International Journal of Intelligent Information Systems
2014; 3(6-1): 98-102
Published online November 11, 2014 (http://www.sciencepublishinggroup.com/j/ijiis)
doi: 10.11648/j.ijiis.s.2014030601.28
ISSN: 2328-7675 (Print); ISSN: 2328-7683 (Online)

Color image encryption by code image and hill algorithm

Ali Moradmard*, Mohammad Tahghighi Sharabiani

Department of Computer Engineering, Islamic Azad University, Zanjan Branch, Zanjan, Iran

Email address:
a.moradmard@gmail.com (A. Moradmard), mtahghighi@yahoo.com (M. T. Sharabiani)

To cite this article:
Ali Moradmard, Mohammad Tahghighi Sharabiani. Color Image Encryption by Code Image and Hill Algorithm. *International Journal of Intelligent Information Systems*. Special Issue: Research and Practices in Information Systems and Technologies in Developing Countries. Vol. 3, No. 6-1, 2014, pp. 98-102. doi: 10.11648/j.ijiis.s.2014030601.28

Abstract: Today in a digital world, protection of information plays an essential role in message exchange and trading. Encryption is used to meet the security needs of safe transaction. Regarding the importance of the issue and the shift of traditional stage to digital stage, familiarity with encryption methods seems necessary. Different data have different methods of encryption. Images are also one type of data for which encryption is critically needed to prevent impermissible access. In this article, first a primary image is selected, then, based on the proportion of the image needing encryption, pixels from code image are picked and is being encrypted by a function. In the next stage, this proportion is being XOR-ed by the pixel proportion of the image needing encryption, and eventually the final proportion is encrypted by Hill Algorithm. MATLAB software has been used for studying the project, and efficiency of this method, in comparison to Hill Algorithm as a standard algorithm, is investigated. At the end, maintaining the image quality after decryption is evaluated by standards such as PSNR and SSID. The results indicate high efficiency of this method.

Keywords: Hill Algorithm, Security, Image Encryption, Efficiency

1. Introduction

A safe data exchange between source and target has al-ways been one of the big challenges in data transmission. The challenge seems more serious whenever the confidentiality of transmitted data is higher. One of the important data in information transmission is digital images. Transmitted images can have military, trading, or even medical applications, but regardless of the field, the security and preventing impermissible access of images is indisputable [1,12].

With the growth of social networks, huge data such as audio files, video files, and images can easily be transmitted to the internet. Therefore it is necessary to protect them from impermissible access. One way of keeping secret data transmission secure is encryption. Encryption, in fact, is the knowledge of changing message body or information by the help of a code key and an encryption algorithm so that only the person who knows keys and algorithm can extract the original information from encrypted information; and a person who does not know one or both cannot have access to them. Regarding image properties, especially high volume of images data, using encryption methods such as RSA [2], DES [3], and AES [4] are not directly applicable for image encryption, because encryption of high volume of image data via above methods is very time-consuming and practically is impossible in immediate usages. On the other hand, we face with the problem of key length in these methods. Since there is a high volume of encrypted data, using a key with a limited length leads to method vulnerability against the attacks of cipher text. To overcome the problems, many articles have been written about the image encryption in which the necessity of changes in the preliminary structure of the provided algorithms is admitted. However the methods are different due to images types.

Generally, images can be divided into many types like gray-scale and color images. Images are composed of units called pixels. Each pixel can show 256 different surfaces, which means an interval of 0 to 255. These surfaces are so-called image brightness. Gray scale images are composed of one matrix. Each house of this matrix saves one number inside. While color images are composed of three color matrix: red, green, and blue. Each pixel gains its own color by mixing these three colors. The encrypted images in this paper are color images.

Encryption Algorithm is divided into two types, symmetrical and asymmetrical. In symmetrical algorithm two sides of sender and receiver use the same key for encryption

and decryption [5, 6]. In this case, data decryption and encryption are two reverse processes.

In this article, first we produce a random matrix to the number of transmitted image pixels by the help of provided encrypted image algorithm, and then, by using extended Hill Algorithm we complete the encryption. To have the best form of encryption, we used all three layers (red, green, blue) and their solidarity in forming the final image caused more encryption of it. Visual analysis, quality analysis, and Histogram analysis have been used for evaluation of the provided method. The analysis results confirm the quality improvement of encrypted image by the proposed algorithm in comparison to the Hill Algorithm.

The research history and literature will be mentioned in the second section. In the third section definitions and the methods used will be discussed. The proposed algorithm will be in the fourth section and section five will include analyzing the proposed algorithm. Section six, the results and findings of the research are discussed.

2. Literature

According to literature about encryption, the history of the science goes back to 1900 B.C. Based on available documents, an Egyptian expressed pictorial texts by unusual images. But most works in digital encryption images have been done in 1990s [7]. Different image encryptions can be divided into two main groups [8]:

a) Chaotic encryption method

b) Non-chaotic encryption method

In most works done by the previous studies, the proposed encryption algorithm could only be implemented on some special formats such as BMP, JPG, TIFF, and just a few of them were applicable for different formats of images.

Kuang TsanLin [1] proposed using Fourier method an image encryption method for transmitting an image between the source and target. Xiaofeng Liao [9] used sound waves for image encryption. In this method the image had been dividing into two parts in which the first part used the other for image encryption. C. J. Tay [10] used two methods for image encryption. In the first method, they separated different parts of color image, which means three layers of red, green, and blue by special lenses, and each of them was encrypted by a special method. In the second method, the image is divided into two parts, image matrix and color map, and color map is encrypted by proposed method. Yicong Zhou [11] used Fibonacci series to image encryption and pixel displacement and compared its quality to original image after decryption by SSIM method. Xingyuan Wang [12] used chaotic function to encrypt color images and simultaneously encrypted all three matrix of red, green, and blue color and showed that the relationship between these three color factors brings about resistance against different attacks.

3. Definition and Methods

In this article, Hill Algorithm will be explained shortly and finally a proposed algorithm for image encryption based on Hill Algorithm will be illustrated.

3.1. Hill Encryption

Hill encryption was introduced by Lester Hill [13] to encrypt text in 1929. The core of encryption was using a matrix for multiplication in numerical equivalent in order to change it to a code and using inverse matrix (as a key) for decryption of numerical equivalent of the text. In the picture below, assuming 3*3 encrypted matrix, mathematical operations of encryption and decryption are shown.

3.1.1. Encryption Stages in Hill

In this example, we assumed that the matrix is 3*3. The procedure of encryption is based on Figure 1.

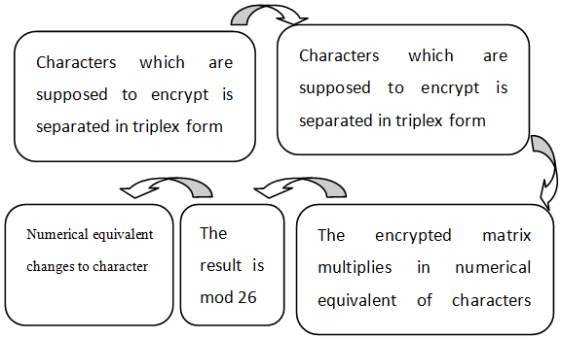

Figure 1. *Encryption stages in Standard Hill.*

$$= \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} Mod\,26 = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix} = "LNS" \begin{pmatrix} c1 \\ c2 \\ c3 \end{pmatrix} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 15"p" \\ 0"A" \\ 24"Y" \end{pmatrix}$$

As it was shown in formula (1), three first letters of (PAY) changed to three letters (LNS) after encryption.

3.1.2. Decryption Stages in Hill

Now the procedure of decryption in the source based on the same matrix 3*3 will be explained. The procedure can be seen in Figure 2.

$$\begin{pmatrix} p1 \\ p2 \\ p3 \end{pmatrix} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \begin{pmatrix} 11"L" \\ 13"N" \\ 18"S" \end{pmatrix} Mod\,26 = \begin{pmatrix} 15"P" \\ 0"A" \\ 24"Y" \end{pmatrix}$$

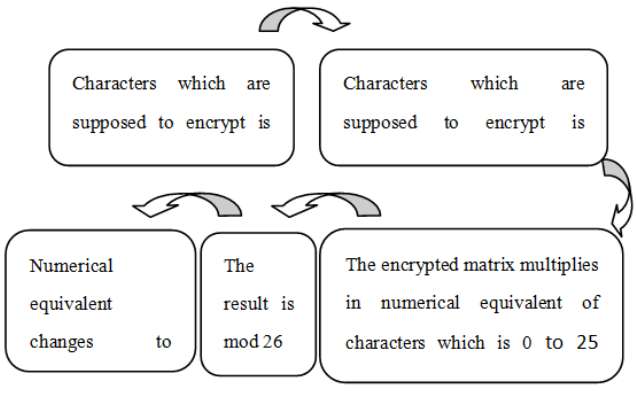

Figure 2. *Decryption stages in Standard Hill*

3.2. Using Encrypted Image Matrix

In this method, first an image will be shared between sender and receiver as a key. Now we select pixels from this picture (key) according to the number of pixels of the image which we want to encrypt.

Then, it will convert to the original encrypt picture by the mentioned equation.

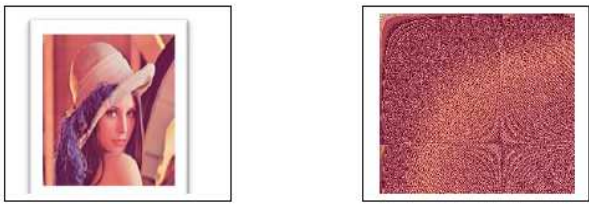

Figure 3. *Encrypted image Lena*

4. The Proposed Algorithm

In the proposed algorithm, first an image will be shared between the sender and receiver. Then, the image we want to encrypt is XOR-ed by key image. In the stage of pixel changing for image encryption, numerical equivalence of pixels in all three levels (blue, red, green) must be multiplied by encrypted matrix. In this article, we used the same multiplication matrix 3*3, and one pixel of each layer has been selected for encryption, and this number will be put instead of numerical equivalent in Hill method.

In Figure 4, you can see peppers image after encryption by preliminary Hill Algorithm by matrix 3*3. Some parts of the encrypted image are not uniform in this encryption, and the primary image is visible in the encrypted one.

Since one of the important factors in encryption quality is image uniformity after decryption, we propose some solutions to improve it.

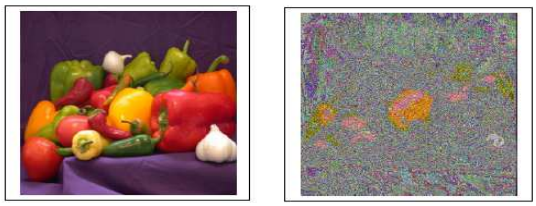

Figure 4. *Primary and encrypted image by Standard Hill Algorithm*

In Figure 5, the spots which were not completely encrypted has been shown in Hill Algorithm, were well covered by the proposed algorithm.

Figure 5. *Primary and encrypted image by the proposed algorithm.*

5. Efficiency Analysis (Result Evaluation)

5.1. Visual Analysis

In this section, to have a better comparison of the two mentioned methods, we used images in which adjacent pixels are very similar to each other because Hill Algorithm has a high efficiency drop in this condition [14] and we can have a better evaluation.

By the help of proposed combined method in this article, it was shown in the visual test that images which were encrypted just by Hill method are largely recognizable Figure 6, but some improvements can be seen in the visual test after using the proposed combined algorithm Figure 7.

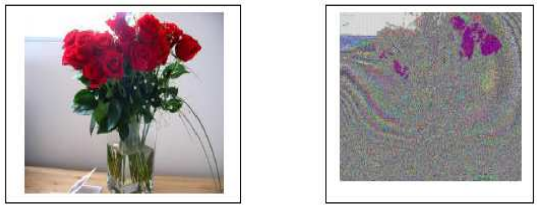

Figure 6. *Decrypted image by Standard Hill algorithm.*

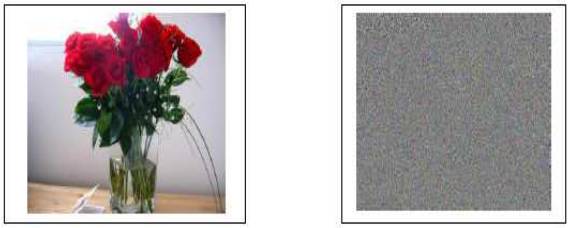

Figure 7. *Decrypted image by the proposed algorithm.*

5.2. Histogram Analysis

One of the most important image encryption principles to avoid information leakage and invaders' attack is that there should not be any statistical similarities between the encrypted image and the original image. Using repetition rate of each pixel in the image, Histogram analysis shows the distribution manner of pixels in it. [15] The more uniformity in the chart surface would bring about the more dispersion of the pixels. The peppers image, which is among available images on MATLAB, has been used for the test. The Histogram comparison of encrypted image (Fig.8) with the original image (Fig.9) shows that these two pictures are totally different and there is no statistical similarity between them. Finally, the comparison of decrypted image with the original image shows the quality of decrypted image.3

Table 1. *The features of quality analysis*

	Image	PSNR	MSE	SSID
1	Encrypted image(Lena)	11,08	5,06	0,09
2	Original image(Lena)	43,29	3,04	0,99
3	Encrypted image(peppers)	10,47	5,82	0,08
4	Original image(peppers)	39,42	6,76	0,99
5	Encrypted image(Flowers)	9,97	6,54	0,19
6	Original image(Flowers)	45,86	1,68	0,99

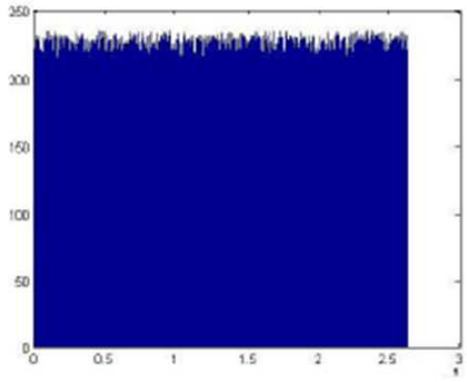

Figure 8. *Histogram of the encrypted image.*

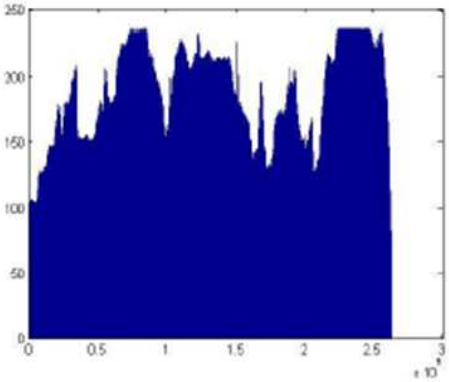

Figure 9. *Histogram of the original image.*

5.3. Quality Analysis

The measure of quality change between the encrypted image and original image:

Structural similarity (SSIM), proposed by Wang [16], is a quality test to measure the similarities between two images. Peak signal-to-noise ratio is used to calculate quality change between two images and two images are more similar to each other when the number is closer to 50 [16].

For testing the similarity between two images in both methods of quality analysis, MATLAB is used.

6. Discussion and Conclusion

In this article, a simple and efficient way for image encrypting by the use of Hill Encryption Algorithm was proposed. In this method, first the original image with N*M pixels was XOR-ed to N*M size by created pixels by produced values of a shared image between the sender and receiver, and the result was encrypted by Hill Algorithm. In Hill Algorithm, pixels values were used for encryption (each time, one red layer, one green layer, and one blue layer). The selected image, with regard to the relationship of these pixels for making related pixel, was encrypted. Three tests named visual test, Histogram analysis, and quality change algorithms were used to compare the original image and decrypted image (PSNR, SSID) and the result of visual test showed an improvement in encrypted images via proposed method comparing to the previous method. Moreover, in evaluating Histogram analysis, there was no similarity between the original image and the encrypted image. In the encrypted image quality test, there is a little difference between the images after decryption comparing to the original images.

References

[1] Kuang Tsan Lin, " Binary encoding method to encrypt Fourier-transformed", information OF 15th Annu. Conf. IEEE EMBS, pp. 778-780, 1993.

[2] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, pp.120-126, 1978.

[3] Eli Biham, Adi Shamir, "Differential cryptanalysis of DES-like cryptosystems", Springer, Volume 4, Issue 1, pp.3-72, 1991.

[4] Joan Daemen, Vincent Rijmen, "The Design of Rijndael: AES The Advanced Encryption Standard", Springer, p.238, February 2002.

[5] R.Kusters and MTuengerthal, "Universally Composable Symmetric Encryption", 2nd IEEE Computer Security Foundations Symposium (CSF '09), pp. 293-307, July 2009.

[6] H Jin, Z.Liao, D.Zou, and C.Li, "Asymmetrical Encryption Based Automated Trust Negotiation Model", The 2nd IEEE International Conference on Digital Ecosystems and Technologies (DEST 2008), pp.363-368, Feb. 2008.

[7] Shiguo Lian, "Multimedia Content Encryption Techniques and Applications", CRC Press,p.3.

[8] Ratinder Kaur, V. K. Banga, "Image Security using Encryption based Algorithm", International Conference on Trends in Electrical, Electronics and Power Engineering (ICTEEP'2012) Singapore, July 15-16, 2012.

[9] Xiaofeng Liao, Shiyue Lai, Qing Zhou, "A novel image encryption algorithm based on self-adaptive", Digital Signal Processing Principles, New York Macmillan, 1992.

[10] C.J. Tay, C. Quan, W. Chen, Y. Fu, "Color image encryption based on interference and virtual optics", Optics & Laser Technology, pp. 409–415, 2010.

[11] Yicong Zhou, Karen Panetta, SosAgaian, C.L. Philip Chen," Image encryption using P-Fibonacci transform and decomposition","Optic s Communications", 285 (2012) 594–608

[12] Xingyuan Wang, Lin Teng, Xue Qin, "A novel colour image encryption algorithm based on chaos", Signal Processing, pp.1101–1108, 92 (2012).

[13] Lester S. Hill, "Cryptography in an Algebraic Alphabet", The American Mathematical Monthly" ,Vol.36, pp. 306–312, June–July 1929.

[14] J.Zillami and D. G. Manolakis, "Encryption Based On Advance Hill, Algorithms and Applications", New York Macmillan, 2008.

[15] Ahmed A. Abd El-Latif, Li Li, Ning Wang, Qi Han, Xiamu Niu, "A new app roach to chaotic image encryption based on quantum chaotic system, exploiting color spaces Signal Processing", Volume 93, pp.387-397, 2013.

[16] Z. Wang, A.C. Bovik, H.R. Sheikh, E.P. Simoncelli, ” Image Quality Assessment: From Error Visibility toStructural Similarity”, Transactions on Image Processing IEEE, pp.600-612, 13 (2004).