Suggested Method for Encryption and Hiding Image using LCG and LSB

Atheer Hussein Zyara
Department of Community Health , College of Health and Medical Technology , Kufa \ Foundation of Technical Education , University of Al- Furat al- Awsat techniques
wwatheer@yahoo.com

Abstract

Maintaining the confidentiality of the data of the very important areas in computer applications , Where many researchers work in the fields of concealment and encryption . So in this research we are working on the combining of the two methods , where confidential data is encrypted by using a proposed method , Then the cover is encrypted (regular image) by LCG algorithm (which generates a series of random numbers) to generate the encrypted cover (irregular image) , After that ,we hide the encrypted data in encrypted cover by depending on the LSB technique, then we convert the irregular image into regular image and thereby getting hidden data in random locations in the cover image , This method is characterized by flexibility in terms of the possibility of hiding the different types of confidential data in different types of media , and durability as that data be hidden in random locations and this what distinguishes the proposed algorithm , and the results showed high security, because the data is hidden in random locations in encrypted image then convert to the original regular image For clarification of the proposed algorithm , it has been applied on a digital image of the gray type using MATLAB language by using the efficiency scales PSNR and MSE .

Keywords : encrypting , hiding , random locations , LCG algorithm , LSB technique, cover image, encoded image , PSNR , MSE .

الخلاصة

من أجل الحفاظ على سريّةِ البياناتِ مِنْ المجالات المهمةِ جداً في تطبيقاتِ الحاسوبِ، عمل العديد مِنْ الباحثين في مجال الإخفاءِ والتشفيرِ لذا في هذا البحثِ نحن نَعْملُ على الجَمْع بين الطريقين، حيث أنَّ البيانات السرّية هي مشُفّرَةَ بإستعمال طريقة مقترحة، ثمّ يتم تُشفيّرُ الغطاءَ (الصورة المنتظمة) بواسطة خوارزميةِ LCG (الذي يُولّدُ سلسلة من الأعدادِ العشوائيةِ) لتَوليد الغطاءِ المشفّرِ (صورة غير منتظمة)، بعد ذلك نحن نَخفي البياناتَ المشفّرَةَ في الغطاءِ المشفّرِ بالإعتِماد على تقنيةِ LSB ، ثمّ تحوّلُ الصورةَ غير المنتظمة الى صورةِ منتظمةِ، وبذلك نحْصلُ على بياناتِ مخفيةِ في مواقعِ عشوائيةِ في صورةِ الغطاءَ، هذه الطريقةِ تمتاز بالمرونةِ حيث بامكاننا إخفاء أنواعِ مختلفةِ من البياناتِ السرّيةِ في أنواعِ مختلفةِ مِنْ وسائط النقل، وتمتاز أيظا بالمتانة حيث أنَّ البياناتِ السرية تَكُونُ مخفيةَ في مواقعِ عشوائيةِ وهذا ما يميّزُ الخوارزميةَ المُقتَرَحةَ، حيث أظهرت النَتائِجَ أمنية عالية، وذلك لأن البياناتَ السرية تكون مخفية داخل الصورةِ المشفّرةِ ثمّ تُحوّلُ إلى الصورةِ المنتظمةِ الأصليةِ، ولتوضيحِ الخوارزميةِ المُقتَرَحةِ تم تطبيقها على صورة رقمية ذات التدرج الرماديِ و بأستحدام لغة ماتلاب مع إستعمال مقاييس الكفاءةِ PSNR و MSE لقياس كفاءة الطريقة المقترحة .

الكلمات المفتاحية: التشفير، الاخفاء ، المواقع العشوائية ، خوارزمية LCG ، تقنية LSB ، صورة الغطاء ، الصورة المشفرة ، PSNR .MSE

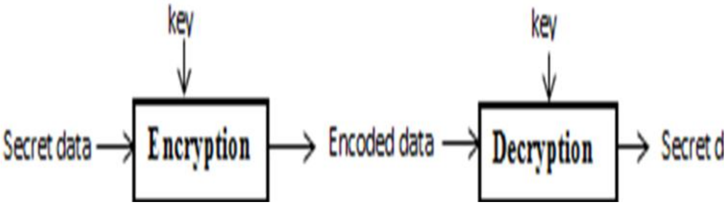
Introduction

The rapid development in the field of computer and data transfer through internal networks and global networks , require maintainng the confidential of data in the area of transfer of confidential information between the countries and banks of personal information and copyright etc . different techniques appeared to maintain the confidentiality of data ; they Can be divided into two parts . the encryption techniques and the concealment techniques ; The encryption techniques are working to change the general form of confidential data , and they are used widely in different areas , but these techniques may be detected because the encrypted information is unclear and this raises doubts among hackers and those who seek to steal the confidential information . Thus the concealment technique is adopted beside encryption technique . Concealment technique is one of the important techniques in maintaining the confidentiality of the transmitted data . The basic principle for this technique is hiding the secret information in cover of the carrier without affecting the human eye [Singh and Agarwal , 2010; Ramanpreet Kaur & Singh, 2012;Saket *et al.,* 2013)].

There can be a combining between the concealment technology and the encryption technology for increasing the confidentiality of data . That is when the secret message is revealed, it will be unclear and this will remove doubt about the existence of a hidden message and this what has been applied in this research where concealment is improved by using LSB technique and combined with the LCG algorithm to generate random locations to hide the confidential data .

1- Encryption

Its One of the methods used in maintaining the security of data which works to change the content of information for symbols that are difficult to be understood . It is divided into two algorithms , symmetric needs one secret key which is used in encryption and decryption , while asymmetric needs two secret keys , a public key is used in encryption, and a private key is used in decryption. We used the symmetric type in this search [Jianying and Yung, (2010)].



Fig(1) Block diagram to encrypt and data decrypt

2- Steganography

Its One of the methods used in maintaining the security of data . the basic principle of this technique is hiding of information in the file of the cover without raising doubts about the existence of hidden data ,There are three basic algorithms for steganography **[Gutte & Chincholkar , 2012; Shikha, 2013].**

3.1-Pure Steganography : This way the information are hidden and retrieved without a secret key .

Hiding : C*M >> CM

Retrieving : CM >> M

3.2- Steganography by using Secret Key : this way the information are hidden and retrieved need a secret key .

Hiding : C*M*K >> CM
Retrieving : K*CM >>M

3.3- Steganography by using Public Key: in this way there are two keys , a public key to hide data and private key to data extraction .

Hiding : C*M*K1 >> CM

Retrieving : K2*CM >>M

where :

C : the cover

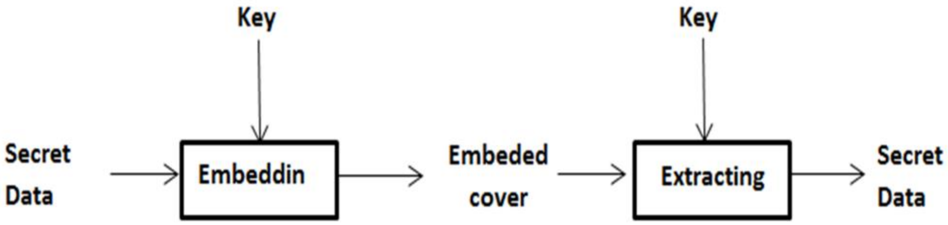
M: the secret data

CM : the Embedded cover

K : the secret key to hide and extract data

K1: the puplic key

K2: the private key



Fig(2) **Block diagram of data hiding and retrieval**

3- Linear congruential generator (LCG)

This algorithm is used to produce a series of random numbers and it can be easily used, especially with computers [Prasada , 2010] where Random numbers are generated by the following equation :

$$X_{n+1}=(aX_n + c) \bmod m$$

Where :

X is the sequence of pseudo random values .

X_0 is the seed ,where X0 >= 0 , and X0 < m .

m is modulus , where m > 0 .

a is the multiplier ,where a > 0 , and a< m .

c is increment ,where c >= 0 , and c < m .

4- The proposed method

The proposed method consists of several stages :

5.1 Encryption of confidential information

The proposed method is intended to encrypt the data, where the binary system consists of 1 and 0, so we will depend on group sequence (1) and group sequence (0). where we convert confidential data to the binary system, and then collect them in a single matrix, then divide the matrix into two matrices. Matrix (1) which contains the sequence (1) with (0) between each two sets of the (1), and matrix (0) and the sequence (0) with (1) between each two sets of the (0), where the matrix (1) is complementary to the matrix (0) and vice versa .

5-2 Encryption of cover image

It means the transformation of the image of the cover to another image but irregularly (unclear), and that depends on the LCG algorithm to generate random locations, we create the random locations matrix , make its dimensions Equal to the dimensions of the cover Matrix , and then put the original image in the matrix generated from LCG algorithm, so the result is irregular image.

5-3 hiding the secret data

Confidential data resulting from the first stage is storing in the irregular image depending on the LSB Technique .

5-4 Converting irregular image to regular image

Irregular Image containing the confidential data is converted to a regular image depending on the LCG algorithm .

Algorithm(1) encoding & hiding the secret data

Input : secret data (D_secr) , original cover image (regular image (cov_im_reg)) , values of variables of LCG algorithm , start of first location (place_1) , start of second location (place_2) .

Output : stego_reg
Step_1 : Encryption of confidential information

1- Reading the secret data (D_secr)

2- Convert (D_secr) to a binary system (D_bin)
3- Put D_bin in Matrix one-dimensional (D_bin_1)
4- separating (by using some instructions) D_bin_1 for matrix of (1) and matrix of (0)

Step_2 : Encryption of cover image

1- reading a cov_im_reg
2- finding the dimensions of the cov_im_reg (N,M)
3- generating a random numbers depending on the LCG algorithm , where the collection of random numbers is equal to N*M (arr_random_1)
4- converting arr_random into a array by two dimensions (arr_random_2) , which conform with dimensions cov_im_reg
5- put cov_im_reg in arr_ran_2 ,we will get on cov_im_irreg

Steps_3 : Hiding of secret data (Matrex of (1)) ,and (Matrex of (0)) in cover (cov_im_irreg)

1- limit two places (place_1 , place_2) from cov_im_irreg
2- hide Matrix of (1) in place_1 in Least Significant Bit from each byte
3- hide Matrix of (0) in place_2 in Least Significant Bit from each byte
4- we will get on stego_irreg

Steps_4 : converting stego_irreg into stego_reg

reversing the operation 5-2 step_5 will leads to the stego_reg

EX(1) : to explain the proposed method (encoding & hiding the secret data)

Stage _1 : encoding a secret data

suppose secret data is " Ir " , where the results are :

D : [73 114]

D_bin : [1001001 ; 1110010]

D_bin_1 : [10010011110010]

Matrex of (1) : [10101111010]

Matrex of (0) : [0010010010]

Stage_2 : encoding a cover image

suppose we have a sample from cover image 5*5 cov_im_reg

167	186	178	187	184
169	178	163	179	178
155	160	165	174	180
160	174	174	179	195
182	175	173	183	190

=

matrix of two dimensions (1) cover image before encoding (cov_im_reg)

N=5 , m=5

arr_random_1 =

[2 5 8 11 14 17 20 23 1 4 7 10
13 16 19 22 25 3 6 9 12 15 18
21 24]

matrix of one dimension (2) generated random numbers by LCG

arr_random_2 =

2	17	7	22	12
5	20	10	25	15
8	23	13	3	18
11	1	16	6	21
14	4	19	9	24

matrix of two dimensions (3) matrix of the Random locations is generated

cov_im_irreg =

169	179	178	178	163
182	183	175	190	173
160	180	165	155	174
178	167	187	186	184
174	160	179	174	195

matrix of two dimensions (4) encoded cover image (cov_im_irreg)

Stage_3 Hiding of secret data (Matrex of (1)) , and (Matrex of (0)) in cover (cov_im_irreg)

stego_irreg =

168	179	179	179	162
182	182	174	191	173
161	180	165	155	174
178	167	186	186	184
174	160	179	175	195

matrix of two dimensions (5) Include confidential data in encrypted cover (stego_irreg)

Stage_4 : stego_irreg into stego_reg

stego_reg =

167	186	178	186	184
168	179	162	179	179
155	161	165	174	180
160	175	174	179	195
182	174	173	182	191

matrix of two dimensions (6) Converting irregular cover (stego_irreg) to regularl cover

Algorithm(2) extracting the secret data from stego_image

Input : stego_reg , values of variables of LCG algorithm , start of first location (place_1) , start of second location (place_2)

Output : secret data (D_secr)

Step_1 : Encryption of stego_reg

1- reading a stego_reg
2- finding the dimensions of the cov_im_reg (N,M)
3- generating a random numbers depending on the LCG algorithm , where the collection of random numbers is equal to N*M (arr_random_1)
4- converting arr_random into a array by two dimensions (arr_random_2) , which conform with dimensions stego_reg
5- put stego_reg in arr_ran_2 ,we will get on stego_im_irreg

Step_2 : **Extraction of secret data (**Matrex of (1) **) , and (**Matrex of (0) **) from cover (**stego_im_irreg**)**

1- limit two places (place_1 , place_2) from stego_im_irreg
2- extract Matrix of (1) from place_1 in Least Significant Bit from each byte
3- extract Matrix of (0) from place_2 in Least Significant Bit from each byte

Step_3 : decryption of confidential information

1- reseparating (by using some instructions) matrix of (1) and matrix of (0) into D_bin_1
2- Puting D_bin_1 in Matrix two-dimensional (D_bin) where , N > 0 , and M=7
3- Converting (D_bin) for (D_secr)

EX(2): to explain the proposed method (extracting the secret data from stego_image)
Stage_1 : Encryption of stego_reg

1- reading a stego_reg

167	186	178	186	184
168	179	162	179	179
155	161	165	174	180
160	175	174	179	195
182	174	173	182	191

matrix of two dimensions (7)
embeded cover (stego_req)

2- finding the dimensions of the cov_im_reg (N,M)
N=5 , M=5

3- generating a random numbers depending on the LCG algorithm , where the collection of random numbers is equal to N*M (arr_random_1)

arr_random_1 =

[2 5 8 11 14 17 20 23 1 4 7
10 13 16 19 22 25 3 6 9 12 15
18 21 24]

matrix of one dimension (8) generated random numbers by LCG

4- converting arr_random into a array by two dimensions (arr_random_2) , which conform with dimensions stego_reg

arr_random_2 =

2	17	7	22	12
5	20	10	25	15
8	23	13	3	18
11	1	16	6	21
14	4	19	9	24

matrix of two dimensions (9) matrix of the Random locations is generated by LCG

5- puting stego_reg in arr_ran_2 ,we will leads to stego_im_irreg

stego_irreg =

168	179	179	179	162
182	182	174	191	173
161	180	165	155	174
178	167	186	186	184
174	160	179	175	195

matrix of two dimensions (10)
encoded cover image (cov_im_irreg)

Stage_2 : Extraction of secret data

Matrex of (1) : [10101111010]

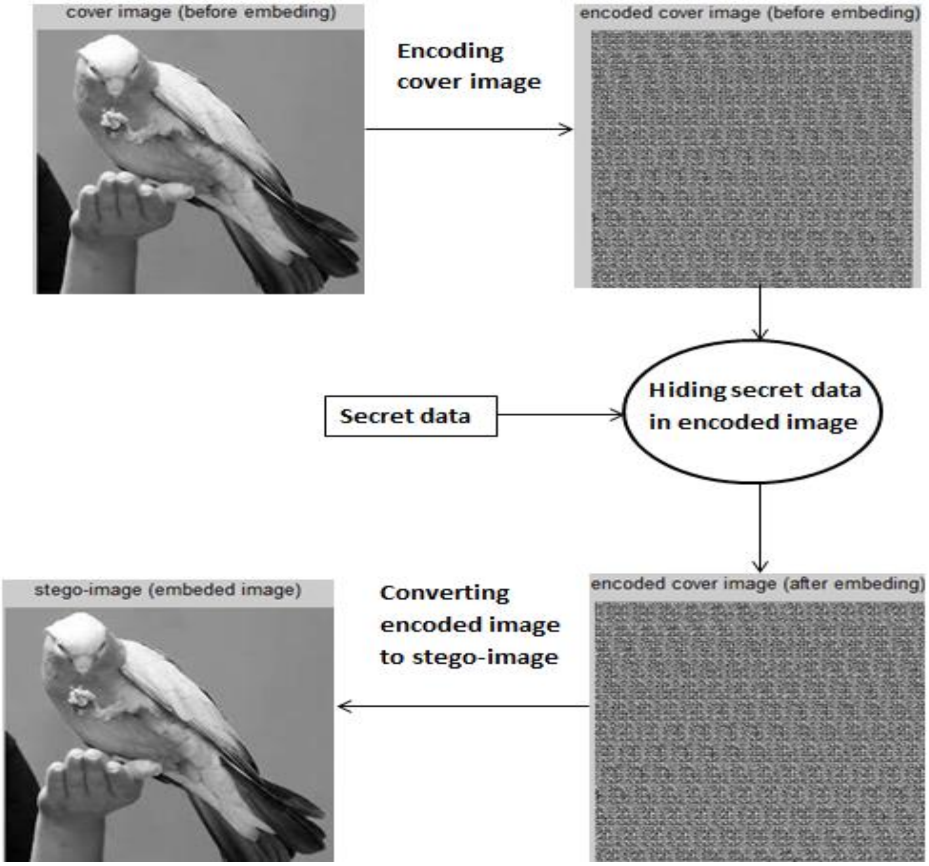
Matrex of (0) : [0010010010]

Stage_3 : decryption of confidential information

1- reseparating (by using some instructions) matrix of (1) and matrix of (0) into D_bin_1 D_bin_1 : [10010011110010]
2- Puting D_bin_1 in Matrix two-dimensional (D_bin) where , N > 0 , and M=7
D_bin : [1001001 ; 1110010]
3- Converting (D_bin) for (D_secr)
D : [73 114] >>> “ Ir“

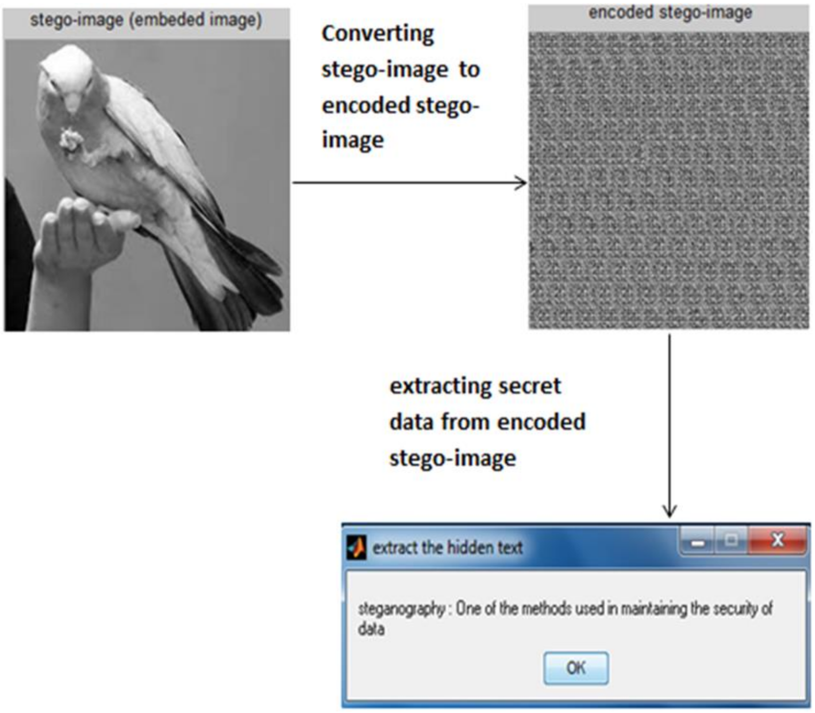
6- Practical tests:

1- encoding & hiding secret data


cover image (before embeding)
Encoding
cover image
encoded cover image (before embeding)
Secret data
Hiding secret data
in encoded image
stego-image (embeded image)
Converting
encoded image
to stego-image
encoded cover image (after embeding)

Fig(3) : block diagram to explain steps of combining between the operation of encrypting and operation of hiding

2- Extracting the secret data


stego-image (embeded image)
Converting stego-image to encoded stego-image
encoded stego-image
extracting secret data from encoded stego-image
extract the hidden text
OK

steganography : One of the methods used in maintaining the security of data

Fig(4) : block diagram to explain steps the operation of extraction the secret data

7- Results

The proposed method has been tested on a gray image with different sizes ,with the use of standards PSNR and MSE to measure the efficiency of the way

$$MSE = \frac{1}{RM * CM} \sum_{i=1}^{RM} \sum_{j=1}^{CM} (cij - scij)$$

$$PSNR = 10 \log_{10} \frac{L^2}{MSE}$$

Where :
RM: The number of rows
CM: The number of columns
cij: image unit before Concealment
scij: image unit after Concealment
L: peak of signal

Table(1) : display the values of for PSNR and MSE

Image name	Image size	LSB location of pixel	Text length by bits	PSNR	MSE
Im_1	200*200	6	629	57.4755	0.1172
Ima1	200*200	7	629	62.9404	0.0333
Ima3	200*200	8	526	69.8079	0.0069
Ima4	250*250	6	629	58.8841	0.0847
Ima5	250*250	7	629	65.0924	0.0203
Ima6	250*250	8	629	71.0993	0.0051
Ima7	300*300	6	1269	57.7072	0.1111
Ima 8	300*300	7	1269	63.5978	0.0286
Ima 9	300*300	8	629	72.4958	0.0037
Ima 10	300*300	6	1909	55.8751	0.1694
Ima 11	300*300	7	1909	61.8234	0.0431
Ima 12	300*300	8	1278	69.4465	0.0074
Ima 13	400*400	6	1909	58.3376	0.0961
Img 14	400*400	7	1269	65.9376	0.0167
Img15	400*400	8	1278	71.9974	0.0041

8- Debate of Results :

After studying the shapes and the results above , it is revealed that :

1- size of image : Directly proportional with PSNR and inversely with MSE
2- LSB : Directly proportional with MSE and inversely with PSNR
3- size of information : Directly proportional with MSE and Inversely with PSNR.

9- Conclusions

1- What distinguishes the proposed algorithm. it is impossible to determine the sites of concealment even by the authorized person , because we hide our data in the encrypted cover.
2- It’s Possible to hide a lot of data without affecting the cover .
3- There is no loss or errors in the recovered data .
4- Use of an LCG algorithm gives high security in the cover-ups in terms of the large number of the possibilities , especially with changing the values (c , r , f() , and the size of image) .
5- It’s characterized by durability in terms of concealing information in different locations .
6- Values os PSNR and MSE, are good even with a large volume of information.

10- Recommendations

1- The method that is used in the encryption of the data can be combined with other encryption methods .

2- The method that is used in the cover encryption can be combined with other encryption methods .

3- The method used in the encryption can be applied to different data types .

4- Other techniques can be used in the process of concealment .

11- References

Singh , S. and Agarwal , G. , (2010) , “Use of Image to Secure Text Message With the Help of LSB Replacement”, International Journal of Applied Engineering Research, Dindigul Vol. 1, No.1.

Jianying Zhou and Moti Yung, (2010) "Applied Cryptography and Network Security", th International Conference, ACNS 2010, Beijing, China, June 22-25, .

Gutte, R.S., Chincholkar Y.D., (2012), "Comparison of Steganography at One LSB and Two LSB Positions", International Journal of Computer Applications, Vol. 49, No.11.

Saket B. Parmar, Piyush P. Pokharna, Abhay B. Patil , (2013) " A Conceptual Study of Various Data Hiding Techniques – A Review" Electronics Department Bharati Vidyapeeth Deemed University Deemed University, India, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 2, February 2013.

Shikha, Kuchhal. Ishank , (2013), “Data Security Using RSA Algorithm in Matlab”, International Journal of Innovative research and development, 2:7, 2013.

Prasada Rao Gurubilli , June 2010 "Random Number Generation and Its better Technique ",computer science and engineering Department,ThaparUniversity,Patiala – 147004.

Ramanpreet Kaur & Prof.Baljit Singh,(2012) " Survey and analysis of various Stganographic Techniques ", [IJESAT] International Journal Of Engineering Science & Advanced Technology Vol-2, Issue-3, 561– 566, May-Jun 2012 .