthermore, the images have a lot of superfluous data that can be utilized to shroud a mystery data[8].

This paper presents an image steganography scheme that combined modifying vernam scheme with inhomogeneous images utilizing the least significant bit into the spatial domain where encryption each channel of color image utilizing three initial keys from grayscale cover then concealing the cipher form of RGB color image into that cover and also encryption a grayscale image utilizing the initial key from one channel of RGB cover image then concealing the cipher form of grayscale image into that cover.

The formation of the paper is as pursue below: Section 2 shows the literature review. Section 3 explains the proposed scheme. Section 4 evaluates the performance of the proposed scheme, Images Database illustrated in Section 5. Simulation results demonstrated in Section 6. Finally, the conclusion presented in section 7 following with related references.

2. LITERATURE REVIEW

D.Rawat and V. Bhandari , 2013[9] propose an image steganography technique that utilizing (LSB) substitution method for 24-bits color cover image. In the proposed technique describe two procedure to implement the concealing of a secret 8-bit color image as follows: In the first procedure, the last (2-LSB) bits of the channels (red, green ,and blue) of the color cover image, is substitute with (2-bits) of the secret color image. In the second procedure, last (LSB) bits of red channel is substitute with first (MSB) bits of a secret color image, last (2-LSB) bits of green channel is substitute with next (2-MSB) bits of color secret image and then last three (LSB) bits of blue channel is substituted with next three bits of secret color image. The proposed method camouflage only (6) bits from the secret image into 24-bits color cover image.

N.Tiwari, et. Al , 2014 [10] propose a scheme that increases the capacity available for hidden data where utilize three (MSB) of one channel of RGB color cover as an indicator for data hiding and then secret data concealing into entire channels according to that indicator bits. For

example, if the channel red select an indicator channel and three (MSB) of it is (101), then two channel utilize for data concealing and another channel not utilize in embedding scheme where bit (1) indicates that channel utilizes for concealing data while bit (0) indicates that channel does not utilize for hiding secret data. The proposed scheme is analyzed utilizing security appraises and exhibit satisfactory result.

P. Das, et al , 2015[11] propose a method that hiding three grayscale images in a single RGB color cover image utilizing (LSB) substitution in the spatial domain. In the proposed strategy before concealing each grayscale image scramble it utilizing Arnold Transform which rearranges every pixel in the image. Then utilize the last three bit of (LSB) bits of the red channel pixels of the cover image to embed randomly the first three MSB bits of the first scramble grayscale image. The random manner that utilizes for the secret bits during the embedding procedure behaves as an additional layer of protection against assaults. In a similar manner, utilize the last three (LSB) bits of the green channel and the last three (LSB) bits of blue channel pixels of the cover image to embed randomly the first three (MSB) bits of the second and third scramble grayscale images respectively. Changed pixels are then joined to create the stego image.

R.K.Thakur and C.Saravanan, 2016 [12] explain an analysis of image steganographic utilizing various bits of LSB embedding for 8-bit color images. The proposed method is accomplished utilizing (2-bit, 3-bit, 4-bit, 5-bit, and 6-bit) of the cover image while (7-bit, 1-bit) embedding aren't regarded due to the fact The 1-bit concealing will produce a bad nature for the retrieved secret image while 7-bit would produce a bad nature of stego image. The outcomes are compared among (2 bits to 6 bits) concealing. The comparative study of this value's outcome that the 4-bit concealing of (LSB) is the optimal consequence because of balances the nature of the stego image and retrieved secret image. However, (4-MSB) bits of a secret image is concealing only in (4-LSB) of the cover image.

P. Mathur and S.Adhikari , 2017 [13] propose a steganographic strategy that utilizes the grayscale image as cover and conceals the bits of secret grayscale image arbitrarily into first or second LSB of the grayscale cover image to increase the security. The random key which was utilized in embedding process should match the random key that utilizes to retrieve secret grayscale image because the random key that utilizes sets the concealing points of the secret data. This strategy primarily upgrades the security of the secret concealed data that embedded into the cover image. However, the extracted secret grayscale image at receiver side don't have same accurateness at the transmitter side.

C.A.Sari , et al , 2019 [14] propose a scheme that incorporates cryptography with steganography techniques utilizing (RGB color ,grayscale) as a cover image to conceal secret image (RGB color ,grayscale). In the proposed scheme, utilize the modified Triple Data Encryption Standards (T-DES) as encryption algorithms with a selective bits to develop the time execution. The description of the modified (T-DES) as follows: first, selected four (MSB) bits of the secret image, then it will be ciphered utilizing (T-DES). After that, combined that ciphered results with other four (LSB) bits. Then, embedded it into a cover image utilizing an inverted (LSB) method. The examining of images that encrypted utilizing the proposed encryption scheme demonstrates that the encryption method is twice quicker than classic (T-DES) and slightly quicker than utilize double (DES) and the concealing scheme created a better quality of stego image. However, the proposed method utilizes three independent keys.

H. H.Al.Ghuraify, et al, 2019[15] propose a data concealing scheme that provides four levels of security to secret message. The proposed scheme utilizes a dual cover image for concealing

cipher form of a secret message like the following procedure: The secret message firstly, cipher it by utilizing the modifying Vernam cipher principle with a private key that originates automatically then concealed that cipher form into grayscale cover image utilizing (LSB) algorithm. After that, encrypted the grayscale stego image by utilizing modifying vernam also then conceal it into another cover image of RGB color type utilizing (LSB) algorithm thus provides four levels of security to guard secret data.

H. H.Al.Ghuraify, et al [16] propose an approach for enhancing the security of (LSB) method where utilize either RGB color or grayscale as cover image to store secret data that be (secret image ,secret message ,both of them) founded on (LSB) algorithm based matrix partition principle into a spatial domain where the manner of hiding procedure as pursue : firstly, segregated a cover image into (Red, Green ,and Blue) matrices if both cover image and secret image of RGB color type then apply matrix partition to each channel separately to obtain (six partition) then concealing each partition separately after scramble each pixel of it by replace (LSB) with (MSB) while if both cover image and secret image of grayscale type, apply matrix partition to grayscale image to obtain (two partitions) then concealing each partition separately after scramble each pixel of it by replacing (LSB) with (MSB). The results illustrated that the scheme is effective to provide security for secret data.

3. PROPOSED SCHEME

3.1. Sending Part

3.1.1 The RGB cover image with a grayscale secret image

The general stages that involve in the sending part of this type depicted it in Fig .3 below.

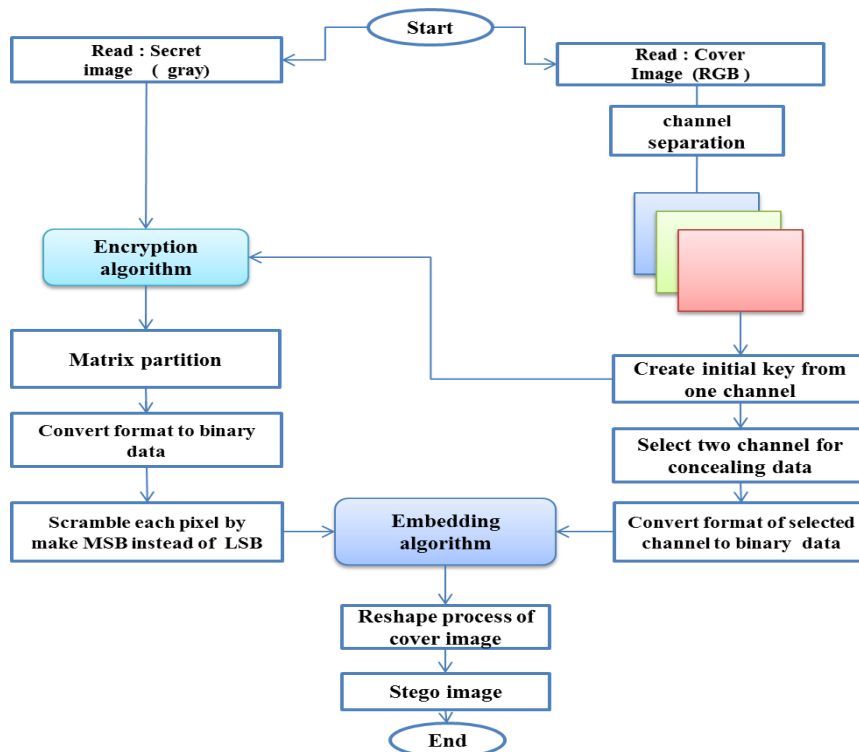


Fig 3: Block diagram of RGB cover image with a grayscale secret image

3.1.2. Grayscale Cover Image With RGB Secret Image

The general stages that involve in the sending part of this type depicted it in Fig.4below .

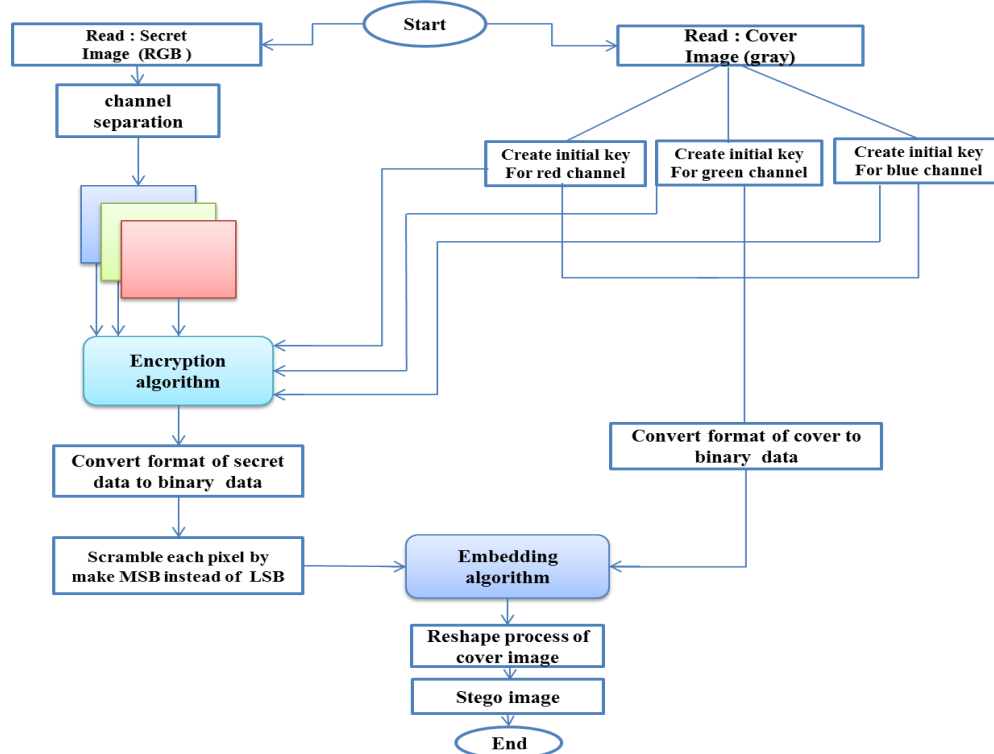


Fig 4 : Block diagram of grayscale cover image with RGB secret image

3.1.3 Depict the Embedding Algorithm

Fig.5 and Fig.6 explicated the implemented of an embedding algorithm of this type for both RGB color cover image and grayscale cover image respectively where describe the procedure for concealing one bit from one pixel of a secret image within one pixel of camouflage cover image as depicted below.

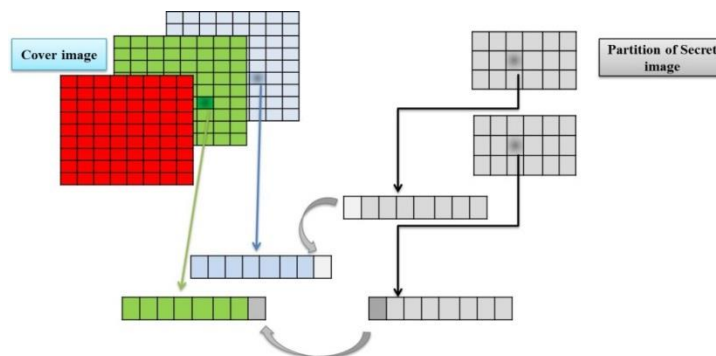


Fig .5:The Embedding Algorithm Of A Grayscale Secret Image Within RGB Cover Image

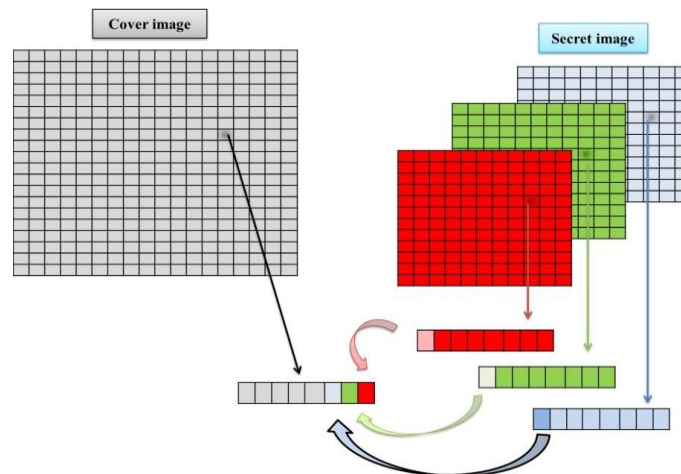


Fig.6 : The embedding algorithm of RGB secret image within grayscale cover image

3.1.4. Modyfing Vernam Scheme

The binary description of producing an encryption key for each channel of a private RGB color image as that depicted for the private grayscale image in Fig.7 below .

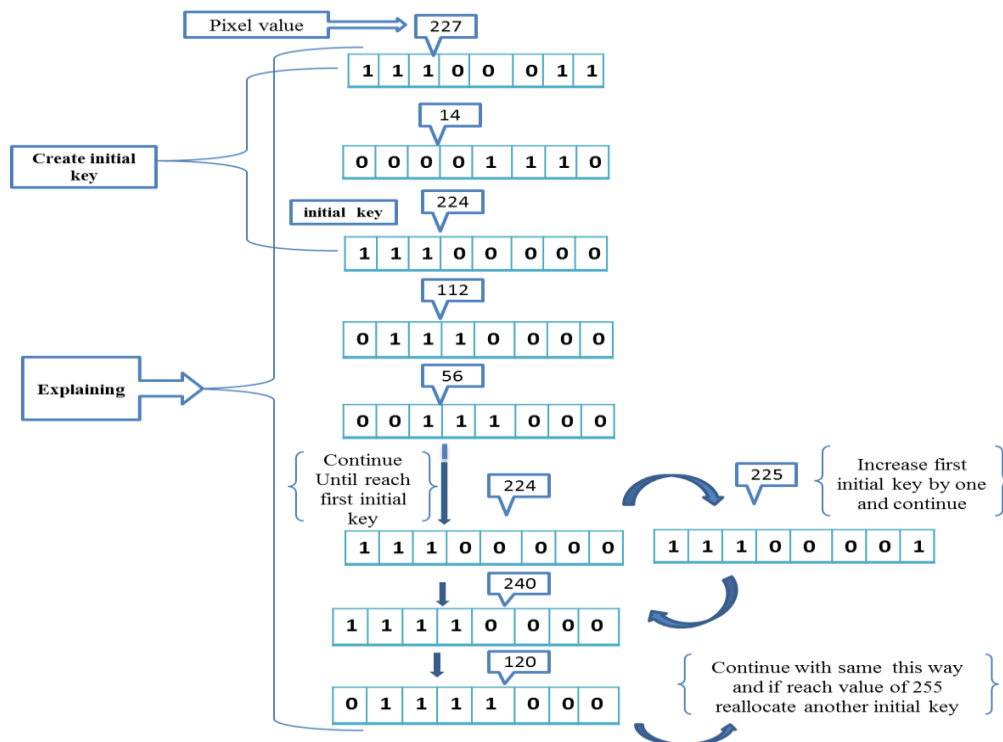


Fig.7 : The binary representation of creating an entire key, based on [15]

Fig.8 explains the algorithm that utilized to cipher both grayscale secret image and each channel of RGB color secret image separately in the cryptographic scheme as depicted below.

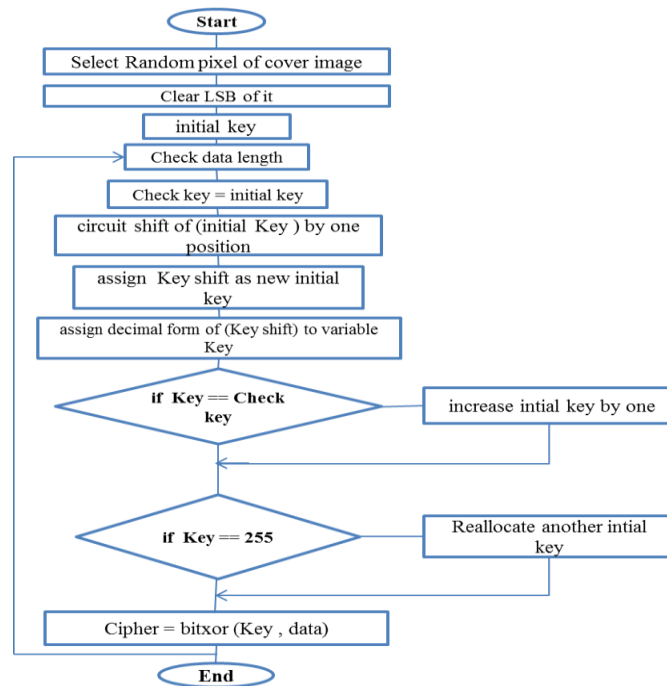


Fig.8 : The algorithms that utilized to cipher secret image

3.2. RECEIVING PART TO EXTRACT A SECRET IMAGE

The block diagram of extract secret data at recipient part depicts in Fig.9.

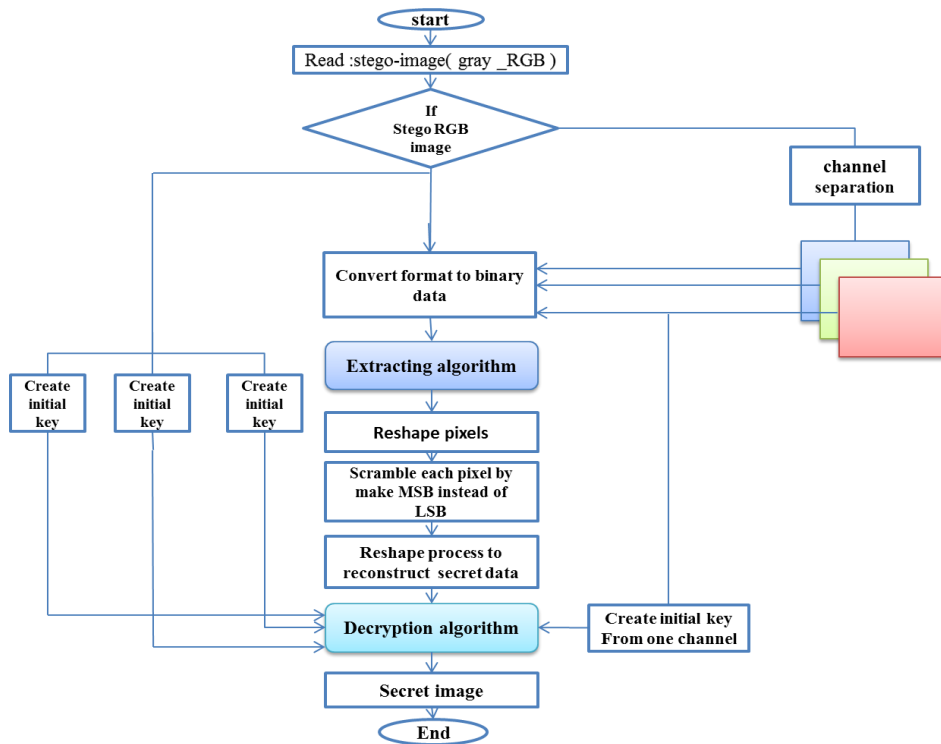


Fig. 9 :Block diagram to extract a secret image at the receiving side

4. EVALUATE THE PERFORMANCE OF THE PROPOSED SCHEME

The consequences of the concealing procedure were examined utilizing two-parameter as the following: Mean Square Error (MSE) and Peak Signal to Noise Ratio to confirm the attribute of the stego image that formation[17]. The two parameters are computed utilizing eq.1 and eq.2

$$MSE = \frac{1}{mn} \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} [Cover(x, y) - Stego(x, y)]^2 \dots \dots \dots (1)$$

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

(MSE) value has represented the value of error that happens into a stego image when regarded it to a cover image. The lesser value of it refers to achieve an elevated performance of a steganography algorithm while a bigger value of (PSNR) refers to that the image with secret data is precisely same to the image without secret data as stated by the visual quality that demonstrated the possess of elevated embedding efficiency. In general, if the value of (PSNR) is bigger than (30 dB), that is referred to extremely difficult to detect the act of distorting after concealing by human eyes [18]. On the other hand, The consequences of encryption scheme were examined utilizing three-parameter as the follow: histogram analysis, entropy, and processing times [14].

The histogram consequence of an encryption scheme which possesses a flat pattern, refer to reduce the opportunity of being assaulted utilizing a statistical manner[17] while the entropy value is utilized to specify the level of randomness into the images[14]. The entropy value is computed utilizing eq.3

$$Entropy(n) = - \sum_{i=0}^{255} probability(n_i) \log_2 probability(n_i) \dots \dots \dots (3)$$

The entropy value of the encrypted image must be close to the value (8) in order to prove the higher randomness that occurs into it [19]. The algorithms that require low time for implementing encryption and decryption procedure consider the best in term of encryption requirement.

5. IMAGES DATABASE

The secret image that utilized can be of diverse size according to a capacity that available into the camouflage cover image, to investigate the performance of the proposed scheme, we utilized (3) images of grayscale type with size (128×128) and (3) RGB color images with size (64×64) respectively as secret images. The explanation to select these images with those sizes is to compare the proposed cryptographic scheme with a cryptographic scheme in [14]. On the other hand the images that utilize as cover images, (1) RGB color images of size (512×512) and also (1) grayscale images of size (512×512), all image from Ref [20].

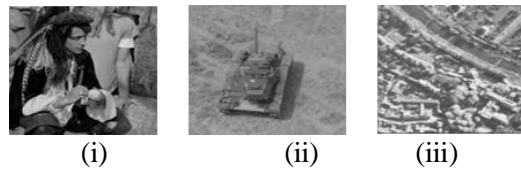


(i)



(ii)

(a) Cover Image: { (i) peppers.bmp , (ii) boat.bmp }



(b) Secret Images of grayscale type : { (i) indian.bmp, (ii) tank.bmp, (iii) aerial.bmp



(c) Secret Images of RGB color type : { (i) F16.bmp , (ii) lena.bmp, (iii) house.bmp }

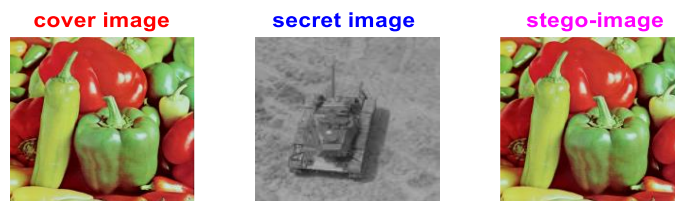
Fig.10: Images Database

6. SUMULATION RESULTS

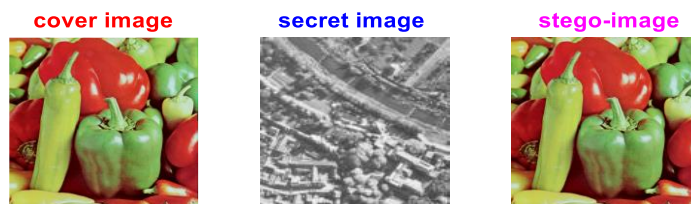
6.1 Visual quality of the proposed scheme using RGB color as cover images with secret images of grayscale type



(a) Pepper as cover image with indain as secret image



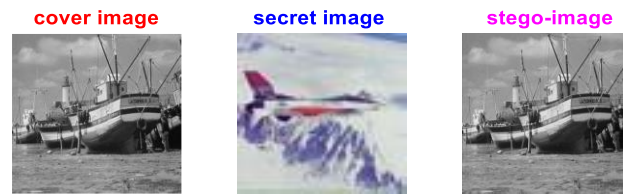
(b) Pepper as cover image with tank as secret image



(c) Pepper as cover images with aerial as secret image

Fig.11: {(a),(b),(c) Pepper as cover images with secret images of grayscale type }

6.2. Visual quality of the proposed scheme using grayscale as cover images with secret images of RGB color type



(a) Boat as cover image with F16 as secret image



(b) Boat as cover image with house as secret image



(c) Boat as cover image with lena as secret image

Fig.12: {(a),(b),(c) Boat as cover image with secret images of RGB color type }

Table 1 and Table 2 display the histogram of secret image before and after encryption for each grayscale and RGB color type respectively.

Table -1: Secret image of grayscale type with its histogram before and after encryption

Secret image	Histogram of secret image	Encrypted image	Histogram of encrypted image

Table -2:Secret image of RGB color type with its histogram before and after encryption



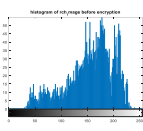


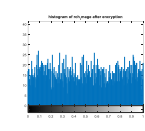

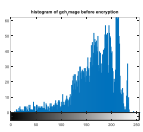

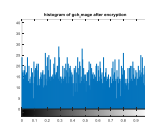

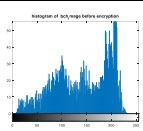

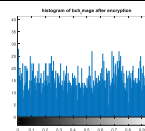


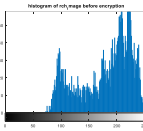
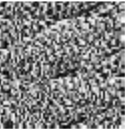

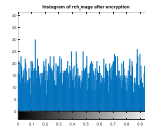

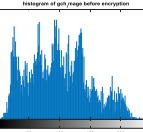
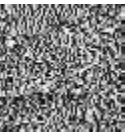


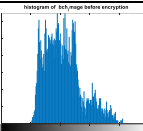

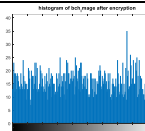

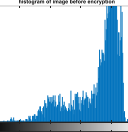



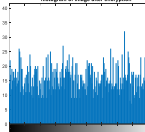
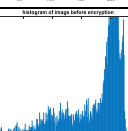


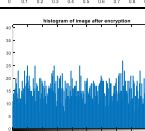
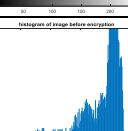


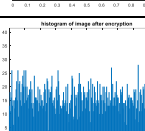
Secret image	Separate channel	Histogram of each channel	Encrypted channels	Encrypted Secret image	Histogram of encrypted channels
					
					
					
					
					
					
					
					
					

Table - 3: Appraisal the performance of a steganographic algorithm using RGB color as secret image

Detail		Proposed scheme	
Cover image	Secret image	MSE	PSNR
Boat	House	1.3725	46.7558
	F16	1.4454	46.531
	Lena	1.3344	46.8778

Table -4: The comparison with ref [14] for appraisal the performance of a cryptographic algorithm using RGB color as secret image

Details		cryptographic algorithm of ref [14]			Proposed cryptographic algorithm			
Cover image	Secret image	Entropy value	Time of encryption process/s	Time of decryption process/s	Entropy value	Time of encryption process/s	Time of decryption process/s	Initial key
Boat	House	7.9770	5.500971	6.410017	7.9815	0.99494	0.9796	128
	F16	7.9795	4.493580	4.683629	7.9847	0.953201	0.9960593	128
	Lena	7.9789	4.557636	4.747543	7.9850	0.959531	0.996949	112

Table - 5: Appraisal the performance of a steganographic algorithm using grayscale as secret image

Details		Proposed Scheme	
Cover image	Secret image	MSE	PSNR
Peppers	Indian	0.08304	58.9165
	Aerial	0.083321	58.9233
	Tank	0.083047	58.9376

Table - 6: Comparison with ref [14] for appraisal the performance of a cryptographic algorithm using grayscale image as secret image

Details		cryptographic algorithm of ref [14]			Proposed cryptographic algorithm			
Cover image	Secret image	Entropy value	Time of encryption process/s	Time of decryption process/s	Entropy value	Time of encryption process/s	Time of decryption process/s	Initial key
Peppers	Indian	7.9840	7.377887	6.339933	7.9888	1.103614	1.115365	176
	Aerial	7.9891	7.827122	6.126059	7.9898	1.44164	1.124792	
	Tank	7.9886	6.206587	7.457710	7.9899	1.09957	1.145587	

Figure 13 and Figure 14 demonstrate the graphical representation for the comparison with ref [14] using grayscale image and RGB color image respectively as secret data.

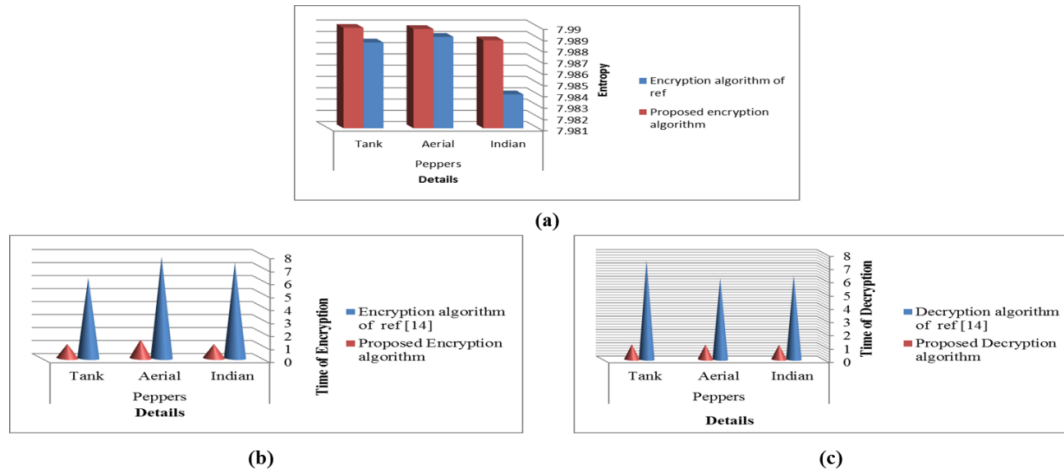


Fig .13: {(a,b,c) Show the graphical comparison with ref [14] using grayscale as secret image}

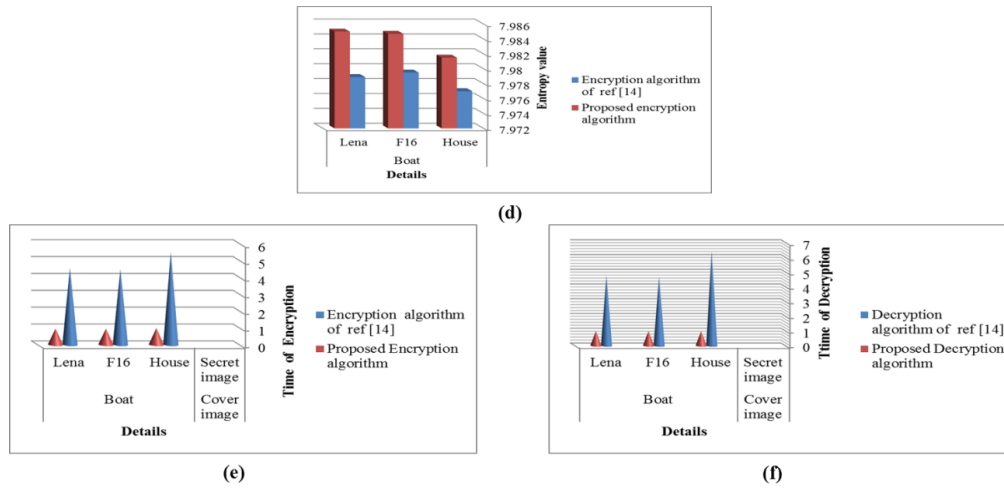


Fig .14: {(d,e,f) Show the graphical comparison with ref [14] using RGB color as secret image}

7. Conclusion

This paper exhibits a method for encryption secret image either grayscale type or RGB color type utilizes the modifying vernam principle. Utilizing the principle of modifying vernam for encryption color image using three initial keys from grayscale cover and also encryption grayscale image using the initial key from one channel of RGB cover image provide two features as below: first encrypt each channel of RGB color image separately without need to trade an encryption key then embedded each channel separately in grayscale cover image provide better vague for RGB color image. On the other hand, encryption of a grayscale image then camouflages it into a cover image of RGB color type offer also superior vague for a grayscale image. Second, the algorithm capable to handle all size of secret image with a key that extends along with the size of a secret image without require to trade it thus can utilize in the application that requires high security for secret image.

REFERENCES

- [1] Rejani. R, D. Murugan&D.V.Krishnan, (2015) "Comparative Study of Spatial Domain Image Steganography Techniques," Int. J. Advanced Networking and Applications, vol. 07, no. 02, pp. 2650-2657.
- [2] J. Singh,M. K. Garcha&G. Kaur,(2015) "Review of Spatial and Frequency Domain Steganographic Approaches," International Journal of Engineering Research & Technology, vol. 4, no. 06, pp. 1122-1125.
- [3] M. Hussain, A.W.A. Wahab, Y.I.B. Idris&A.T.S. Ho, K.-H. Jung, (2018) "Image Steganography in Spatial Domain : A Survey," Signal Processing: Image Communication,Elsevier.
- [4] H.A. Prajapati and N. G. Chitaliya, (2015) "Secured and Robust Dual Image Steganography : A Survey," International Journal of Innovative Research in Computer and Communication Engineering, vol. 03, no. 1, pp. 30-37.
- [5] T. Morkel , J.H.P. Eloff &M.S. Olivier, (2005) "AN OVERVIEW OF IMAGE STEGANOGRAPHY," Information and Computer Security Architecture (ICSA) Research Group, pp. 1-11.
- [6] N. Hamid,A.Yahya ,R. B. Ahmad,&O. M. Al-Qershi , (2012) "Image Steganography Techniques: An Overview," International Journal of Computer Science and Security (IJCSS), vol. 6, no. 3, pp. 168-187.
- [7] Z. Khan&A. Bin Mansoor, (2009) . "Evaluation of Wavelet Filters Performance for Steganalysis," 2nd International Conference on Computer, Control and Communication, IEEE, pp. 1-5.
- [8] Shikha&V. K. Dutt,(2014) "Steganography: The Art of Hiding Text in Image using Matlab," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 9, pp. 822-828.
- [9] D. Rawat and V. Bhandari, "A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image," International Journal of Computer Applications, vol. 64, no. 20, pp. 16-19, 2013.
- [10] N.Tiwari, M.Sandilya,&M. Chawla, (2014) "Spatial Domain Image Steganography based on Security and Randomization," International Journal of Advanced Computer Science and Applications, vol. 5, no. 1, pp. 156-159.
- [11] P.Das, S. C. Kushwaha ,&M. Chakraborty ,(2015) "MULTIPLE EMBEDDING SECRET KEY IMAGE STEGANOGRAPHY USING LSB SUBSTITUTION AND ARNOLD TRANSFORM," IEEE SPONSORED 2ND INTERNATIONAL CONFERENCE ON ELECTRONICS AND COMMUNICATION SYSTEM, pp. 845-849.
- [12] R. K.Thakur, Ch. Saravanan,(2016) "Analysis of Steganography with Various Bits of LSB for Color Images," International Conference on Electrical, Electronics, and Optimization Techniques,IEEE, pp. 2154-2158.
- [13] P. MATHUR, &S. ADHIKARI, (2017) "DATA HIDING IN DIGITAL IMAGES USING STAGNOGRAPHY PARADIGM: STATE OF THE ART," International Journal of Advances in Electronics and Computer Science, vol. 4, no. 2, pp. 98-102.
- [14] Ch. A. Sari, E.H. Rachmawanto, & E. J. Kusuma, (2019) "GOOD PERFORMANCE IMAGES ENCRYPTION USING SELECTIVE BIT T-DES ON INVERTED LSB STEGANOGRAPHY," Journal of a Science and Information, vol. 12, no. 1, pp. 41-49.

- [15] H. H. Al Ghuraify, A.A. Al-Bakry, &A.T. Al-Jayashi, (2019) "QUATERNION SECURITY USING MODIFYING VERNAM CIPHER WITH IMAGE STEGANOGRAPHY," The International Journal of Multimedia & Its Applications, vol. 11, no. 3, pp. 1-20.
- [16] H. H. Al Ghuraify, A.A. Al-Bakry, & Ahmad T. Al-Jayashi, (2019) "DUAL SECURITY USING IMAGE STEGANOGRAPHY," International Journal of Network Security & Its Applications (IJNSA), vol. 11, no. 2, pp. 14-31.
- [17] E.J. Kusuma, Ch. A.Sari, E. H. Rachmawanto, and D. R. I.M. Setiadi, (2018) "A Combination of Inverted LSB, RSA, and Arnold Transformation to get Secure and Imperceptible Image Steganography," J. ICT Res. Appl., vol. 12, no. 2, pp. 103-119.
- [18] H. Ogras, (2019) "An Efficient Steganography Technique for Images using Chaotic Bitstream," I. J. Computer Network and Information Security, vol. 2, pp. 21-27.
- [19] S. Namasudra & G. Ch.Deka, (2019) "Advances of DNA Computing in Cryptography", Taylor&francis Group.
- [20] "SIPI Image Database," [Online].

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 Technical 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 received his B.Scand M.Sc.in electrical engineering department, college of engineering, university ofBaghdad, 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 stabilityand 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 College, AL-Furat AL-Awsat Technical University. His interested control theory,advance image processing,security of communication system,robotics mainpulation systems. He hadbeen chosen as a reviewer for many journals and conferences.

