

Using LSB Method For Hiding Hill Encrypted Grayscale And RGB Images In RGB Image

¹Huda adel ali , ²Enas wahab Abood , ³Wafaa A. Khudhair

¹Collage of computer science and information technology ,/university of Basrah

²Collage of Science , university of Basrah

³Collage of Science , university of Basrah

Abstract

Availability of data anywhere and ease of access and interception the information in different forms as text ,images ,video...etc., create an important issue represented by data security both steganography and encryption was appeared to achieve this mission . In this paper a hybrid technique was used to secure messages of grayscale and colored images in RGB cover image by encrypting the message with Hill encrypting algorithm and hiding it by LSB method in RGB image with random locations generated by seed number and taking three LSB bits , many different sizes of images was experimented and results was analyzed by PSNR , Correlation and histogram analysis methods , all proves the efficiency of proposed technique in securing images .

1. Introduction

Steganography is used to hide message of data in other cover data using key ,so the cover data seemed irrelevant , the message and cover could be any type of data such as text, image ,audio and video[1].only the sender and receiver who has the key is able to extract the message out of cover file. Steganography sometimes is applied for securing messages and for avoiding unwanted attention or uses in places where the usage of encryption is illegal[2] .Various methods have been proposed for image steganography depending on the image data domain . The image domain is classified into two categories: - (a) Spatial Domain, and (b) Transform Domain. For spatial domain , the most widespread method and the simplest one is the LSB(Least_Significant_Bit), which substitutes the least significant bit of cover image pixels that selected to hide the message bits [3]. Transform or frequency domain techniques are depended on the manipulation of the orthogonal transform of the image rather than the image itself [4] including transforms like discrete cosine transform DCT, discrete Fourier transform DFT , Hartley Transform, etc.

The encryption from other hand is a way of transforming the overall view of understood data to disfigured one, so the encrypted messages seemed to be obvious holding important data needed to be figured out and it fails if the intruder able to decrypt the cipher message, At other hand Steganography fails to secure data when the attacker detects the presence of a secret data inside another cover file [5]. Thus, for more ensuring data security, steganography and Encryption is used together so any observer finds difficulty in realizing the presence of messages and if its retrieved it stills understood and meaningless. In this paper, A hybrid approach of cryptography and steganography is proposed to strengthen security insurance for grayscale and colored images. The cryptography was implemented by using Hill cipher algorithm which is a polygraphic cipher algorithm based on linear transformation while a LSB was employed for steganography with a modification as a random spreading of bits and more than one least bit.

2. Related Work:

The data security system witnesses a continuous increasing in threats lately which makes the data security issue is a matter of concerning for the researchers and security experts. Many techniques of

steganography and Cryptography are presented to defeat these threats. Many researchers nowadays blended both of these techniques for acquiring a higher level of security [5]. Ankit Dhamija et al. [5] proposed a strategy for cloud architecture called (Secure Cloud Migration Architecture using Cryptography and Steganography) SCMACS to secure information transmission from the organization of client to servers of the provider of Cloud Service (CSP) by combining the approach of steganography and cryptography to provide two levels of security for transmitted data, the data transformed to code with encryption algorithm then converted into image by using steganography.

Al-Mashadi H. M. and Khalaf A. A. [6] presented three efficient hybrid homomorphic encryption techniques to encrypt images for exchanging images in public cloud safely. The suggested methods are restricted to El-Gamal and EHC (Enhanced Homomorphic Cryptosystem). The proposed system proves to be immunity and effective in security and time compared with El-Gamal and EHC schemes. Abduljaleel I. Q. [7] proposed a system combined of two techniques for securing color images by encrypting the secret image using Integer Wavelet Transform (IWT) and scrambled it with Arnold transform then XORed it with key of chaotic map. For more security the secret encrypted image has been hidden in a color image as a cover by using (LSB) method. Sevierda R. et al. [2] describes the effectiveness of Steganography for secret messages of grayscale images hidden in a cover RGB images, the secret image is encrypted by using Rubik's cube principle based method that moves the pixels position of digital image. To obtain more security level, LSB method used for hiding encrypted image. Efficiency of the suggested scheme is verified using analysis schemes like histogram analysis, Brute-Force attack, Avalanche effect, visual attack and analysis of Chi-Square statistical attack.

Astuti Y. P. et al. [8] Proposed a safe and simple method for hiding messages using LSB techniques with a modification to avoid the predictability of LSB. XOR operation is implemented three times to encrypt the message then embedded on the LSB. To simplify the encryption and decryption processes of message, the keys in XOR operations are used by three MSB bits. It provides security for messages with a simple operation, the softness quality of the stego image scores a PSNR value above 50 dB. Gotfried C. Prasetyadi et al. [1] they produced steganography method called append insertion which hides any type of computer file in a carrier or cover certain type computer file for removing the restrictions on message file type. AES_256 algorithm is used for encryption with passphrase. For identification and verification of original message a block of bytes is specialized. This system was tested using five secret files of different types as messages. A SHS_256 is used to calculate files integrity before being hidden and after retrieving that produce exact hash values. Bairagi [9] produced a security system using even-odd encryption method depends on ASCII code and converting the encrypted message with Gray code then embedding the message in a picture to burden cryptanalyst's job. Qiang Zhang et al. [10] proposed algorithm based on DNA sequence addition combining with chaos method for image encryption. The secret image is encoded by DNA sequence matrix, then this matrix segmented and added together, A complement operation is accomplished using two Logistic maps to the DNA sequence and DNA sequence matrix that produced is decoded to obtain the encrypted image.

3. Proposed System

A hybrid technique in this paper is contained two phases:

1. Encryption phase: the system accepts a secret message of grayscale or RGB image to be encrypted using Hill Algorithm that based on a linear transformation with Key of $n \times n$ integer numbers matrix, the key is a non-singular matrix which n is the size of the block that the message is divided to. Hill Cipher algorithm can resist the frequency analysis, high speed and high throughput [11].

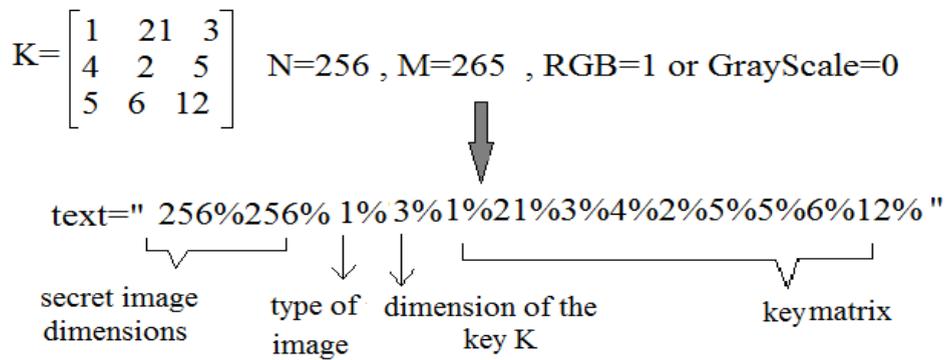
The message or data of image called I is encrypted as:

$$C_I = KI \pmod{256}$$

Where 256 is the largest value of image pixel, C_I is the cipher image block.

The decryption of cipher image C_I to produce secret image I is obtained by using inverse matrix of the encryption key K ,

$$I = K^{-1} C_I \pmod{256}$$



Fig(3) transformation the key K and image information into text to be hidden in cover file

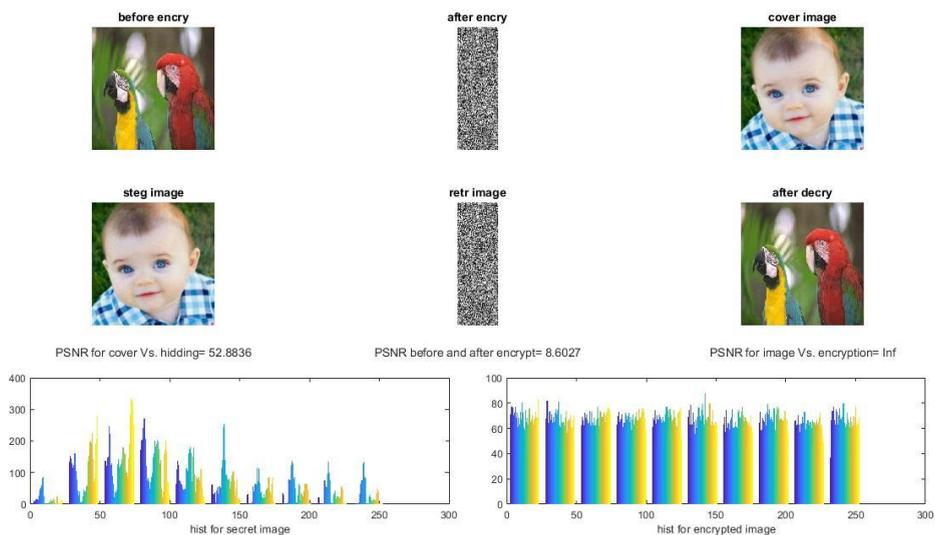
In the receiver side the key K_H is used for generation the random location of the encryption key K and secret image information then the summation of the key K used to unhide the secret pixels as a matrix.

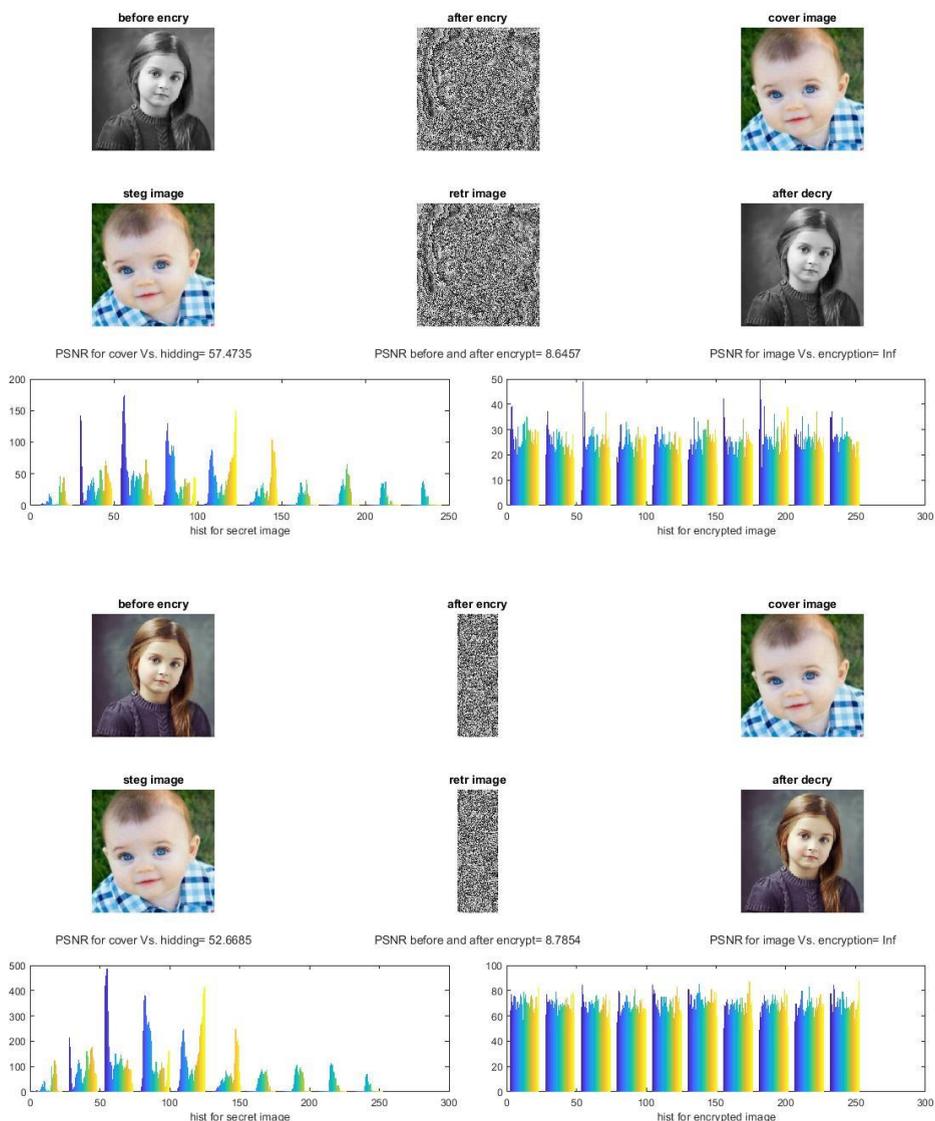
4. Experimental Results Analysis:

Many different size and types of (gray or RGB) secret images was encrypted and hidden in various RGB images with proposed system and three types of security analysis methods was used for testing system effectiveness

1. Histogram analysis:

Histogram is used for showing the frequency allocation of pixel weights in an image, in this paper histogram was used for ciphered image to show its uniformed that make it resistible for statistical attack, fig(4).





Fig(4) the histogram for secret plain image Vs. encrypted image

2. PSNR Analysis:

PSNR is most common analysis based on mean squared error (MSE) between two images such as plant and ciphered or cover images before and after hiding to show the noise approximation scale .MSE and PSNR(in dB) is calculated as :

$$MSE = \frac{1}{MN} \sum_{k=1}^M \sum_{h=1}^N (I(k, h) - \hat{I}(k, h))^2$$

$$PSNR = 10 * \log_{10} \frac{255}{\sqrt{MSE}}$$

Thus, I is a noise-free MN monochrome image and its noisy approximation \hat{I}

The value of PSNR higher than 50 dB for 8 bits image is better, For 16-bit data most acceptable values for the PSNR are between 60 and 80 dB .when the noise is absence , the two images I and \hat{I} are matching, that leads MSE to be zero. In this case the PSNR value is undefined or infinite [12].

In this paper the PSNR was calculated for plain and encrypted images that was very low which means they differ a lot. The PSNR for secret image and reconstructed image was infinity leads to that the MSE is 0 and they are identical. Table(1).

Table(1) PSNR results between the original image and reconstructed image(grayscale and RGB)

Image	PSNR for plain grayscale image		PSNR for plain RGB image	
	With encrypted image	With reconstructed image	With encrypted image	With reconstructed image
	8.235	Inf	8.6027	Inf
	9.308	Inf	9.55	Inf
	8.6475	Inf	8.7548	Inf
	8.4256	Inf	8.8792	Inf

3. Correlation Analysis

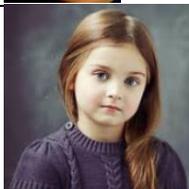
Correlation analysis is widely used to measure the similarity between two images[13][14].,Here we use it between original and the cipher image. The correlation is defined as follow :

$$c = \frac{\sum_{h=1}^N \sum_{k=1}^M (I_1(h, k) - \bar{I}_1)(I_2(h, k) - \bar{I}_2)}{\sqrt{\sum_{h=1}^N \sum_{k=1}^M (I_1(h, k) - \bar{I}_1)^2 * \sum_{h=1}^N \sum_{k=1}^M (I_2(h, k) - \bar{I}_2)^2}}$$

Here $I_1(h,k)$ is pixel intensity of gray-scale original image, $I_2(h,k)$ is the gray-scale value of the cipher image, \bar{I}_1 and \bar{I}_2 are the mean values of the images I_1 and I_2 respectively.

For RGB Image we calculate the correlation between each color component then take their mean. The value of correlation ranged in [0,1], for identical images should be high close to 1 , whereas it decreases close to 0 as much as they differ, table(2) shows the results of correlation analysis between encrypted and plain images.

Table(1) correlation coefficients between the original image and reconstructed image(grayscale and RGB)

Image	Correlation for plain grayscale image		Correlation for plain RGB image	
	With encrypted image	With reconstructed image	With encrypted image	With reconstructed image
	0.0137	1	0.0219	1
	0.0127	1	0.0025	1
	0.0071	1	0.0082	1
	0.0198	1	-0.0194	1

Conclusions

The security of transferred data became an important issue because the ease of data access via transmitted channels, The security experts and researchers tend to use and develop many security aspects like cryptography and steganography. The algorithm proposed in this paper was combined of two methods encryption with Hill method and hiding by LSB technique for securing grayscale and RGB images in a cover file of RGB image. The analytical methods proved the efficiency of the system via testing many types and sizes of secret and cover image with condition the cover is always bigger than the secret. The time consumption for overall process (encryption and hiding for grayscale) was low, it ranged from (0.0011) to (0.0021)seconds for encryption and from (0.017) to (0.169) hiding, while for (encryption and hiding for color image) was ranged from (0.0141) to (0.02) for encryption and from (0.16) to (0.2) hiding .Also the statistical results was very acceptable that for PSNR less than (10) dB that show the effectiveness for encryption technique and was (Infinity) dB for retrieved secret image which means it identical with no information loss.

The correlation analysis scores a degrees close to 0 for encrypted image Vs. original image means they not related to each other and immune against attacker analysis. At the other hand, the histogram analysis for ciphered images reflects its homogeneity that makes it opponent. From all analytical statistics results the systemproves to be an effective tool for securing images against attackers.

References:

1. Gotfried C. Prasetyadi ; Achmad Benny Mutiara ; Rina Refianti (2018) ,File encryption and hiding application based on advanced encryption standard (AES) and append insertion ,steganography method . 2017 Second International Conference on Informatics and Computing (ICIC), Jayapura, Indonesia.

2. Sevierda Raniprima ; Bambang Hidayat ; Nur Andini (2017).Digital image steganography with encryption based on rubik's cube principle. 2016 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC). Bandung, Indonesia.
3. Praneeta D., & Padma B.(2014) , Hiding Image in Image by using FMM with LSB Substitution in Image Steganography , International Journal of Advance Research in Computer Science and Management Studies, Vol. 2, Issue 11.
4. Snehal O.Mundhada, V. K.Shandilya (2012).Spatial and Transformation Domain Techniques for Image Enhancement. International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 1, Issue 2, ISSN: 2319-5967.
5. Ankit Dhamija; Vijay Dhaka (2016).A Novel Cryptographic and Steganographic Approach for Secure Cloud Data Migration. 2015 International Conference on Green Computing and Internet of Things (ICGCIoT). 978-1-4673-7910-6/15/\$31.00 ,2015 IEEE.
6. Haider M. Al-Mashadi, Ala'a A. Khalaf .(2018) .Hybrid Homomorphic Cryptosystem For Secure Transfer Of Color Image On Public Cloud . Journal of Theoretical and Applied Information Technology. Vol.96. No 19. ISSN: 1992-8645.
7. Iman Qays Abduljaleel.(2016).Using IWT and LSB Method to Hide Encrypted image in Color image . Journal of Basrah Researches ((Sciences)) Vol. (42). No. (1) A.
8. Yani Parti Astuti ; De Rosal Ignatius Moses Setiadi ; Eko Hari Rachmawanto ; Christy Atika Sari (2018). Simple and secure image steganography using LSB and triple XOR operation on MSB. 2018 International Conference on Information and Communications Technology (ICOIACT). Publisher: IEEE. Yogyakarta, Indonesia.
9. Bairai, A. K.(2011), ASCII based Even-Odd Cryptography with Gray code and Image Steganography: A dimension in Data Security, ISSN:2078-5828 (Print), ISSN 2218- 5224 (Online), Vol.01,No.2, , pp:37-41, Manuscript Code: 110112.
10. Qiang Zhang , Ling Guo, Xiaopeng Wei, (2010). Image encryption using DNA addition combining with chaotic maps. Mathematical and Computer Modelling, Vol. 52, PP. 2028–2035.
11. Adinarayana Reddy Ka, Vishnuvardhan Bb, Madhuvishwanathamc, Krishna A. V. N.d (2012) .A Modified Hill Cipher Based on Circulant Matrices. Procedia Technology 4(2012) 114 – 118. 2212-0173 © 2012 Published by Elsevier Ltd. doi: 10.1016/j.protcy.2012.05.016 .
12. Raouf Hamzaoui, Dietmar Saupe . (2006). Barni, Mauro, ed. Fractal Image Compression. Document and Image Compression. 968. CRC Press. pp. 168–169. ISBN 9780849335563. Retrieved 5 April 2011.
13. Haider M. Al-Mashhadi.(2017).Quality Assessment for Image Encryption Techniques using Fuzzy Logic System. International Journal of Computer Applications,Vol. 157, No 5 .
14. Haider M. Al-Mashhadi; Iman Q. Abduljaleel.(2017) .Color Image Encryption using Chaotic Maps, Triangular Scrambling, with DNA Sequences. 2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT), Slemani – Iraq. 978-1-5386-2955-0/17/\$31.00 ©2017 IEEE.