Journal of Engineering and Applied Sciences 13 (Special Issue 8): 6359-6364, 2018
ISSN: 1816-949X

An Efficient Method for Encryption and Hiding Any File in Color Image

[1]Baheja K. Shukur, [2]Zaid Rajih Mohammed and [1]Sawsan Hadi
[1]Department of Information Technology, Babylon University, Hillah, Iraq
[2]Information Center, Jaber Ibn Hayyan Medical University, Najaf, Iraq

Abstract: Steganography is the process for hiding information into cover media. Many of techniques have been used for performing this process on electronic data, particularly audio and image data. Also, cryptography is considered as one of the most valuable and complicated areas in computer science. The need for cryptographic techniques in software used by the general public has increased with the domination of the internet due to the requirements to transmit secret information on a public network that facilitates information intercept and eavesdropping on its communications. Encryption can be defined as the procedure of altering the contents of text (data) into symbols and figures that are hard to interpret. The coding procedure is done with the use of many mathematic algorithms. In this study which deepened on two an effective and secure methods to encryption and hide information in color image. The suggest encryption method depend on the multi-level index and the generation of the content of the table randomly based on the generated equation ,in addition to that the range of the table take the range between 0-255 in both direction. This method is used to encryption any file for any extension. Moreover, to increase the production for this secure files concealing them in image. Applying an effective equation for hiding the secure file in random image position by making special calculating. To evaluate an encryption method number of evaluator measurement used between the original and encrypted file such as histogram, correlation and entropy. Also, we used PSNR, SSIM and NCC measurements to show the robustness for the steganography method. The system showing the good results in each method.

Key words: Steganography, cryptography, PSNR, SSIM, NCC, entropy

INTRODUCTION

The security of images becomes increasingly important for many applications such as military confidential transmission and medical applications where the amount of the digital images on internet has increased quickly. Therefore, the security of the conversion of the concealed information could be reached in 2 ways, cryptography and steganography. Those methods can be combined to made the security of data increased (Azzawi, 2014). In steganography, the cover image (or any media)used to embedded secret message in it, after that the recipient obtains the secret data from the cover image (Tomar, 2012). Once the private data is embedded, the cover image becomes known as a stego-image. Which is cannot be distinguished from the original image, consequently that the hacker can't realize any included data. In cryptography, the message is altered in such means that no message can be uncovered if received by a hacker (Meena *et al*., 2011).

The steganography might be utilized for hiding the presence of communication of enciphered message within a cover file which might be of different data types like text, image, audio and video using different steganographic algorithms (Sravanthi *et al*., 2012).

The idea of both cryptography and steganography is to give secret communication (Venkatraman *et al*., 2004). Steganography hides the presence of a message whereas encryption hides the content of the private message from a hacker. In cryptography if the hacker is capable of reading the confidential message then the system is broken (Bailey and Curran, 2006). While breaking a stego-system is composed of two phases: first the steganography algorithm may be detected by the attacker, the second stage is ability to read the embedded message (Tiwari *et al*., 2014). Also, the security of information is one of the most valuable elements of information technology and communications. To encipher and decipher the messages for the sake of keeping them secure many different methods and the secrecy of communication have been developed. In some cases it

Corresponding Author: Baheja K. Shukur, Department of Information Technology, Babylon Univesity, Hillah, Iraq

isn't sufficient keeping the content of the message private, it could in addition be essential to remain the presence of the message secret. For implementing this process the steganographic techniques are used (Usha *et al*., 2014).

To enhance the security of the embedded data the combination of these two methods have been use which assure the number of criterial like the robustness capacity and security for the secure data transfer via an open channel. In this study, the combination of cryptography and steganography methods have been used order to supply strong security.

MATERIALS AND METHODS

Performance criteria: One of the main needs for any image stego-system fidelity is the high fidelity which refers to the better visual quality of the stego image, from the viewpoint of image steganography means the visual quality of the resulting stego image after the procedure of embedding has happened. Number of standard image quality measurements might be utilized for the calculation of the fidelity of the steganography image. PSNR is the one most common measurement which refers to the peak Signal to noise ratio which represents the amount of degradation resulted in the stego image compared to the original image. It is essential defining Mean Square Error (MSE) in the computation of PSNR. Which canbe defined as follows (Roy and Changder, 2016):

$$MSE(cover,\ stego)=\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}\frac{\left(\begin{matrix}cover(i,\ j)-\\ stego(i,\ uj)\end{matrix}\right)^2}{M\times N} \quad (1)$$

$$PSNR(cover,\ stego)=10\times\log_{10}\left(\frac{255^2}{MSE}\right) \quad (2)$$

The other matrices is the SSIM (Structural Similarity Index Metric) which is given by Eq. 3:

$$SSIM=\frac{(2\times\bar{x}+\bar{y}+C1)(2\times\sigma_{xy}+C2)}{(\sigma_x^2+\sigma_y^2+C2)\times((\bar{x})^2+(\bar{y})^2+C1)} \quad (3)$$

Where C1 and C2 represent constants. $\bar{x}$, $\bar{y}$, σ_x^2, σ_y^2 and σ_{xy} are given (Varnan *et al*., 2011):

$$\bar{x}=\frac{1}{N}\sum_{i=0}^{N}x_i \quad (4)$$

$$\bar{y}=\frac{1}{N}\sum_{i=0}^{N}yi \quad (5)$$

$$\sigma_x^2=\frac{1}{N\text{-}1}\sum_{i=0}^{N}(x_i-\bar{x})^2 \quad (6)$$

$$\sigma_y^2=\frac{1}{N\text{-}1}\sum_{i=0}^{N}(y_i-\bar{y})^2 \quad (7)$$

$$\sigma_{xy}=\frac{1}{N\text{-}1}\sum_{i=0}^{N}(x_i-\bar{x})(y_i-\bar{y}) \quad (8)$$

To determine the efficiency of a cryptographic approach, it must be based on visual inspection, however, it doesn't give a view concerning how much information has been concealed. Thus an image encryption algorithm is considered to be good in the case where it's capable of concealing many image properties. Therefore, number of statistical matrices have been used such entropy as shown in Eq. 9 (Jawad and Fawad, 2013). The image entropy is considered using equality:

$$Entropy=-\sum_{i=0}^{N-1}P(i)*\log_2 P(i) \quad (9)$$

Where:

P (i) = Represents the probability of frequency of a pixel with gray level valuable 1

N = **T**he number of grey level in the image and the typical entropy of a 256 grey level image has to be 8

The other matrices is the correlation between original and ciphered images C.C which is computed as follows:

$$CC=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(A_{ij}-\bar{A})(B_{ij}-\bar{B})}{\sqrt{\left(\sum_{i=1}^{M}\sum_{j=1}^{N}(A_{ij}-\bar{A})^2\right)\left(\sum_{i=1}^{M}\sum_{j=1}^{N}(B_{ij}-\bar{B})^2\right)}} \quad (10)$$

With, $\bar{A}=\frac{1}{M\times N}\sum_{i-1}^{M}\sum_{j-1}^{N}A_{ij}$ and $\bar{B}=\frac{1}{M\times N}\sum_{i-1}^{M}\sum_{j-1}^{N}B_{ij}$

Where:

A = The original image

B = The ciphered image

i, j = The number of rows and columns

$\bar{A}$ and $\bar{B}$ = The average values of matrices A and B. M1 and M2 are the height and width of the original/ciphered image (Zhu, 2012)

Finally of these matrices is the Normalized Cross Correlation (NCC) which can be written as follow (Ganesan and Bhavani, 2013):

$$NCC = \sum_{j=1}^{M}\sum_{k=1}^{N}\left(X_{j,k}-X'_{j,k}\right)\frac{1}{\sum_{j=2}^{M}\sum_{k=2}^{N}\left(X_{j,k}\right)^{2}} \quad (11)$$

Suggested technique: The study suggested a new secure approach that hides the secret file into image in randomized manner; It is consists of two stages, i.e., cryptography and steganography. The suggested technique is random way to hide encrypted file into image which designed based LSB (Least Significant Bit) method. The following sections will illustration each process involved in detail.

Encryption stage: In the first stage, encrypting hidden file using suggested encryption algorithm, the proposed algorithm for modified playfair encryption and decryption are given, We have data structure have three parts:
First part: Two integer indexes is integer value ascending order.

Second part: Two char index is char random arrange, the char index take value from range between (A, B, ..., O, P).

Third part: Matrix (16*16) has random value between (0-255).

Encryption Algorithm 1:

Step 1: In this step, we want to convert all input value from byte vale to pairs of character take value from range between (A, B, ..., O, P) can do that as following steps:

1. Take prechiper as temporary variable for store the pairs of mapping values
2. Take value from plaintext as byte value
3. Map this value in Random matrix
4. Take the vertical char index and horizontal char index for the mapping value and put them in pair (XY)
5. prechiper = prechiper+pair(XY)
6. Repeat (2-5) until finish (take all value in input data)

Step 2: In this step, we want to increasing randomness by rearrange the data according following steps:

1. N = length of prechiper
2. H = N/2
3. I = 0
4. Take midchiper as temporary variable for store the new pairs
5. Take char of index I from prechiper and put it in midchiper
6. Take char of index (I+H) from prechiper and put it in midchiper
7. Increasing I by 1
8. Repeat (5-7) until (I = H)

Step 3: In this step, we want to increasing randomness by using double indexing and hash function as following steps:

1. Take output_chiper as temporary variable for store the encryption values
2. I = 0
3. Take char of index I from midchiper
4. X = find the hash function to this char
5. Increasing I by 1
6. Take char of index I from midchiper
7. Y = find the hash function to this char
8. Increasing I by 1
9. Mapping the values (X, Y) in random matrix to find Encryption value and put it in output_chiper
10. Repeat (3, ..., 9) until finish(take all value in midchiper)

Steganography stage: In second stage, in proposal method of steganography we using the Least Significant Bits (LSB) to store byte from encryption secret file in pixel from caver image that pixel is selected as random according the following algorithm.

Steganography Algorithm 2: This algorithm can by describe in following steps

Part one:-initial value
In this part we using set of initial value using in algorithm

1. Width = image width
2. Height = image height
3. Size= the size of hide file
4. The initial state of (x, y and z) is primary number between (0, 255) and must take large number as possible
5. K = 0, this is index to processing all byte of secret file
6. V = 0, this counter using to process the deadlock satiation

Part two: - Processing steps:
This part is consists of series steps must repeated until processing all byte of secret file

1. Flag = true, Boolean variable
2. Check if flag = true then go to step 3 else go to step 14
3. i = ((x * y) + z) mod width
4. j = (x + (y * z)) mod height
5. check if pixel of indexing (i, j) is not used to hide byte then go to step 6 else go to step 8
6. Using this pixel of indexing (i, j) to store one byte and set this pixel is used
7. flag = false
8. Update the values of x, y and z by using different equations and using (*, +, mod) operator
9. Check if flag = true then increasing V by one, else go to step 10
10. Check if V = 100 then go to step 11, else go to 13
11. Using new initial state for (x, y and z)
12. V = 0
13. Go to step 2
14. Increasing K by one
15. Check if (K = size of hide file) then go to End, else go to step 1.

End

RESULTS AND DISCUSSION

The testing result: The performance of the proposed technique has been evaluated by using several type of measures like (Structural Similarity Index (SSIM), Peak Signal to Noise Ratio (PSNR) and Normalized Cross Correlation (NCC)). To conform the performance the proposed technique applied on various types of files that have different size. Table 1 presented the histogram, entropy, max frequency for secret file and encrypted file and cross correlation between secret file and encrypted file. Table 2 showed the values of image quality metrics for stego image after hiding the secret file. Table 3 displayed the image quality metrics values when use various cover images and different secret file size.

Table 1: File extension, file size, histogram, entropy, max frequency and cross correlation for secret file and encrypted file

File extension	File size (kB)	Histogram of secret file	Max. frequency	Entropy	Histogram of encrypted file	Max. frequency	Entropy	Cross correlation
DOCX	179.4072		3756	7.9495		853	7.9965	0.00027
BMP	147.052		4627	6.7067		920	7.9599	-0.00567
TXT	42.701		7265	4.7624		1275	7.4739	-0.00703
JPG	58.0156		6560	7.755		1140	7.9775	0.00167
PDF	98.342		1334	7.9393		479	7.9957	0.00030
WMA	173.635		13672	7.738		1937	7.914	0.000255
RAR	164.954		3880	7.891		798	7.994	-0.00244
MP3	157.391		4226	7.874		1094	7.9769	-0.000284
+RTF	107.933		13422	5.2150		2117	7.7047	-0.00153
EXE	137		39418	5.625		7467	7.3412	0.00089
JPEN	99.1162		958	7.928		511	7.9905	-0.00054

Table 2: The cover image, stego image and image quality metrics values for stego image

Original image	Stego-image	SSIM	PNSR	NCC
		0.999692	47.45031	0.999689
		0.999673	47.47252	0.999668
		0.999652	47.4668	0.999647

Table 3: Image quality metrics values for different cover and secret file size

Image			Secret file		Image measurement		
Image name	Image size	No. of pixel	Secret file size (kB)	No. of byte	SSIM	NCC	PSNR
Lena	128*128	16384	7	7168	0.999675888160221	0.999672081364647	47.321971555265000
Lena	192*192	36864	16	16384	0.999677306497237	0.999673559384473	47.269531222057600
Lena	224*224	50176	21	21504	0.999687318724221	0.999683793647122	47.381989948354800
Lena	256*256	65536	27	27648	0.999692906651395	0.999689409827223	47.450311348067700
Lena	384*384	147456	61	62464	0.999694049344038	0.999690514851675	47.441940449326800
Lena	512*512	262144	108	110592	0.999696830222513	0.999693399297003	47.463177408725100
Baboon	224*224	50176	21	21504	0.999633154108805	0.999627787554186	47.358524135002000
Baboon	256*256	65536	27	27648	0.999652279552937	0.999647316516007	47.466829969979900
Airplane	224*224	50176	21	21504	0.999671885137972	0.999667023617230	47.472007347623900
Airplane	256*256	65536	27	27648	0.999673376590895	0.999668489950866	47.472521008663900

CONCLUSION

In this study, a combination of cryptography technique and steganography has been proposed. The proposed algorithm encrypts the information before hiding it in image file to increase the complexity of encryption/decryption process. The first method is to encrypt files containing evidence regardless of the file type, we encrypt data by the proposed method. The second way to protect data is hide files inside an image file in the suggested approach. The simulation outputs reflect the difference between the cover image and the stego image will be barely perceivable to the human eye.

REFERENCES

Azzawi, H.M., 2014. A proposed method for encrypting data in image by using cryptography technique and steganography. Mansour J., 22: 95-109.

Bailey, K. and K. Curran, 2006. An evaluation of image based steganography methods. Multimedia Tools Appl., 30: 55-88.

Ganesan, P. and R. Bhavani, 2013. A high secure and robust image steganography using dual wavelet and blending model. J. Comput. Sci., 9: 277-284.

Jawad, A. and A. Fawad, 2013. Efficiency analysis and security evaluation of image encryption schemes. Int. J. Video Image Process. Network Secur., 12: 18-31.

Meena, M.K., S. Kumar and N. Gupta, 2011. Image steganography tool using adaptive encoding approach to maximize image hiding capacity. Intl. J. Soft Comput. Eng. IJSCE., 1: 7-11.

Roy, R. and S. Changder, 2016. Quality evaluation of image steganography techniques: A heuristics based approach. Intl. J. Secur. Appl., 10: 179-196.

Sravanthi, G.S., B.S. Devi, S.M. Riyazoddin and M.J. Reddy, 2012. A spatial domain image steganography technique based on plane bit substitution method. Global J. Comput. Sci. Technol. Graphics Vision, 12: 1-8.

Tiwari, N., M. Sandilya and M. Chawla, 2014. Spatial domain image steganography based on security and randomization. Intl. J. Adv. Comput. Sci. Appl., 5: 156-159.

Tomar, G., 2012. Effect of noise on hidden data. Intl. J. Comput. Sci. Commun. Networks, 2: 12-15.

Usha, B.A., N.K. Srinath, S.M. D'souza and K.N. Sangeetha, 2014. Image and audio embedding technique in image steganography using neural networks. Intl. J. Adv. Res. Comput. Commun. Eng., 3: 7720-7725.

Varnan, C.S., A. Jagan, J. Kaur, D. Jyoti and D.S. Rao, 2011. Image quality assessment techniques on spatial domain. Int. J. Comput. Sci. Technol., 2: 177-184.

Venkatraman, S., A. Abraham and M. Paprzycki, 2004. Significance of steganography on data security. Int. Conf. Inform. Technol., 2: 347-351.

Zhu, C., 2012. A novel image encryption scheme based on improved hyperchaotic sequences. Opt. Commun., 285: 29-37.