An Approach for Embedding the Colored Secret Image based on Multi-Cover Sharing Scheme

Dr.Mahmood Zaki Abdullah
Assistant professor
Computer Engineering Department
Al-Mustansiriyah University
Baghdad-Iraq
Email: drmzaali@gmail.com
zinah jamal Khaleefah
Computer Engineering Department
Al-Mustansiriyah University
Baghdad-Iraq
Email: zinah_jamal@yahoo.com

Abstract:-

Cryptography and steganography are the two major techniques used for securing the information during communication. This paper proposed an algorithm for cryptography and steganography based on image sharing and chaotic system (ISCS), Where the ISCS algorithm has been applied to perform three operation. firstly, encrypt the secret color image based on Lorenz chaotic map. Then, sharing the cipher image to n shadow based on secret sharing scheme. Finally, embedding n shadow with n cover images. Several security analysis for image encryption are used, such as secret key space and sensitivity, histogram, autocorrelations, entropy, and differential analysis. The peak signal to noise ratio PSNR is used for testing and measuring the quality and performance for cover images of the proposed algorithm. With numerical simulation results, The proposed ISCS algorithm have high level for security, large key space for image encryption and high payload capacity reached to 0.75 M of pixels that embedding in four cover images size (512*512) with quality reached to 44 db of PSNR.

Keywords: Steganography, cryptography, Lorenz chaotic map, secret sharing scheme.

1. Introduction

The development of communication and mobile systems needs to be important to use modern approaches to information security. Cryptography and steganography are the most important types that can provide information security, The Cryptography can scramble a message so it cannot be understood but, while the steganography can hide the message so it cannot be seen. The combination of these two methods will maintain the confidentiality of the data encrypted and enhance the security of the data embedded[13]. The secret image sharing scheme with steganography provided a new technique for data secret [3]. The main aim of this paper is to produce a new approach that can give a high capacity of hiding information of secret image embedding the colored secret image based on multi-cover sharing scheme.

Steganography is a technique of hiding information through scrambling a message. The meaning of steganography is derived principally from the Greek words steganos, which means “covered”, and graphia, which means “writing”. The main building blocks of any steganographic algorithm are based on cover media, the establishing and extracting algorithms, and Stego [8]. Any steganographic algorithm that is used must be having the following characteristics:

1) embedding capacity: is the maximum number of bits that can be hidden in a given cover work [8].
2) Robustness: The algorithm must be robust against different attacks from any intruder [5].
3) Security: a secure steganographic scheme means a statistically undetectable scheme [8].
4) Imperceptible: It is the ability of steganography rule to avoid revelation of hidden message through the human visual system (HVS) and statistical analysis. It can be weighted through peak signal to noise ratio (PSNR) [9].

Cryptography is the science of secret writing with the aim of securing the meaning of a message [4]. Cryptography was formed as a method for hiding information and maintains the secrecy of the communication system, so different techniques have been adapted to encrypt and decrypt information in order to hide the original meaning of the message [9].

In 1963, Edward N. Lorenz tries to build a system of differential equations that would clarify some of the unpredictable manners of the weather. Lorenz discussed a various and simpler to analyze system [11]. When anybody thinks about a chaotic system, the first thing that comes to mind is “Unpredictability”. Lorenz has contrived a system of three differential equations known as Lorenz equations form, as given in equations (1), (2), and (3) [8] .

$$dx/dt= \sigma\ (y-x) \tag{1}$$

$$dy/dt= \gamma\ x-xz-y \tag{2}$$

$$dz/dt=xy- \beta\ z \tag{3}$$

Where t, x, y, z, σ, γ , $\beta \in R$ and σ, γ, β are positive constants. If $\sigma = 10$ and $\beta = 8/3$, when $\gamma > 24.74$, the dynamical orbit will be confused [13]. Lorenz equations are very sensitive to initial conditions; this is one of the main properties of a confused system [11].

Secret Sharing Scheme based Shamir (t, n) threshold scheme to fulfill spread storage, was firstly created by Shamir in 1979. In (t, n) threshold scheme provided rule of sharing secret message among n shadow, t and n are positive integer numbers and t less or equal to n. The secret message can be recovered only with the number of shadows equal to t or more than t. The shadow array obtains from equation (4) [6]:

$$s(x_n)=m+s_1x_n+.....+s_{t-1}x_n^{t-1} \bmod p \quad (4)$$

2. Related Works

The related works can be classified into three domains: image cryptography based chaotic rule, secret sharing scheme, hiding the secret image in cover based on the chaotic rule.

In[10] presented a good steganography algorithm with two-stage authentication for secret image sharing, this algorithm provided an enhancement in both quality of stego image and security of secret image.

In [12] presented a new scheme for image steganography based on different size image segmentation (DSIS) and gives its modification.

In [13] presented an algorithm for image steganography with higher confidentiality and high capacity based on Lorenz chaotic map and Kekre's Advanced Multiple LSB Algorithm (KAMLA).

In [1] developed a new technique for image steganography based on encrypted secret image by Lorenz, hide encrypted data with 3 level Discrete Wavelet Transform.

In [15] presented an algorithm for data encryption scheme based on cellular automata and chaotic map that employs piecewise linear nonlinearity, this scheme offers high level of security and fast processing time.

In [2] the proposed method gives a good distribution for the secret image among participant, this method based on (t, n) threshold secret sharing scheme, without loss of information.

In [7] the proposed an algorithm for image encryption with two-dimensional transform with a key quantum chaotic map, this rule, offers a high level security for information.

In [3] gave a new approach to secret image sharing with steganography, this approach can save storage space with enhances the quality of the secret image.

In [16] gave a new approach to secret image sharing based on linear cellular automata, hash functions, and digital signature to proposed a novel (t,n) threshold image sharing scheme with steganography.

3. Proposed Method

The proposed algorithm in this paper contains two main parts: embedding part and extraction part.

In the embedding part, they are three phases: image encryption, secret sharing scheme and image steganography. The phases of the proposed algorithm are as follows, which is shown in **Fig. 1.**

Phase1: encrypts the secret image with Lorenz chaotic equations to increase the confidentiality.

Phase2: divides the encrypted image from phase1 to four shadows based on secret sharing scheme to distributed these shadows to the four cover images.

Phase3: embeds the shadows from phase2 with cover images based on random sequence generated from Lorenz equations.

A. Lorenz Encryption Phase

Random values with very sensitive to initial values are generated with Lorenz system. The encryption process for the secret image is done in the following steps which are shown in **Fig. 2**.

Input: secret image, secret key (32 ASCII char.), and sensitive parameters.
output: cipher image.
steps:

1) XOR function applied between fraction part from the mean of secret key and plain images as shown in **Fig. 3**. The result was enter to the Lorenz chaotic system.
2) Three array x, y, z are generated.
3) Apply some process on x,y,z arrays value are generated from step1 and change the value of the x,y in ascending sequence.
4) Save the index of the x arrays to generate key1.
5) XOR function applied between y and z array to generate key2.
6) Divided the secret image to blocks with size 8*8.
7) Scrambling the bits for each block with key1.
8) XOR function applied on secret image with key2 array in the forms of row, column, lower triangular and upper with two directions triangular as shown in **Fig. 4**.

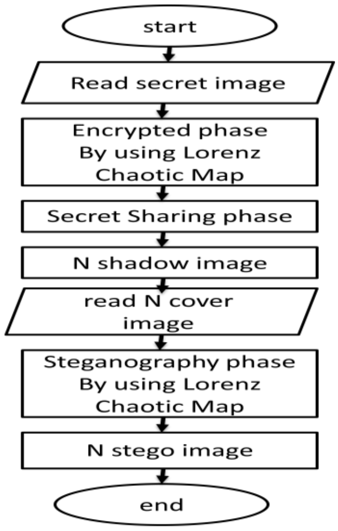

Fig. 1 The proposed algorithm for embedding part.

B. Secret Sharing Scheme Phase

Apply a (t, n) threshold scheme on the encrypted image to generated n different shadow. In proposed algorithm take t=4 and n =4, The process for sharing is done in the following steps which are shown in **Fig. 5**.

Input: cipher image.

output: n shadow.

steps:

1) Reshape the input image to new dimension r rows and t columns.
2) for each row of the array from step 1, apply the Shamir's threshold scheme equation [6]:

$$s_j(x_i) = s_{j0}+s_{j1}x_i+s_{j2}x_i^{\,2} \mod 257 \quad (5)$$

the value of base number equals 257. since the value of the color or gray image is between 0 and 255, 257 is the closest prime number to 255.

3)Repeat step2 with n different integers values of x_1, x_2, x_3, x_4.

4)Four shadow $s(x_1)$, $s(x_2)$, $s(x_3)$, and $s(x_4)$ are generated.

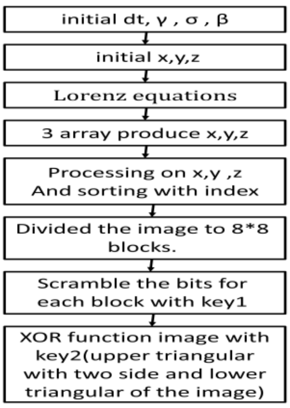

Fig. 2 The encryption phase with Lorenz map.

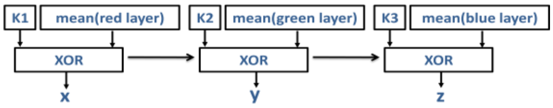

Fig. 3 Generation the initial values for Lorenz map.

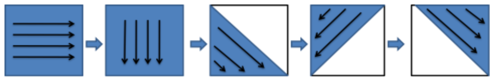

Fig. 4 The direction of the XOR function.

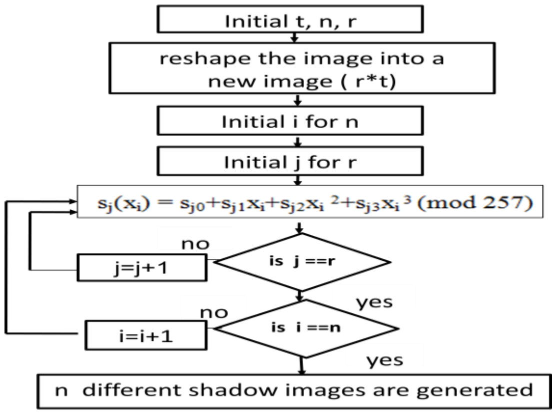

Fig. 5 The secret sharing phase.

C. Steganography Phase

Embedding process in this phase take randomly sequence based Lorenz equations, these process is done in the following steps which are shown in **Fig. 6**.

Input: n cover image, n shadow.

output: n stego image.

steps:

1) x,y,z arrays are generated with new initial value.
2) For each i-th cover image divided into 8*8 blocks.
3) select the blocks sequence with x,y,z arrays, with x,y selected the

sequence of the blocks in i-th cover and z selected the sequence of the pixels in the blocks.

4) Embedding the i-th shadow in blocks of i-th cover with pre-selected these blocks in step 3 with LSB method.

In secret sharing scheme phase with step2, It is possible that the value of the pixel in shadow equal 256, These values take nine bits rather than eight bits. In the proposed algorithm, for every eight pixels embedding nine bits with LSB for pixels as shown in **Fig. 7**, These step provided the maintain for the quality of the secret image when extracting.

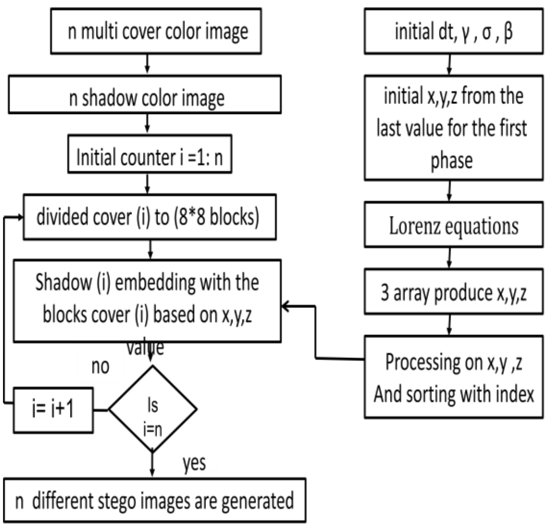

Fig. 6 Steganography phase.

b_{11}...b_{14}......$b_{17}b_{18}$	b_{21}...b_{24}......$b_{27}b_{28}$	b_{31}...b_{34}......$b_{37}b_{38}$	b_{41}...b_{44}......$b_{47}b_{48}$
b_{51}...b_{54}......$b_{57}b_{58}$	b_{61}...b_{64}......$b_{67}b_{68}$	b_{71}...b_{74}......$b_{77}b_{78}$	b_{81}...b_{84}......$b_{87}b_{88}$

(a)

b_{11}...b_{14}......s1s2	b_{21}...b_{24}......b_{27}s3	b_{31}...b_{34}......b_{37}s4	b_{41}...b_{44}......b_{47}s5
b_{51}...b_{54}......b_{57}s6	b_{61}...b_{64}......b_{67}s7	b_{71}...b_{74}......b_{77}s8	b_{81}...b_{84}......b_{87}s9

(b)

Fig. 7 The embedding method, (a) 8-pixels of the 8*8 pixels block in the cover image, (b) 9-Secret bits embedded with these pixels.

In the extracting part, all the phases in embedding part applied with reverse direction, The phases of the proposed extracting algorithm are as follows, which is shown in **Fig. 8**.

Phase1: extracted n shadows from n cover images based on the random sequence generated from Lorenz equations.

Phase2: inverse secret sharing scheme applied on n shadow to produce an encrypted secret image.

Phase3: Decrypts the secret image with Lorenz chaotic equations to produce the secret image.

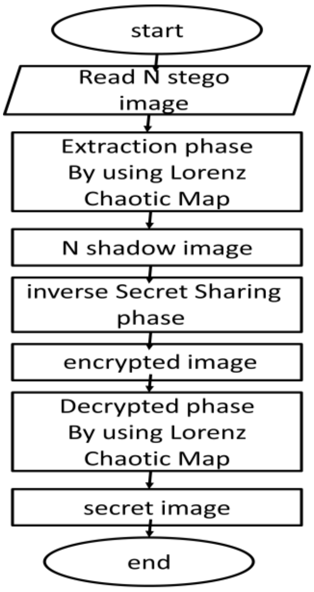

Fig. 8 The proposed algorithm for extracting part.

4. Experimental Result

In proposed algorithm, two parts are performed in this section : In the first part, check the performance of proposed encryption algorithm with cipher image.

A. **Encryption and Histogram**

An ideal cipher image should have a uniform distribution about the frequency. Two images (baboon 512*512 and sailboat 512*512) from the USC-SIPI image database were used in the proposed encryption algorithm as shown in the **Fig. 9, 11**. These images tested with histogram, The result shown in the **Fig. 10, 12**. In the flowing the secret keys are used.

k1=Z&QBZH8ATBaCdaFEHijkkl-Z23456N#9

k2=B2BB5M7#AC%+cdEfgQijNkl m1M%4567#

k3=BZHO56BZ8AAbCdeRgHiJk*l %1234567#

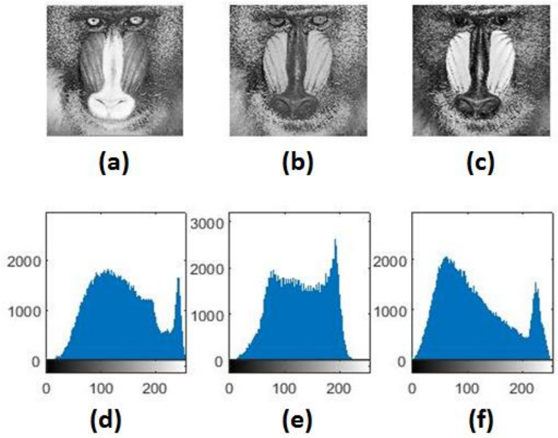

Fig. 9 The secret image baboon, (a) Red layer, (b) Green layer, (c) Blue layer, (d) Histogram for red layer, (e) Histogram for green layer, (f) Histogram for blue layer.

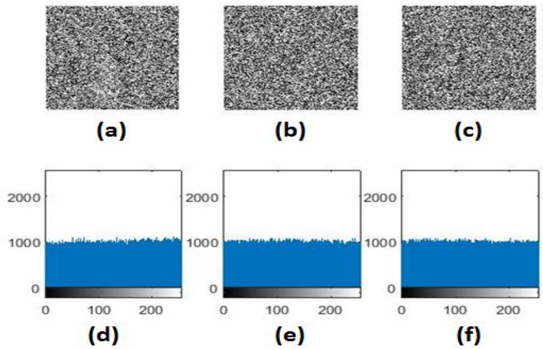

Fig.10 The secret image baboon encrypted, (a) Red layer, (b) Green layer, (c) Blue layer, (d) Histogram for red layer, (e) Histogram for green layer, (f) Histogram for blue layer..

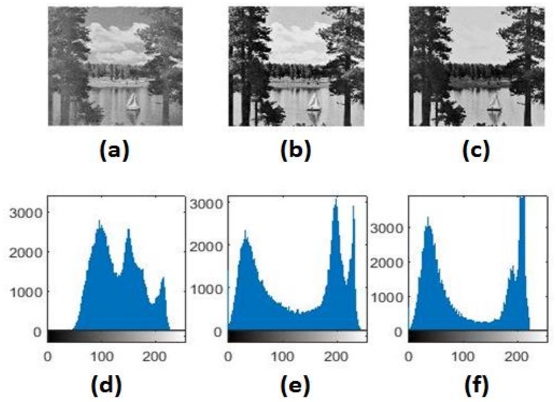

Fig. 11 The secret image sailboat, (a) Red layer, (b) Green layer, (c) Blue layer, (d) Histogram for red layer, (e) Histogram for green layer, (f) Histogram for blue layer.

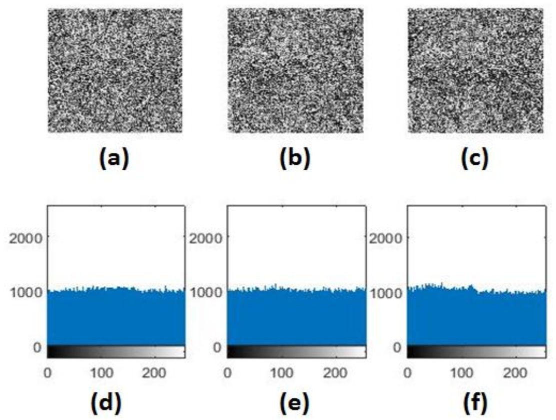

Fig. 12 The secret image sailboat encrypted, (a) Red layer, (b) Green layer, (c) Blue layer, (d) Histogram for red layer, (e) Histogram for green layer, (f) Histogram for blue layer.

B. Secret Key Space

In the proposed algorithm, three key (32 ASCII char.) are used. For each ASCII char have 2^7 possible values, then the proposed algorithm have $(2^7)^{32*3} = 2^{672}$ possible key size.

C. Secret Key Sensitivity

A good encryption system must be very sensitive with secret keys[15]. **Fig. 13**, show the decrypted baboon image by using the wrong key.

k1=Y&QBZH8ATBaCdaFEHijkklZ23456N#9
k2=B2BB5M7#BC%+cdEfgQijNkm1M%4567#
k3=BZHO56BZ8AAbCdeRgHiJk*l%1234567#

D.Correlation Coefficient Analysis

Correlation values determine the relationship between original image and cipher image [15], **Table.1** show the results of the correlation between them for each layer (red, green, and blue).

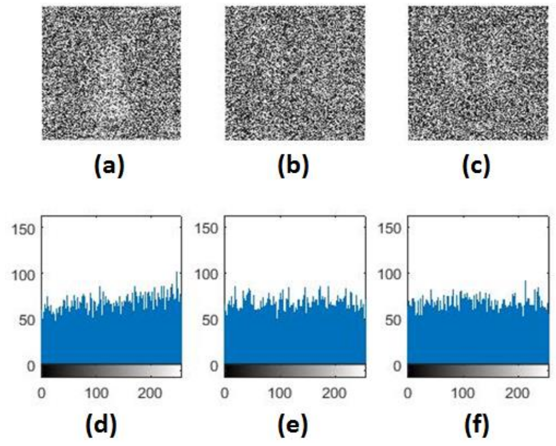

Fig. 13 The secret image baboon encrypted with wrong key, (a) Red layer, (b) Green layer, (c) Blue layer, (d) Histogram for red layer, (e) Histogram for green layer, (f) Histogram for blue layer.

Table.1 Correlation Coefficient Of The Original And Cipher Images.

Correlation	
Layers	**Correlation Result**
C_{RR}	0.000801
C_{RG}	0.008324

Correlation	
Layers	**Correlation Result**
C_{RB}	0.013390
C_{GR}	0.004451
C_{GG}	0.006319
C_{GB}	0.013551
C_{BR}	0.008920
C_{BG}	0.006611
C_{BB}	0.011195

E. Information Entropy Analysis

Information entropy represents the probability of the pixel value in the original and cipher image, **Table.2** show the results of the entropy for both original and cipher image for each layer. The entropy calculated with equation below, $p(m_i)$ denotes the probability of symbol m_i [15].

$$H(m)=\sum_{i=0}^{2^N-1} p(m_i)\ \log_2\left(\frac{1}{p(m_i)}\right) \quad (6)$$

Table.2 Information Entropy Of The Original And Cipher Images.

Information Entropy			
Image	**Red**	**Green**	**Blue**
Oreginal	7.248629	7.587695	6.926869
Cipher	7.996827	7.997011	7.997061

F.Differential Analysis

NPCR (Net Pixel Change Rate) and UACI (Unified Average Changing Intensity) are two measurements to evaluate the relationship between two encrypted images when change one pixel value of original image [15], **Table.3** show the results of the NPCR and UACI for two cipher images. The NPCR and UACI are calculated with equations below, c1(i) c2(i) are the pixels of cipher image and N is the number of the pixels.

$$NPCR=\frac{\sum_{i=1}^{N} W(i)}{N}*100\% \quad (7)$$

$$W(i)=\begin{cases}0, & if\ c1(i)=c2(i)\\ 1, & if\ c1(i)\neq c2(i)\end{cases} \quad (8)$$

$$UACI=\frac{100}{N*255}\sum_{i=1}^{N}|c1-c2| \quad (9)$$

Table.3 NPCR And UACI Results.

NPCR and UACI			
	Red	**Green**	**Blue**
NPCR	99.560547	99.603271	99.650574
UACI	32.718482	32.767418	32.841845

In the second part, check the quality of the stego images. The PSNR is calculated from below equation [14].

$$PSNR=10*\log((255)^2/MSE) \quad (10)$$

Baboon secret image with tree different size (128*128 - 256*256 - 512*512) as shown in the **Fig. 14** was embedding with cover images. Four cover images from the USC-SIPI database with size 512*512 as shown in the **Fig. 15**. The results of PSNR for the stego images are as follows in **Table. 4**, and shown in the **Fig. 16, 17, and 18**. The secret image extracted from the stego images based on extraction proposed algorithm as shown in the **Fig. 19**.

Table.4 PSNR Result For Cover Images.

Secret Image Size	Cover with Size 512*512	PSNR
128*128	Sailboat	62.3767 db
	Baboon	62.5201 db
	Airplane	67.9313 db
	Peppers	60.9228 db
256*256	Sailboat	54.7777 db
	Baboon	55.2847 db
	Airplane	59.5838 db
	Peppers	54.4472 db
512*512	Sailboat	44.4009 db
	Baboon	44.2718 db
	Airplane	50.0085 db
	Peppers	43.8685 db

Finally, **Table. 5** summarizes the comparison between the proposed algorithm in [4] and our proposed algorithm with PSNR measure. In these algorithms, five test gray images (USC-SIPI Image Database) are used, one as secret image (Airplane Jet-F16) with size 256*256 and four cover images (Lena, Pepper , Baboon , and Elaine) with size 512*512.

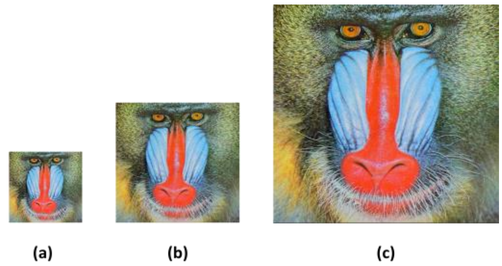

Fig. 14 Baboon secret image (a) Size 128*128, (b) Size 256*256, (c) Size 512*512.

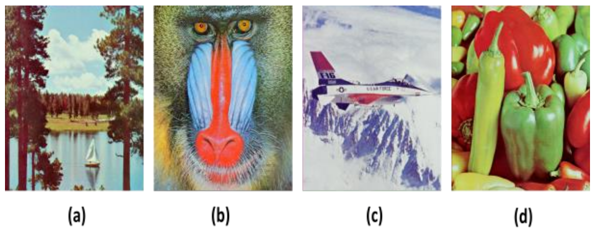

Fig. 15 Cover images (a) Sailboat, (b) Baboon, (c) Airplane, (d) Peppers.

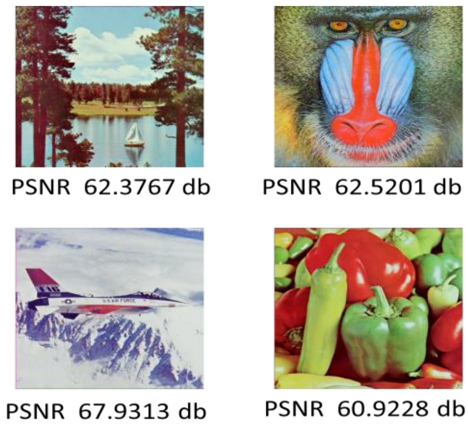

Fig. 16 PSNR result for stego images when embedding (128*128) secret image.

Table.5 Comparison Between Conventional Method and Proposed Method With PSNR.

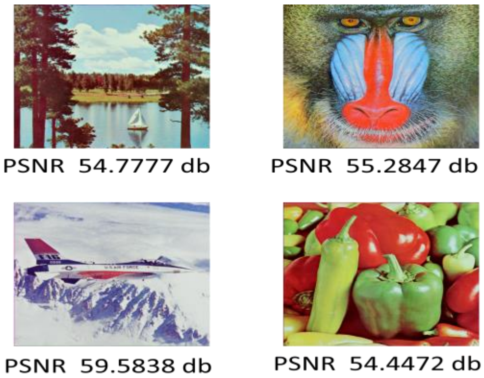

Fig. 17 PSNR result for stego image when embedding (256*256) secret

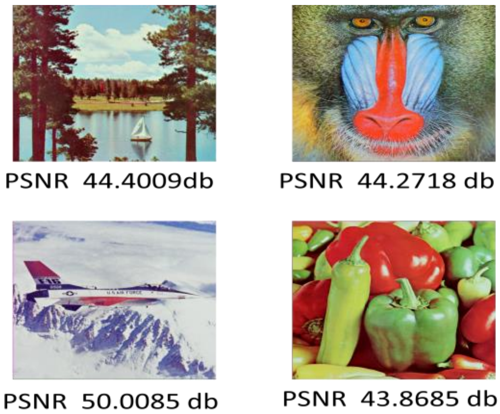

Fig.18 PSNR result for stego image when embedding (512*512) secret image.

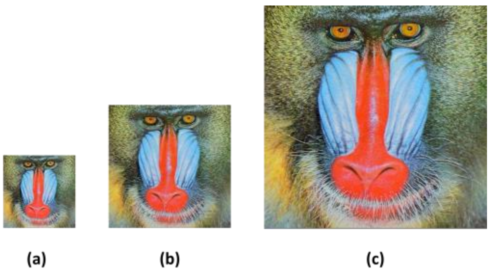

Fig. 19. The baboon secret image after extraction (a) Size 128*128, (b) Size 256*256, (c) Size 512*512.

Methods	Cover with Size 512*512	PSNR
Conventional Method (Ref. [10])	Lena	49.47 db
	Pepper	49.47 db
	Baboon	49.50 db
	Elaine	49.51 db
Our Proposed Method	Lena	55.20 db
	Pepper	54.95 db
	Baboon	55.72 db
	Elaine	56.39 db

5. Conclusion

In this paper a novel method of steganography has been proposed. Which is using Lorenz chaotic map to encrypt the secret image and secret sharing scheme for secret sharing with multi-cover images. As mentioned in Sec. 3, The ISSC proposed method achieved main goals:

1) Achieving a high level for security, large key space for image encryption by:

a) Encrypts the image with sensitive encrypted key based Lorenz chaotic map in the proposed algorithm.

b) Sharing the secret image to four shadows based secret sharing schemes.

c) Embeds the secret image with Lorenz chaotic map in the proposed algorithm.

2) high payload capacity reached to 0.75 M of pixels that embedding in four cover images size (512*512) with quality reached to 44 db of PSNR.

References

1. B. G. Banik and S. K. Bandyopadhyay,2015,“Secret Sharing using 3 level DWT method of Image Steganography based on Lorenz Chaotic Encryption and Visual Cryptography”, International Conference on Computational Intelligence and Communication Networks, IEEE.
2. B. L. Sirisha, S. S. Kumar and B. C. Mohan, 2016, “Steganography based image sharing with reversibility”, Journal of Discrete Mathematical Sciences & Cryptography, Vol. 19, No. 1, pp. 67–80.
3. C.C. Wu, M.S. Hwang and S.J. Kao, 2009, “ A new approach to the secret image sharing with steganography and authentication ” , The Imaging Science Journal, Vol 57.
4. C. Paar and J. Pelzl, 2010, “ Understanding Cryptography “,springer.
5. D. A and S. Thenmozhi, 2016, “Steganography: Various Techniques In Spatial and Transform Domain”, International Journal of Advanced Scientific Research and Management, Vol. 1 Issue 3, March.
6. E. B. Abdelsatir, S. Salahaldeen, H. Omar, and A. Hashim, 2014, “A Novel (K,N) Secret Sharing Scheme From Quadratic Residues For Grayscale Images”, IJNSA, Vol.6, No.4.
7. H. Liu and C. Jin, 2017, “A Color Image Encryption Scheme Based on Arnold Scrambling and Quantum Chaotic”, International Journal of Network Security, Vol.19, No.3, PP.347-357.
8. I. J. Cox, M. L. Miller, J. A. Bloom, and J. Fridrich, 2008, “Digital Watermarking and Steganography”, 2nd ed., Morcan Kaufmann, pp.425-430.
9. I. Maurya, 2016, “An Analysis of Key Dependent Image Steganography using Hybrid Edge Detection in Spatial Domain”, IJCST Vol. 7, Issue 3, July.
10. L. Liu, A. Wang, C. Chang, and Zhihong Li, 2017, “A Secret Image Sharing with Deep-steganography and Two-stage Authentication Based on Matrix Encoding ”, International Journal of

Network Security, Vol.19, No.3, PP.327-334.

11. M. W. Hirsch, S. Smale, and R. L. Devaney, 2013, “Differential Equations, Dynamical Systems, and an Introduction to Chaos”, 3ed ed., The Boulevard, Langford Lane, Kidlington, Oxford, pp.307-309.
12. O. M. Al-Shatanawi and N. N. El. Emam, 2015, “A New Image Steganography Algorithm Based on Mlsb Method with Random Pixels Selection”, International Journal of Network Security & Its Applications, Vol.7, No.2, March.
13. R. Moieni, S. Ibrahim, and L. Roohi, 2013, “A High Capacity Image Steganography Method Using Lorenz Chaotic Map ”, ACIT.
14. V.S.Vora, Prof. A.C.Suthar, Y.N.Makwana, and S.J. Davda, 2010, “Analysis of Compressed Image Quality Assessments ”, Published in International Journal of Advanced Engineering & Application, Jan.
15. W. Srichavengsup and W. San-Um, 2016, “Data Encryption Scheme Based on Rules of Cellular Automata and Chaotic Map Function for Information Security”, International Journal of Network Security, Vol.18, No.6,PP.1130-1142,Nov.
16. Z. Eslami, S. H. Razzaghi,and J. Z. Ahmadabadi, 2010, “Secret image sharing based on cellular automata and steganography,” Elsevier, Pattern Recognition 43, pp.397-404.

نهجا يرتكز على أخفاء صورة سرية ملونة مبنية على مخطط مشاركة متعددة التغطية

د.محمود زكي عبد الله
استاذ مساعد
قسم هندسة الحاسوب
الجامعه المستنصرية
زينة جمال خليفه
قسم هندسة الحاسوب
الجامعه المستنصرية

الخلاصة:

التشفير والتخزين هي التقنيات الرئيسية المستخدمة لتأمين المعلومات أثناء الاتصالات. تقترح هذه الورقة خوارزمية للتشفير والتدريج على أساس تقاسم الصور ونظام الفوضى، حيث تم تطبيق هذه الخوارزمية لأداء ثلاث عمليات. أولا، تشفير الصورة السرية الملونة على أساس مبدأ لورينز (خريطة الفوضى). ثم، تقاسم الصورة المشفره إلى عدد غير محدد من بيانات الظل على أساس مخطط تقاسم السرية. أخيرا، تضمين هذا العدد من بيانات الظل مع عدد من صور الغطاء. تم استخدام العديد من التحليل الأمني لتشفير الصور، مثل سعة وحساسية المفتاح السري، الرسم البياني، مدى الترابط بين البيانات المشفره، الإنتروبيا، والتحليل التفاضلي. وتستخدم نسبة ذروة الإشارة إلى الضوضاء لاختبار وقياس نوعية وأداء صور الغلاف للخوارزمية المقترحة. تم تطبيق الخوارزمية المقترحة في هذا البحث فكانت الخوارزميه المقترحة لديها مستوى عال للأمن، سعة وحساسية المفتاح السري, سعه حجم البيانات السرية تصل الى 0.75 MB المضمنه داخل اربع من صور الغطاء ذات حجم 512*512, مع الحفاظ على جودة صور الغطاء التي تصل الى 44 db من نسبة ذروة الاشارة الى الضوضاء.