International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(2): 183-188
The Society of Digital Information and Wireless Communications (SDIWC), 2018 ISSN: 2305-001

A New Scheme to Secure Communication and Data, based on the Integration of Cryptography and Steganography

Massoud Hadian Dehkordi [1], Amin Asgari [2], Ali Moradian [3]
School of Mathematics, Iran University of Science & Technology, Narmak, Tehran, 1684613114, *Iran*[1,2,3]
[1] mhadian@iust.ac.ir , [2] amin_asgari@mathdep.iust.ac.ir , [3] ali_moradian@mathdep.iust.ac.ir

ABSTRACT

Today, data and communication security have become challenging issues. Since in cryptography, encrypted messages are available to eavesdroppers, security is the subject of concern and the need for steganography and hiding the information has been raised. In this paper, by integrating cryptography and Steganography, a new scheme is proposed to enhance the data security. In encryption section, the CBC (Cipher Block Chaining) mode of operation is used, and in steganography section, we use graph coloring problem and the correlation of pixel blocks in LSB (Least Significant Bit) method. This helps to increase the capacity and security of steganography. The analysis of the quality functions shows that, in this method, the PSNR (Peak Signal-to-Noise Ratio) increases more than other methods.

KEYWORDS

Cryptography, Steganography, Correlation of Pixel Blocks, Graph coloring,

1 INTRODUCTION

Steganography is a skill of hiding a message over a communication channel or link, so that the secret message is deliberately latent among other irrelevant observed information which will result in hiding the presence of communication, and is based on the use of the spaces of the information carriers which does not damage the carrier's identity. Information carriers can be image, video, audio signal or text [1]. Cryptography is the art of the securing the information. This art, provides data security with concentration on storing and transmitting information safely over an insecure system, such as the Internet, by encrypting text data into an undetectable format and with the help of various encryption algorithms [2].

Information cryptography also uses cryptographic operations to provide more security, and both methods can be used simultaneously. Sometimes the methods of hiding information are designed in a way that the operation of cryptography was the basis of that method and is an integral part of it. [3,4]

The purpose of this paper is to enhance data security by using a block cypher mode of operation CBC, which is a symmetric cryptosystem (private key), before steganography, and by using the graph coloring and the correlation of pixels which optimize the information steganography algorithm and create a variable capacity at each threshold.

2 CYPHER BLOCK CHAINING (CBC) MODE OF OPERATION

In advanced cryptography block cypher modes have been designed to be applied to data formats. An easy way to encrypt a message m by using a block cypher of length n is to bring its length up to a multiple of the block size n by adding null bytes to the plain text if the message length is not divisible by n. This method is called padding. Then the plain text is decomposed into blocks of length n and each block is encrypted separately by applying a proper block cypher mode of operation. [5]

Pseudo-random permutations have many applications in modern cryptography and are known as block cyphers. In other words, one of the important tools for designing security protocols is block cypher. The easiest way to use a block cypher is to apply it to the main text format. To encrypt the message m with a specified length, firstly we bring it up to a multiple of the block size by using a padding technic (for example, adding a bit "1" and the adequate number of "0" at the end of the message). Then the plain text is decomposed into blocks of length m_i. The block cypher transforms n-bit blocks of plaintext as m_i into n-bit blocks of cypher text as C_i. [6]

In the CBC mode of operation, firstly, a random initialization vector IV of length n is chosen which can

be a part of the encrypted text, then the encrypted text is obtained (Figure 1).

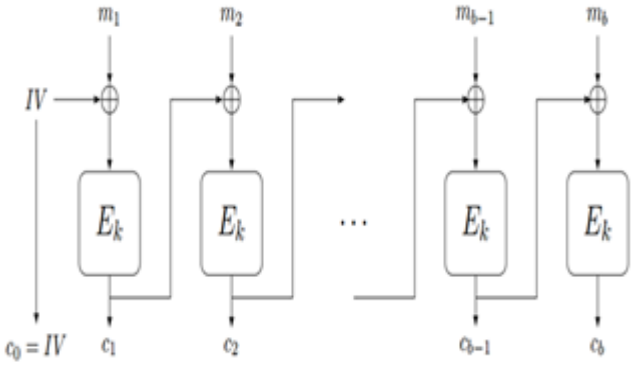


Figure 1. A crypto system in the operational mode of CBC

As it is shown in Fig. 1, the encryption function is defined as follows:

$$C_i = E_k(C_{i-1} \oplus m_i) \qquad C_i = IV \qquad 1 \le i \le b \quad (1)$$

The obtained cypher text is

$$C = < IV, C_1, C_2, \ldots, C_b >$$

To decrypt this cypher text, we get m_i by the following, and then the random sequence (IV) is deleted

$$m_i = E_k^{-1}(C_i) \oplus C_{i-1} \qquad (2)$$

It can be proven that if E is pseudo-random, permutation, the block cypher in the CBC operational mode has single-message and multi-message security, and is secured against the chosen-message attack. [7,8]

3 CORRELATION AMONG PIXEL BLOCKS IN THE HOST IMAGE

The correlation in the host image is the degree of dependence and relationship between each pixel with its surrounding pixels, and what is decisive in correlation in images is the numerical relationship between values of pixels, which can be used as an essential criterion for determining the quality and the capacity of steganography. But in the blocks correlation, the correlation among the host image block pixels are checked and according to correlation threshold, blocks are selected for data embedding. [9]

Since a data bit is embedded into the block, so it is clear that more blocks will result in more steganography capacity. When we want to split a picture of the size $X \times Y$ into $n \times n$ blocks, the number of blocks is obtained from the following equation.

$$t = \frac{(x \times y) - \begin{bmatrix} the\ number\ of\ pixels \\ on\ the\ edge\ hoet\ image \end{bmatrix}}{n \times n}$$

where t is the number of bits to be embedded. The pixels on the edge of host image are only used in calculation of correlation matrix, but not in prevention of distortion of the image edges in the process of embedding data.

4 STEGANOGRAPHY USING GRAPH COLORING AND PIXELS CORRELATION

Steganography by using graph coloring began in 2007 by Frederic et al. [9]. They analyzed the graph coloring in steganography, and proposed their scheme by combination of the Hemming code and a graph coloring. In the following years, the combination of coloring problem and ternary code was examined by another group. [10] In recent years, the use of steganography has been discussing for black and white photos, which is based on the definite similarity of pixel pairs in the entire image. [11]

In steganography by graph coloring scheme, the most important principles are having a graphical view to the picture, and for coloring the image, selection the best color number which is then saved in the colored pixels. See [12,13,14] for more information about graph coloring.

For coloring, various configurations in pixels are used. For example, consider the 3 × 3 pixel block in Figure (2-a). Its central pixel (node) has four neighbors which are numbered 2, 3, 4 and 5. For this block, from graph theory point of view, if the graph extends to infinity in all directions, we can conclude that all nodes have four neighbors (except the pixels in the first and last rows and columns, all of them have 4 neighboring pixels), or in other words, the extended graph, forms a 4-regular graph, and as we know, the maximum color number of a regular k-graphs is $1 + k$ [18]. So we can conclude that, the graph in (2-a) can be colored with 5 colors.

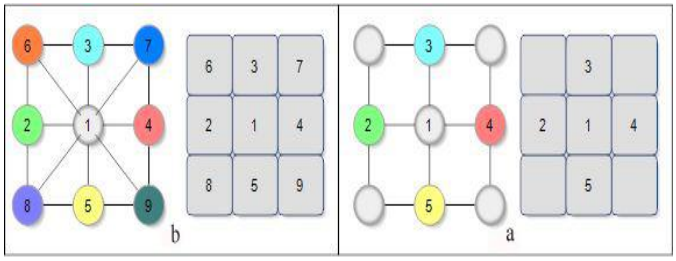


Figure 2. portion of Regular graph in the 3 × 3 pixel block

In Fig (2-b), a 3 × 3 pixel block has 8 neighbors and is marked with numbers 2 to 9. If this graph extends in all directions, we can see that all nodes will have 8 neighboring nodes that is somehow associated with an 8-regular graph. Then the graph can be colored by at least 9 colors. So except the pixels in the first and last rows and columns, all pixels form an 8-regular graph, and can be colored by 9 distinct colors.

Sometimes, according to requirements (image resolution or information embedding capacity), the color number is not taken into account and the pixel coloring starts with the appropriate color number, and with larger color numbers for coloring the desired image.

After coloring, the independent image pixels are put together. The independent image pixels have been modeled on the definition of maximal independent sets in graph coloring. [15] Now, the correlation among pixels is implemented in the new image with consideration of the different thresholds of information in the desired image. Then image reverts to the original state and is sent to the recipient.

5 PROPOSED SCHEME

In the proposed method, data is encrypted in the CBC mode of operation before being concealed. For this purpose, as described in section 2, firstly, we need to raise the main message length up to a multiple of the block size by using a padding scheme and then encrypt the blocks and separate *IV* from it, and then to embed the encrypted message in carrier image, we transform it into a bits array. As described in section 4, we color the host image with the agreed color number and put the independent pixels together, then split the image into blocks of 2×2, and by using the pixels correlation, as described in section 3, the blocks which have the desired threshold are used to embed the data in their LSB pixels. The steps of the proposed method are shown in Figure 3.

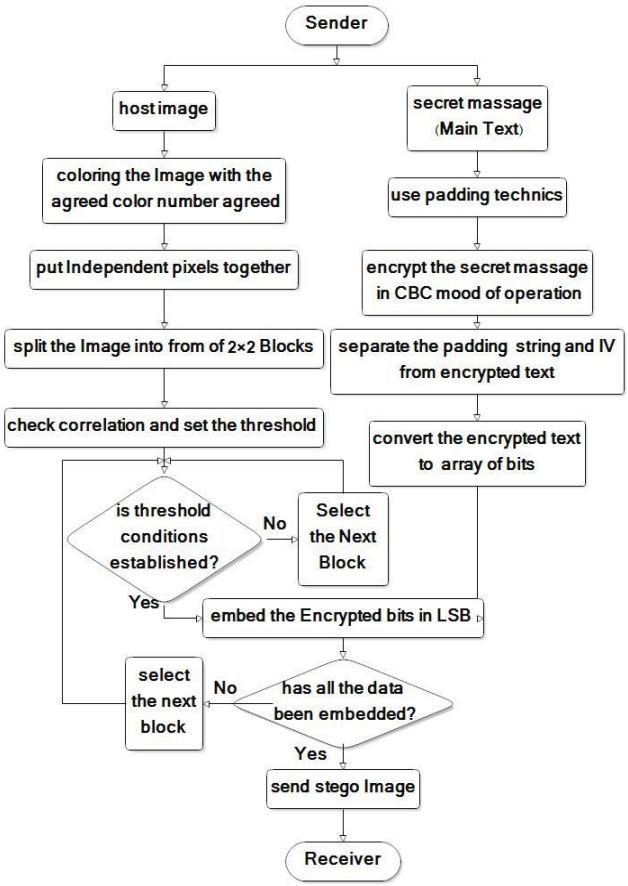


Figure 3. Schematic Algorithm for the proposed scheme

6 EVALUATION AND ANALYSIS OF THE PROPOSED METHOD

As described in Section 2, using random input *IV* makes the cryptographic function to become non-deterministic which provides the required security in CBC mode in the proposed scheme. So it resists against challenger's attack e.g. (single message, multi-message, CPA) [14]

To analyze the visual quality of the carrier image in steganography, the *PSNR* parameter is used, which is known as the maximum signal-to-noise ratio. This criterion is defined in dB as follows.

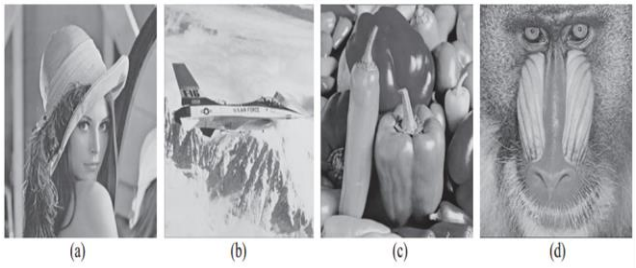
$$PSNR = 10 \times \mathrm{Log}(\frac{C_{max}^2}{MSE})$$

in which C_{max} is the maximum numerical value of pixel for each image, and *MSE* (Mean Squared Error) represents the mean square brightness used to measure image quality and is calculated as follows.

$$MSE = \frac{1}{\mathrm{M} \times \mathrm{N}} \sum_{x=1}^{M} \sum_{y=1}^{N} (S_{xy} - C_{xy})^2$$

where *x* and *y* are image coordinates, *M* and *N* are image dimensions, and the C_{xy} and S_{xy} are cover and carrier images, respectively. As above, with increase in the difference between covering and carrier images, *MSE* value increases and the *PSNR* value decreases. Therefore, a higher *PSNR* illustrates the higher quality of career image.

In order to discuss the results, we consider the following images. In Table 1, according to the explanations in Section 3, the correlation among their pixels has been calculated from the lowest to highest, respectively.



a) Lena b) jet c) pepper d) baboon

Figure 4. cover images with size 512 × 512

Table 1. Correlation Number of Image

number	1	2	3	4
Image name	Lena	baboon	pepper	jet
Correlation number	0/1002	0/112	0/1601	0/1702

Calculations have been done in Matlab 7.8, Windows 8 PC, 1.8 GHz CPU, intel ®core™ i5-3337U.

In the pixel correlation method, with increase in correlation, more blocks are used to embed data, which results in increasing the cache capacity. According to the Table 1, the Lena image has the lowest correlation, with 0.3 threshold and 0.206 hiding capacity, and the jet image, has the highest correlation, with a 0.3 threshold and 0.24 hiding capacity.

By calculating the *PSNR* for different images and the same threshold, it can be concluded that the *PSNR* is inversely related to the correlation number. For example, the *PSNR* at the 0.3 threshold for the Lena image, which has the lowest correlation number, is equal to 93/2556 and for the jet image with the highest correlation number is 93/012. This trend is true for all images and the overall result is that *PSNR* has a reverse relationship with the concealment capacity, i.e. the higher concealment capacity is, the lower *PSNR* value and therefor the lower resolution we have. It is clear that with lower threshold, more blocks will be selected to embed data, and this will also increase the cache capacity.

For example, consider Calculations for the jet image in Figure5, by using the graph coloring, the capacity at 0.3 threshold for colored numbers 5, 9, 203, 342 are 0.215, 0.2130, 0.2468, 0.2448 respectively, and 0.24 for the block correlation. (the colored numbers 203 and 342 refer to free graph coloring described in section 4), and in Lena image, capacity at 0.3 threshold for the mentioned colored numbers is 0.2274, 0.2102, 0.2425, 0, 2337, respectively, and in block correlation is 0.2060 (Figure 6). The above numbers indicate the creation of variable capacity in illustrated images; however, the difference between these numbers would increase at higher thresholds.

The numerical comparison of *PSNR* in block correlation with the coloring combination method and correlation shows that *PSNR* has almost the same value. In other words, it can be argued that by using graph coloring and block correlation, it is possible to create different variable capacity at different thresholds for image, which would appears more clearly by increasing the image correlation.

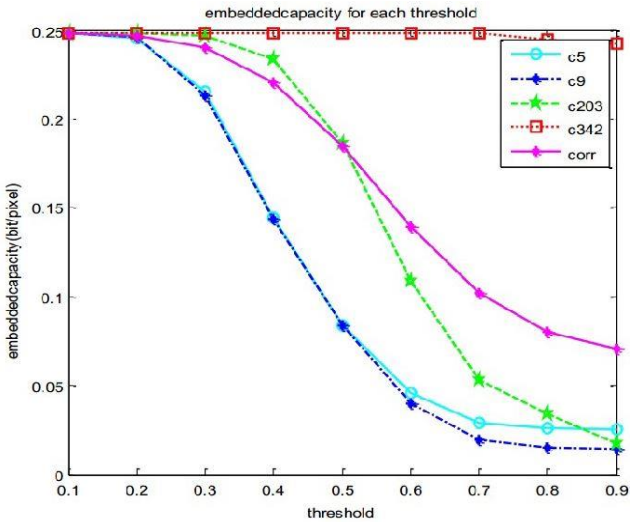


Figure 5. Embedded Capacity for each threshold

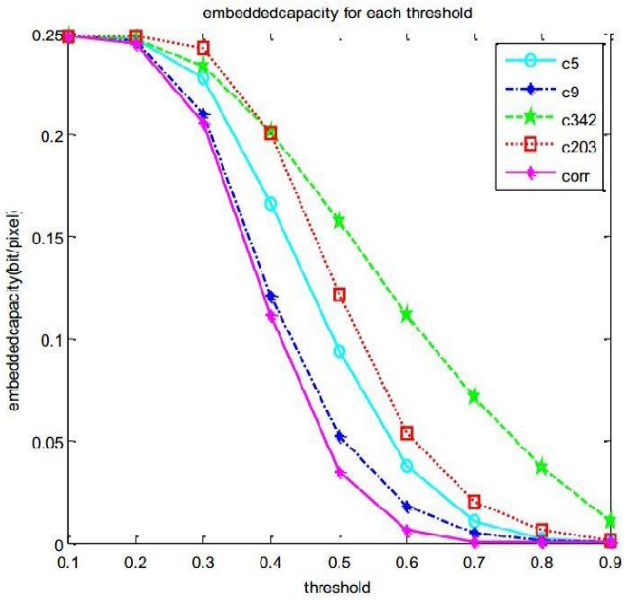


Figure 6. Embedded Capacity for each thrshold

7 BENEFITS OF PROPOSED SCHEME COMPARED TO OTHER METHODS AND CONCLUSION

7.1 Benefits of Proposed Scheme Compared to Other Methods

(1) In the proposed method, we can use the colored images which, due to the high redundancy, have more storage capacity, as well as the intangibility of changes made either in terms of appearance or in terms of process measurement quantities, such as *PSNR*. For further comparison see the Table 2. (It should be noted that the results were experimented in the same conditions).

Table 2. Comparative *PSNR* Performance of different methods and our proposed algorithm (512 × 512 pix)

schemes	PSNR Stego-image	
	Lena	baboon
LSB steganography & RSA cryptography[17]	41.58	40.15
Steganography with Genetic algorithm & blowfish system [18]	56.62	56.47
Proposed scheme	58.01	58.61

And results in figure7 or figure8 show that there is no difference between the original image and the stego-image for human visual.

(a) (b)

Figure 7. Figure 3 Hiding a message on Lena image. (a) cover images with size *512 × 512*, (b) is stego-image.

(c) (d)

Figure 8 Hiding a message on Baboon image. (c) cover images with size *512 × 512*, (d) is stego-image.

(2) The confidential text has been encrypted by a suitable and standard algorithm, which, even if the hidden secret text is discovered, it cannot be used without the encryption key.
(3) Although, key exchange requires a secure channel, it has more speed than public key methods.
(4) In this method, the Steganography is based on the pixel correlations, and is stored in the lowest bit of that channel, which causes the least visual changes in image, and the changes are not visible at all which results in steganography security.
(5) In terms of storing the message length, there would be little constraint on sending a different messages with a carrier image, as different capacity can be created with a different colored number.
(6) As *IV* in block cypher is generated randomly at each stage, if the attacker has access to the cryptographic function, he/she cannot retrieve any information from the embedded message, because each message at each stage of encryption in this cryptosystem would be different, due to the random input and non-deterministic encryption function. This will provide more security for the cached message.

7.2 Conclusion

In the proposed method, as the results suggest, the image quality is better than other methods. By assigning the appropriate color number to each image, the maximum capacity for each image can be created at different thresholds. Especially when image correlation increases, this value is highly variable in all thresholds. Also, CBC mode of operation allows us to ensure the security of the data embedded in the carrier image. The results of the implementation of the proposed method show that with the use of the cryptography and steganography combination the information security can be increased.

REFERENCES

1. R. Shreelekshmi, M. Wilscy and M. Wilscy , "Preprocessing Cover Images for More Secure LSB Steganography" International Journal of Computer Theory an Engineering, Vol. 2, No. 4, (August, 2010).pp1793-8201.
2. A. Singh and S. Malik "Securing Data by Using Cryptography with Steganography" International Journal of Advanced Computer Science and Software Engineering,Volume 3, Issue 5, (May 2013).
3. R. A. Adhipathi, and B. N. Chaterji 2004, "A new wavelet based logo watermarking scheme",Patter Recognition Letters, (September 2004).
4. P. Meerwald and A. Ulh, "A survey of Waveletdomain Watermarking Algorithms" ,Department of Scientific Computing, University of Salzburg, Austria, (2001).
5. M. Bellare. Practice-oriented provable security. Available via http://www.cse.ucsd.edu/users/mihir/crypto-papers.html (2008).
6. J. Katz and Y. Lindell, "Introduction to Modern Cryptography" ,Series Editor Douglas R. Stinson by Taylor & Francis Group, LLC (2008).
7. M. Bellare, J. Kilian and P. Rogaway. The security of the cipher block chaining CBC message authentication code. Journal of Computer and System Sciences, (Dec 2000).
8. W. D. Brent."Introduction to Graph Theory "University of Illinois at Urbana – Champaign, (1953).
9. M. Nafari, G. H. Sheisi, and M. Nejati Jahromi. "New Data Hiding Method Based on Neighboring Correlation of Blocked Image". Springer-Verlag Berlin Heidelberg (2011).
10. J. Fridrich and P. Lisonˇek. "Grid colorings in steganography". IEEE Trans. Inform. Theory, 53(4):1547–1549, (2007).
11. W. Zhang, X. Zhang, S. Wang. "Twice Grid Coloring in Steganography".IEEE .information conference on intelligent information hiding and multimedia signal procecing, (2008).
12. E. S. Mahmoodian, and F. S. Mousavi. "Coloring the square of products of cycles and paths".Sharif University Tehran Iran (February 2010).
13. J. A. Bondy , U. S. R. Murty , "Graph Theory" Graduate Texts in Mathematics ,Editorial Board S.Axler K.A.Ribet , ISBN: 978-1-84628-969-9, (2008).
14. S.Yue, Z. H. Wang, C. Y. Chang, C. C. Chang, and M. C. Li. "Image Data Hiding Schemes Based on Graph Coloring". In Springer Verlag Berlin Heidelberg (2011).
15. G. Qu and M. Potkonja. "Hiding Signatures in Graph Coloring". Computer Science Department, University of California, Los Angeles,USA, (June 2015), fgangqu,miodragg@cs.ucla.ed
16. M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation. Proceedings of the 38th Symposium on Foundations of Computer Science, IEEE, (1997).
17. S. Shetty, Minu P. Abraham "A Proposal to Secure Visual Cryptographic Shares of Secret Image using RSA" International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 12, (December 2014).
18. R. Begum, and S. Pradeep "Best Approach for LSB Based Steganography Using Genetic Algorithm and Visual Cryptography for Secured Data Hiding and Transmission over Networks" International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 4, Issue 6,(June 2014).