مجلة

كلية التـــراث الجامعة

مجلة علمية محكمة

متعددة التخصصات نصف سنوية

العدد التاسع والثلاثون

عدد خاص بوقائع المؤتمر العلمي السنوي السادس عشر (الدولي الخامس)

18 نيسان 2024

ISSN 2074-5621

رقم الايداع في دار الكتب والوثائق 719 لسنة 2011

مجلة كلية التراث الجامعة معترف بها من قبل وزارة التعليم العالي والبحث العلمي بكتابها المرقم (ب 3059/4) والمؤرخ في (2014/ 4/7)

Image Verification Using Hidden Compressed Encrypted Data and Rabin System

Ass. Prof. Dr. Saad A. Adbdual Rahman*
Ass. Prof. Dr. Sanaa Ahmed Kadhim**
*Al Mamoon University Collage
**University of information technology and communications

Abstract
Many recent applications demand image transmission through the net in the same time trying to keep the integrity and authenticity of these images till they reach destination. In this paper, image verification is applied using lossless compression technique "Huffman" and steganography methods and cryptographic technique "Rabin" are used to boost security. The verification process includes encrypting specific text, compressing it then hiding the result in selected places within the image. The system was tested based on PSNR with respect to the size of images, and compression ratio.

Keywords: LSB, Improved diagonal queue, Steganography, Cryptography, Huffman compression, Rabin technique.

1- Introduction

On the Internet, the amount of digital photos has rapidly expanded. For many applications, including military, medical, video surveillance, and sensitive transmission, image security is becoming more and more crucial [1]. In steganography, the secret message is hidden within an image (or other type of media) that is referred to as a cover image. The cover image is then given to the recipient, who separates the secret message from it. To prevent the attacker from figuring out whether there is an embedded message, the data shouldn't be recognizable from the cover image. Steganography and encryption are two methods that may be used to secure the transmission of concealed data. Data security can be improved by combining the two methods [2]. When a communication is encrypted, it is altered in a way that prevents any data from being revealed even if it is intercepted by an adversary [3]. There are several methods for encrypting data [4], and each one varies in terms of security, reliability, performance, and other factors [5]. Encrypted data will be hiding beneath the image; the most common hiding method is utilizing LSB of many pixels to insert a message into a colored image [6]. In this paper a new method for securing hidden data in digital images using the combination benefits of encryption using Rabin method for key exchange, compression using Huffman and hiding using LSB with specific method for selecting hiding bits. The new method showed significant results in reducing the size of data and distributing bits within the image.

The rest of the paper will be divided as follows: section two for previous work, section three for background methodology, section four for the suggested method, then the results and analysis, and finally the conclusions.

2- Related Work

For decades, researchers try to reach the optimality in stego-methods for digital images. [7] suggested to hide data within digital images using diamond encoding method in which the secrete message could be extracted without the use of the original image. The method gave high payload with minimum distortion. [8] suggested the used of JPEG images us a carrier for hidden data after the analyzation using EMD method and the AC cofactors with DCT transformer. The suggested method gave high payload with minimum distortion. [9] suggested a method for steganography for medical images using Rabin and queues to distribute the encrypted data in different blocks within the medical image. The method showed high payload with minimum distortion. [10] suggested a method for expanding the secrecy of Rabin by producing fake modulus to be added to the exact modulus. The suggested method increases the complexity of extracting the original primes of Rabin and preventing factorization applied by hackers. [11] suggested a method that combines both Rabin with OTP to expand the secrecy of the encryption of images.

3- Background Methodology

3-1 Rabin's scheme

Rabin had invented a mathematical method for public key system in which the modular number is created from two primes that are congruent to modular 4 [9]. The schema will be:

1- Chose A,B such that:

$$A \neq B \text{ , and, } A \equiv B \equiv 3 \bmod 4$$

2- Calculate K= A * B, consider K as the public key.

For encryption, the following equation is used:

$$C = P^2 \bmod K, \qquad (P \text{ is the message})$$

For decryption:

$$P = \sqrt{C} \bmod K$$

Since K is large, finding the root of C is complicated unless knowing the factors of K (A,B) which are known only for the authorized person. Using that the decryption process will be:

$$(P_A)^2 \equiv C \bmod A$$

$$(P_B)^2 \equiv C \bmod B$$

Then:

$$P_A = C^{(A+1)/4} \bmod A \quad \text{and} \quad P_B = C^{(B+1)/4} \bmod B$$

The result of finding the roots of the previous equations will be four different numbers, using the Chinese remainder theorem and farther calculations the correct number of plain text will be chosen.

3-2 Huffman Method

Transmitting data through wide communication media will demand compression to fasten the transmission and to minimize files sizes. Huffman was invented to compress text with simple and unique code[12]. Huffman code was proved to obtain the shortest compressed code with variant length encoding depending on the texts to be compressed[13]. The size will be smaller than the original one specially for long files. It is applied by creating a specific tree named the encoding tree or the Huffman tree in which each character will has a code of one bit, two bits, three bits or more depending on the frequently appearing of the letter within the text.

3-3 Square Matrix Permutation

Hiding data within media like image or sound will infer the use of square matrices in which certain blocks of the cover media will be written as a square matrix to be used (depending on the hiding method) in embedding the secrete data bits. Parts of the covered image will be converted to square matrices (8*8) of 8 pixels. Only one part of the RGB pixel will be used for creating the matrix(8 pixels with 8 bits only from each pixel). Table 1 below shows the suggested square matrix with 8.

Table 1: the suggested square matrix (8*8)

A1	A2	A3	A4	A5	A6	A7	A8
B1	B2	B3	B4	B5	B6	B7	B8
C1	C2	C3	C4	C5	C6	C7	C8
D1	D2	D3	D4	D5	D6	D7	D8
E1	E2	E3	E4	E5	E6	E7	E8
F1	F2	F3	F4	F5	F6	F7	F8
G1	G2	G3	G4	G5	G6	G7	G8
H1	H2	H3	H4	H5	H6	H7	H8

The square matrix then will be permuted using a permutation table shown in table 2, each number represent the position of bit from the square matrix.

Table2: permutation table

33	8	48	9	49	24	64	25
34	7	47	10	50	23	63	26
35	6	46	11	51	22	62	27
36	5	45	12	52	21	61	28
37	4	44	13	53	20	60	29
38	3	43	14	54	19	59	30
39	2	42	15	55	18	58	31
40	1	41	16	56	17	57	32

After permutation, the bits will be as table 3 below:

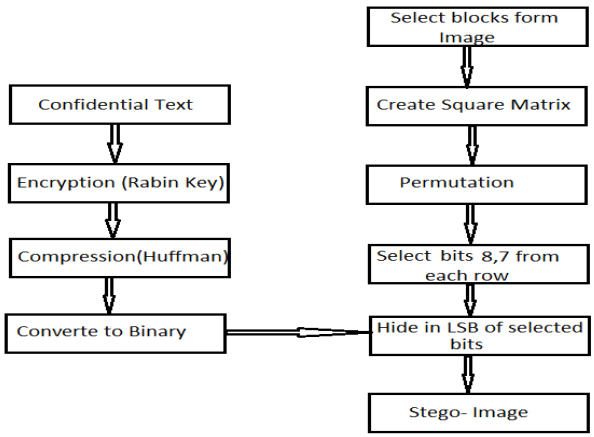
Table 3: permuted matrix

E1	A8	F8	B1	G1	C8	H8	D1
E2	A7	F7	B2	G2	C7	H7	D2
E3	A6	F6	B3	G3	C6	H6	D3
E4	A5	F5	B4	G4	C5	H5	D4
E5	A4	F4	B5	G5	C4	H4	D5
E6	A3	F3	B6	G6	C3	H3	D6
E7	A2	F2	B7	G7	C2	H2	D7
E8	A1	F1	B8	G8	C1	H1	D8

From each row of the permuted matrix, the bits of the two higher positions (7,8) in each row will be used for embedding with the same sequence they appeared in the permuted matrix.
Selected bits=(A8,F8,C8,H8,A7,F7,C7,H7,E7,B7,G7,D7,E8,B8,G8,D8)

4- The proposed method

The suggested method has many steps starting with encrypting data to be hidden using the keys obtained from Rabin. The letters will be considered as sequence (position) within the English letters before executed in Rabins encryption. The numbers will be compressed using Huffman algorithm, then hidden in the cover image using the square matrix. The following block diagram explains the proposed method steps:



Block diagram 1: Steps of the proposed method

As shown in block diagram 1, the proposed method has two parts: the first part is related to the confidential text which will be encrypted using Rabin's key, then compressed using Huffman coding tree, and final use the binary bits resulted from compression to be hidden. The second part is related with the cover image. Certain blocks of the cover image will be chosen where each block consists of 64 pixels (8*8). The square matrix will be permuted then only pixels of position 7 and 8 will be used in hiding data bits within one of the parts RGB. The hiding process will use the LSB of chosen pixels. The result will be the stego_image.

5- Implementation

Suppose the text to be hidden is "layla sabah mohmed", then the letters, their weights and their encryption is shown table 4 below:

Table 4: weight and code of text letters

Plain text	Weight	Cipher **code**
A	1	1
L	12	4
H	8	64
M	13	169
Y	25	625
S	19	361
B	2	4
O	15	225
E	5	25
D	4	16

Huffman tree will be created depending on the frequency of each character. The coding tree is shown in figure 1 below:

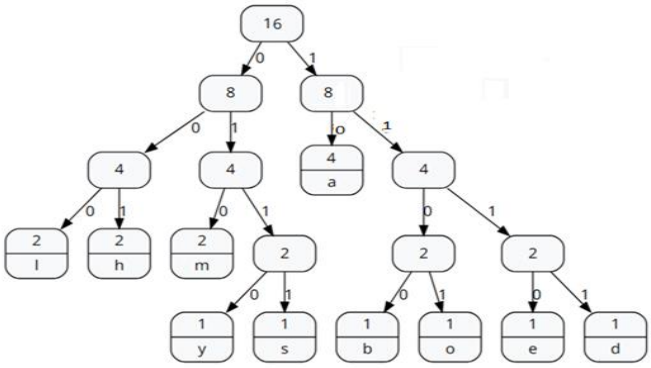


Figure 1: Huffman tree for plain text

The frequency of each character, its code and the number of bits needed before and after compression is shown in table 5 below:

Table 5: frequency and code

Character	Frequency	Code	Original size	Compressed size	No. of bits saved for each character
A	4	01	4*8=32	4*2=8	32-8 =24 bits
L	2	000	2*8=16	2*3=6	16-6 =10 bits
H	2	100	2*8=16	2*3=6	16-6 =10 bits
M	2	010	2*8=16	2*3=6	16-6 =10 bits
Y	1	0110	1*8=8	1*4=4	8 -4 =4 bits
S	1	1110	1*8=8	1*4=4	8 -4 =4 bits
B	1	0011	1*8=8	1*4=4	8 -4 =4 bits
O	1	1011	1*8=8	1*4=4	8 -4 =4 bits
E	1	0111	1*8=8	1*4=4	8 -4 =4 bits
D	1	1111	1*8=8	1*4=4	8 -4 =4 bits
Total	16 char.		128 bit	50	78 bit

The number of bits for the text will be 50 instead of 128 which mean 78 bits less. By this, the average code length for the text is 50/16=3.125.

The same method of encoding will be applied to the values resulted from Rabin method for the same letters. By this step, the text to be hidden is now encrypted and compressed. The bits obtained will be hidden in selected bits of any image after applying table 1,2,3 respectively to get the selected bits (Selected bits = (A8, F8, C8, H8, A7, F7, C7, H7, E7, B7, G7, D7, E8, B8, G8, D8)).

6- Results And Analysis

One of the most important applications in multimedia transmission is hiding data in a digital image to keep it secure and unreadable. Attackers usually try to extract the hidden data using various methods, so, to increase security and increase the chances for hackers to predict hidden data, more than one method are involved. The suggested method produces a security technique

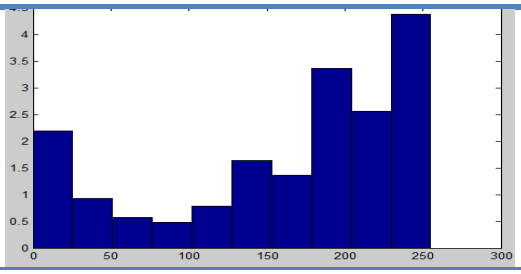
in which the data is encrypted the compressed before hiding. This will make the prediction of data very complicated process.
The suggested method showed a high payload with minimum distortion since the data is smaller than the original and the hiding procedure use two bits of each pixel instead of LSB only. There are no sequencing in the order of bits since the procedure use a permutation matrix and then row selection; this gave a sort of randomness in the sequencing. The suggested method cause no distortion to the cover image since it used only one part of the colors of the pixel (R, G, or B) therefore the effect of hiding will be unremarkable. Table 6 below shows the PSNR for hiding various lengths of data in the same image.

Table 6: PSNR for three images

Image size	Data size (bits)	PSNR	PSNR(average)
275*183	200	80.9436	78.51888
	280	79.3891	
	360	77.9053	
	576	75.8375	
193*615	200	79.0979	76.79198
	280	77.5079	
	360	76.2506	
	576	74.3115	
234*780	200	80.6579	78.54475
	280	79.2517	
	360	78.1194	
	576	76.15	

It is clear from table 6, even that the value of PSNR is decreased with the increasing of the hidden bits number (which is logically), the value of PSNR still high which indicates the minimum distortion of the stego_image.

Table 7 below shoes the histogram and PSNR for images with 576 bits hidden.

Image	**Image size**	**PSNR**	**Image histogram**
	275*183	78.51888	

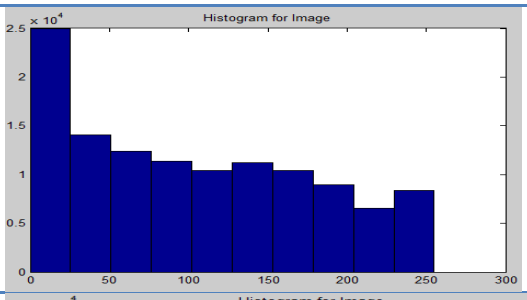
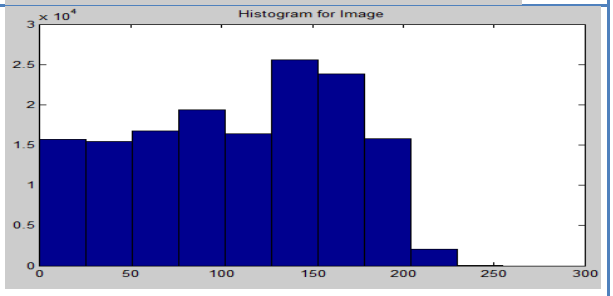
	193*615	76.79198	
	234*780	78.54475	

Table 8 below shows the comparison of PSNR for the proposed method with other researches.

Table 8: PSNR comparison

Research_article	PSNR
Ref[23]	65.53
Ref[14]	50.50
Ref[16]	44.20
Ref[17]	44.15
Ref[15]	37.90
Ref[19]	36.00
Ref[20]	33.53
Ref[21]	30.48
Ref[9]	70.37
Proposed method	78.54

The proposed method showed the best value for PSNR with respect other works of hiding data within color images.

7- Conclusion

Steganography is one of the most important fields in data transmission. To avoid hacking, manipulation and faking images through lines, steganography is used in which specific data are hidden securely in a cover image without making any distortion and keeping the attacker unaware about that hidden data. The proposed method employed the methods of Huffman and Rabin to minimize the size of data to be hidden. The positions in which data bits will be hidden are selected using permutation tables such that the bits are neither sequential nor pure random but in between with an acceptable randomness. The proposed method showed a best PSNR compared to other previous methods.

References

[1] Verdiyev S.G., Naghiyeva A.F., "A Brief overwiew of data hiding methods in digital images",Infokommunikacionnya technologii, vol.18, no. 4, 2020.
[2] Hao-Tian Wu,· Ruoyan Jia, Jean-Luc Dugelay, Junhui He, "Reversible image visual transformation for privacy and content protection", Multimedia Tools and Applications https://doi.org/10.1007/s11042-020-09985-1.
[3] F. Petitcolas, R. Anderson and M. Kuhn, "Information Hiding-A Survey", Proceedings of the IEEE, Special Issue on Protection of Multimedia Content, Vol. 87, Issue 7, July 1999, pp. 1062-1078.
[4] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.
[5] Dalia Nashat, Loay Mamdouh," An efficient steganographic technique for hiding data", Nashat and Mamdouh Journal of the Egyptian Mathematical Society (2019) 27:57 https://doi.org/10.1186/s42787-019-0061-6.
[6] Sabah A. Jebur, Abbas K. Nawar, Lubna E. Kadhim, Mothefer M. Jahefer, "Hiding Information in Digital Images Using LSB Steganography Technique", iJIM – Vol. 17, No. 07, 2023.
[7] Ruey-Ming Chao, Hsien-Chu Wu, Chih-Chiang Lee,Yen-Ping Chu," A Novel Image Data Hiding Scheme with Diamond Encoding", Hindawi Publishing Corporation EURASIP Journal on Information Security Volume 2009, Article ID 658047, 9 pages doi:10.1155/2009/658047.
[8] Xiao-Zhu Xie, Chin-Chen Chang and Ji-Hwei Horng," An EMD-based data hiding scheme for JPEG images", CONNECTION SCIENCE 2021, VOL. 33, NO. 3, 515–531 https://doi.org/10.1080/09540091.2020.1853055.
[9] Mamta Jain . Saroj Kumar Lenka, "Diagonal queue medical image steganography with Rabin cryptosystem", Brain Informatics (2016) 3:39–51.
[10] Raghunandan K. R. , Radhakrishna D., Surendra S., Ganesh A., Monalisa S. and Aditya K. S., "A Novel and Secure Fake-Modulus Based Rabin-3 Cryptosystem", Cryptography 2023, 7, 44. https://doi.org/10.3390/cryptography7030044.
[11] M A Budiman, M Zarlis, and Hafrizah, "Implementation of hybrid cryptosystem using Rabin-p algorithm and One Time Pad to secure images", Journal of Physics: Conference Series 1898 (2021) 012037, IOP Publishing doi:10.1088/1742-6596/1898/1/012037.
[12] Usama, M., Malluhi, Q.M., Zakaria, N. et al. An efficient secure data compression technique based on chaos and adaptive Huffman coding. Peer-to-Peer Netw. Appl. 14, 2651–2664 (2021). https://doi.org/10.1007/s12083-020-00981-8.
[13] Liu Y, Li B, Zhang Y, Zhao X. A Huffman-Based Joint Compression and Encryption Scheme for Secure Data Storage Using Physical Unclonable Functions. Electronics. 2021; 10(11):1267. https://doi.org/10.3390/electronics10111267.
[14] Gandharba S, Lenka SK (2012) LSB array based image steganography technique by exploring the four least significant bits. In: Proceedings of 4th international conference, Obcom 2011, CCIS, vol 2(270), pp 479–488 (ISBN: 978-3-642-29216-3). doi:10.1007/978-3-642-29216-3_52.pdf)
[15] Wu DC, Tsai WH (2003) A steganographic method for images by pixel value differencing. Pattern Recogn Lett 24(9-10):1613–1626
[16] Wang R, Chen Y (2006) High payload image steganography using two-way block matching. IEEE Signal Process Lett 13(3):161–164

[17] Kumar PM, Roopa D (2007) An image steganography framework with improved tamper proofing. Asian J Inf Technol 6(10): 1023–1029. http://medwelljournals.com/abstract/?doi=ajit.2007. 1023.1029
[18] Parvez MT, Gutub AA (2008) RGB based variable-bits image steganography. In: Proceedings of IEEE Asia Pacific services computing conference, pp 1322–1327 (ISBN: 978-0-7695-3473-2). www.ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4780862)
[19] Zhang X, Wang S (2004) Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recogn Lett 25(12):331–339
[20] Chang CC, Tseng HW (2004) A steganographic method for digital images using side match. Pattern Recogn Lett 25(12): 1431–1437
[21] Nag A, Singh JP, Khan S, Ghosh S (2001) A weighted location based lsb image steganography technique. Springer ACC 2011, 50 M. Jain, S. K. Lenka 123 CCIS 2(191):620–627 (ISBN: 978-3-642-22714-1). http://link. springer.com/content/pdf/10.1007/978-3-642-22714-1_64.pdf
[22] Maiti C, Baksi D, Zamider I, Gorai P, Kisku DR (2011) Data hiding in images using some efficient steganography techniques. Springer SIP 2011, CCIS 2(260):195–203 (ISBN: 978-3-642- 27183-0). http://link.springer.com/chapter/10.1007%2F978-3- 642-27183-0_21
[23] Thiyagarajan, P., and Aghila, G., ‘‘Reversible dynamic secure steganography for medical image using graph coloring,’’ Health Policy and Technology, vol. 2, no. 3, pp. 151–161, 2013. (http://www.sciencedirect.com/science/article/pii/ S2211883713000403)