A Novel Encryption Method for Image Security

Mohammed Abbas Fadhil Al-Husainy

Department of Multimedia Systems, Faculty of Science and Information Technology, Al-Zaytoonah University of Jordan. Amman-Jordan
P.O. Box: 130 Amman (11733) Jordan, Tel.: 962 79 6846110, Fax: 962 6 4291432
dralhusainy@yahoo.com , alhusainy@alzaytoonah.edu.jo

Abstract

Image encryption is one of the most methods of information hiding. A novel secure encryption method for image hiding is presented in this paper. The proposed method provides good confusion and diffusion properties that ensures high security due to mixing the two Boolean operations: XOR and Rotation that are done on the bits of the pixels in the image. This method is implemented by firstly doing a sequential XOR operation on all the bits of pixels in the image, and secondly makes a circular rotate right of these bits. These two operations are repeated many times during the encryption phase. The security and performance of the proposed encryption method have been evaluated by applying it on images and analyze the recorded results using key space analysis, key sensitivity analysis, and statistical analysis. The performance experiments show that the proposed method is promising to use effectively in wide fields of image encryption.

Keywords: *Rotation, XOR, Information Security, Cryptography, Confusion, Diffusion*

1. Introduction

Data encryption is a product of the information theory area of mathematics, an area that addresses various ways to manage and manipulate information. Cryptography contains two basic processes: one process is when recognizable data, called plain data, is transformed into an unrecognizable form, called cipher data. To transform data in this way is called to encipher the data or encryption. The second process is when the cipher data is transformed back to the original plain data, this is called to decipher, or decrypting the data. To be able to determine if a user is allowed to access information a key is often used. Once a key has been used to encipher information, only someone who knows the correct key can decipher the encrypted data. The key is the foundation of most data encryptions algorithms today. A good encryption algorithm should still be secure even if the algorithm is known [1-5].

Encryption is the process of transforming the information to insure its security. With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks. It is often true that a large part of this information is either confidential or private. As a result, different security techniques have been used to provide the required protection [6].

With the advancements of multimedia and networks technologies, a vast number of digital images now transmitted over Internet and through wireless networks for convenient accessing and sharing [5]. Multimedia security in general is provided by a method or a set of methods used to protect the multimedia content. These methods are heavily based on cryptography and they enable either communication security, or security against piracy (Digital Rights

Management and watermarking), or both. Communication security of digital images and textual digital media can be accomplished by means of standard symmetric key cryptography. Such media can be treated as binary sequence and the whole data can be encrypted using a cryptosystem such as Advanced Encryption Standard (AES) or Data Encryption Standard (DES) [7]. In general, when the multimedia data is static (not a real-time streaming) it can treated as a regular binary data and the conventional encryption techniques can be used. Deciding upon what level of security is needed is harder than it looks. To identify an optimal security level, the cost of the multimedia information to be protected and the cost of the protection itself are to be compared carefully.

As a result, protection of digital images against illegal copying and distribution has become an important issue [5, 8-10]. Image encryption techniques try to convert an image to another one that is hard to understand [11]. On the other hand, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types.

At present, there are many available image encryption algorithms such as Arnold map, Tangram algorithm [12], Baker's transformation [13], Magic cube transformation [14], and Affine transformation [15] etc. In some algorithms, the secret-key and algorithm cannot be separated effectively. This does not satisfy the requirements of the modern cryptographic mechanism and are prone to various attacks. In recent years, the image encryption has been developed to overcome above disadvantages as discussed in [7, 16]. Conventional encryption algorithms such as DES, AES, IDEA are not suitable for practical image cipher due to some intrinsic features of images such as bulk data capacity, high redundancy, strong correlation among adjacent pixels, etc. It is desirable to develop an efficient image cryptosystem, especially for real-time secure image communication over open networks. To meet this challenge, a variety of image encryption schemes have been proposed. Among them, chaos-based algorithm has suggested a new and efficient way to deal with the intractable problems of fast and highly secure image encryption. The fundamental features of chaotic dynamical systems such as ergodicity, mixing property, sensitivity to initial conditions/system parameters, etc. can be considered analogous to some ideal cryptographic properties such as confusion, diffusion, balance, avalanche properties, etc. [17-20].

2. The Proposed Method

The main idea behind the proposed method to encrypt digital images is trying to create an easiest and high secure encryption and decryption method that is satisfying good confusion and diffusion features in the encrypted image. Many recent researches have proved that the confusion module has a relatively low security level. It is weak against many kinds of attacks, especially statistical attack since the histogram of the shuffled image is completely unchanged. Thus the security of the cryptosystem mainly relies on the diffusion process. To improve the security of the confusion module and further the whole image cryptosystem, this paper proposes a bit-level permutation method which introduces a certain diffusion effect with confusion effect. The architecture of the encryption and decryption phases of the proposed method is depicted in Figure 1:

First of all, some definitions and terminologies are given bellow which is helping in understand the encryption and decryption operations of the proposed method.

- Secret Key Length (***k***): is a number of bits that the secret key consists of. Such that, it may be any number can be represented as (8**P*) bits, where $P \geq 1$. For example, the secret key length *k* may be 64-bits, 128-bits, 256-bits, …. This key must keep secret between the sender and the receiver of the image.

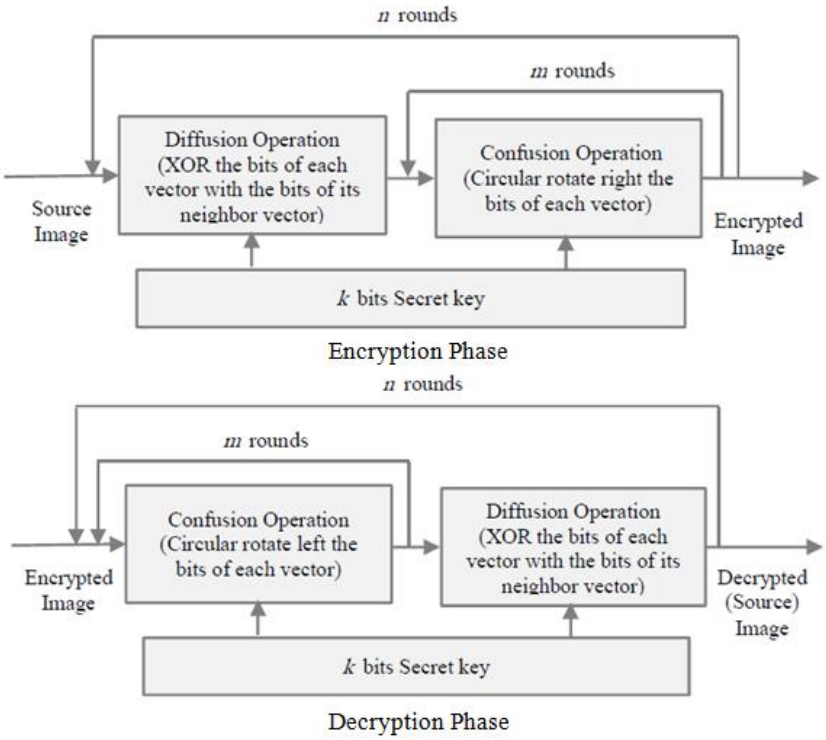


Figure 1: Architecture of the Encryption and Decryption Phases

- Source Image $\boldsymbol{I_S}$**(*Length*)**: Obviously, any bitmap image, like of type (.bmp) which is choosing in this work for the purpose of test, is a two dimensional array list of pixels. Each image has Width, Height and Palette. The proposed method look in a different view to the image file, it treats the image file as a binary file that is consisting of a contiguous series of bits by converting all the bytes values in the file to the equivalent bits representation, where each byte value is between (0...255) and (1byte = 8bits). Therefore, in this work, the total number of bits in the source image $\boldsymbol{I_S}$ (i.e., ***Length***) equal (Width×Height×Palette×8)
- Encrypted Image $\boldsymbol{I_E}$**(*Length*)**: It is similar to the source image $\boldsymbol{I_S}$, and it is produced from $\boldsymbol{I_S}$ after applying the operations that are doing in the encryption phase of the proposed method.
- Decrypted Image $\boldsymbol{I_D}$**(*Length*)**: It is similar to the source image $\boldsymbol{I_S}$, but it is produced from $\boldsymbol{I_E}$ after applying the operations that are doing in the decryption phase of the proposed method.
- XOR Bit Operation: is a Boolean operation which is using in this work to make a change in the bits during the encryption and decryption phases of the proposed method.
- Rotate-right and Rotate-left Bit Operations: these are two Boolean operations which are using in this work to make a circular rotate (right/left) on the bits during the encryption and decryption phases of the proposed method.

A. Encryption Phase: to create the I_E from the I_S, the following steps clarify in detail the operations that are doing in this phase of the proposed method.

Step1: Select a *Secret Key* of length (number of bits)=*k*;

Step2: Create a list of binary vectors *VectorList* [*NoOfVectors*] by splitting the I_S into a set of vectors, each vector consist of *k* number of bits. Where *NoOfVectors* = *Length*/*k*, and the indices of vectors in *VectorList* (0… *NoOfVectors*-1).

Step3: Set *TempVector*=*VectorList* [0] and set *VectorList* [0]=*Secret Key*

Step4: Set number of rounds *n* = number of 1s bits in the vector *VectorList* [0]

Step5: For *Round*=1 to *n*

Diffusion Operation:

For *Index*=1 to *NoOfVectors*-1

Set *VectorList* [*Index*]= *VectorList* [*Index*-1] XOR *VectorList* [*Index*];

(for example: (10100110) XOR (10010111) → (00110001))

Confusion Operation:

For *Index*=0 to *NoOfVectors*-1

Circular Rotate-Right *VectorList*[*Index*] number of times equal to the number of 0s bits in It;

(for example: Rotate-Right (10100110) → (01101010))

Step6: Set *VectorList* [0]=*TempVector*

Step7: Restore the *VectorList* in I_E

B. Decryption Phase: In reverse, to create the I_D from the I_E, the following steps clarify in detail the operations that are doing in this phase of the proposed method.

Step1: Use the same *Secret Key* of length *k*, that is selected in encryption phase;

Step2: Create a list of binary vectors *VectorList* [*NoOfVectors*] by splitting the I_E into a set of vectors, each vector consist of *k* number of bits. Where *NoOfVectors* = *Length*/*k*, and the indices of vectors in *VectorList* (0… *NoOfVectors*-1).

Step3: Set *TempVector*=*VectorList* [0] and set *VectorList* [0]=*Secret Key*

Step4: Set number of rounds *n* = number of 1s bits in the vector *VectorList* [0]

Step5: For *Round*=1 to *n*

Confusion Operation:

For *Index*=0 to *NoOfVectors*-1

Circular Rotate-Left *VectorList*[*Index*] number of times equal to the number of 0s bits in It;

(for example: Rotate-Right (01101010) → (10100110))

Diffusion Operation:

For *Index*= *NoOfVectors*-2 to 0

Set *VectorList* [*Index*+1]= *VectorList* [*Index*] XOR *VectorList* [*Index*+1];

(for example: (10100110) XOR (00110001) → (10010111))

Step6: Set *VectorList* [0]=*TempVector*

Step7: Restore the *VectorList* in I_D

3. Experimental Results and Security Analysis

To evaluate the proposed encryption method, this method is tested on a number of bitmap images of type (.bmp) which have different sizes. Some security analysis has been performed on the proposed image encryption method, including the most important ones like key space analysis, key sensitivity analysis, and statistical analysis, to demonstrate that the proposed method has good security features.

A. Key Space Analysis

For an effective cryptosystem, the key space should be large enough to make brute-force attack infeasible. The secret key space in the proposed method is (8**P*) bits, where $P \geq 1$, this means that the cryptosystem can has a wide range of key space (from 2^8 to $2^{(8*P)}$) bits. Figure 2 shows different encrypted images, of the same source image, by using 16-bits and 64-bit key length. Thus this cryptosystem is a $2^{(8*P)}$ bits key space, while the key space of the most well-known secure encryption algorithm AES is 128-bits. So this is proof that the proposed cryptosystem is good at resisting brute-force attack.

Figure 2: (a) Source Image. (b) Encrypted Image with 16-bits Key. (c) Encrypted Image with 64-bits Key

B. Key Sensitivity

To evaluate the key sensitivity feature of the proposed method, a one bit change is made in the secret key and then used it to decrypt the encrypted image. The decrypted image with the wrong key is completely different when it is compared with the decrypted image by using the correct key as shown in Figure 3. It is the conclusion that the proposed encryption method is highly sensitive to the key, even an almost perfect guess of the key does not reveal any information about the plain image.

Figure 3: (a) Source Image. (b) Decrypted Image with Wrong Key

C. Statistical Analysis

Statistical attack is a commonly used method in cryptanalysis and hence an effective cryptosystem should be robust against any statistical attack. Calculating the histogram and the correlation between the neighbors pixels in the source and in the encrypted image are the statistical analysis to prove the strong of the proposed cryptosystem against any statistical attack.

Figure 4 shows the histograms of source image and its encrypted image respectively. It's clear from figure 4 that the histogram of the encrypted image is completely different from the histogram of the source image and does not provide any useful information to employ statistical attack.

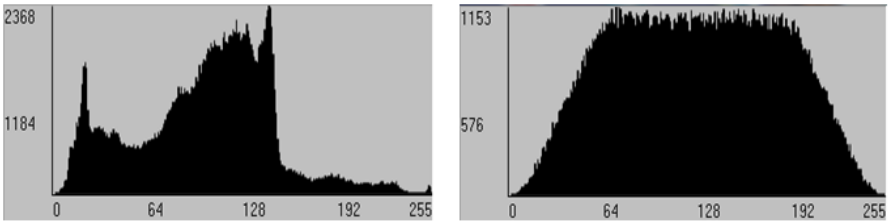


Figure 4: (a) Histogram of the Source Image in Figure (2)a. (b) Histogram of the Encrypted Image in Figure (2)c

The correlation coefficient *r* is calculating by using the following formulas:

$$r = \frac{\sum_{i=1}^{N}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{N}(x_i - \overline{x})^2 \times \sum_{i=1}^{N}(y_i - \overline{y})^2}}$$

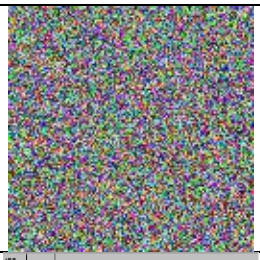
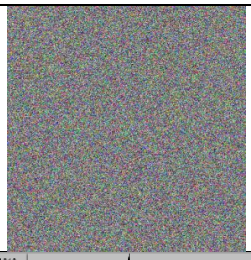
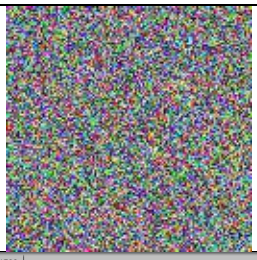
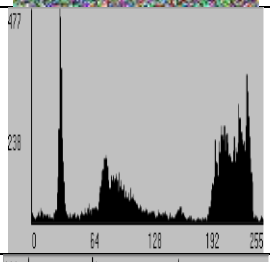
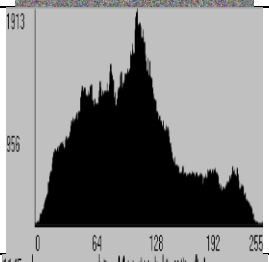
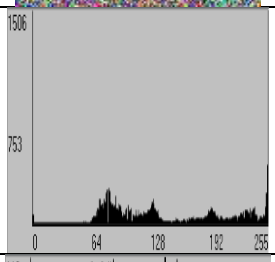
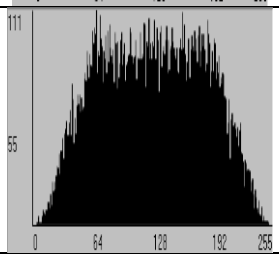
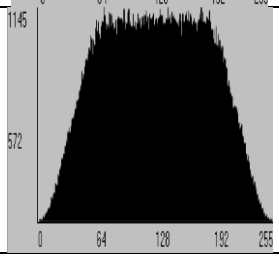
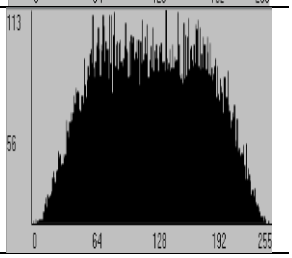
Where *N* is the number of pixel pairs, $\overline{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$ and $\overline{y} = \frac{1}{N}\sum_{i=1}^{N} y_i$

The correlation coefficient for horizontal neighbor pixels of the source image is *r*=0.59971 while *r*=0.00412 for the encrypted image in figure 2c. It is clear from these two different values for the correlation coefficient that the strong correlation between neighbor pixels in source image is greatly reduced in the encrypted image. The results of the correlation coefficient for vertical and diagonal neighbor pixels are similar to the horizontal neighbor pixels.

Also, other experiments on some bitmap images are done to encrypt these images by using the proposed encryption method and the results of these experiments are summarized in Table 1 follow:

Table 1: Experiments and their Security Analysis Measures

Source Image			

Encrypted Image			
Histogram of Source Image			
Histogram of Encrypted Image			
Correlation of Source Image	0.673263	0.848757	0.355331
Correlation of Encrypted Image	0.002959	0.000302	0.002147

4. Conclusions

In this paper, a novel simple and strong encryption method has been proposed for image security. The simplicity came from using two Boolean operations XOR and Rotate to make a satisfactory diffusion and confusion in the bits of the pixels of the image. And the strong came from the ability of the cryptosystem to use a large number of bits in the secret key. The security analysis measures show that when we applied the proposed method to encrypt images, the method results a high secure image. Based on the results that are recorded from the experiments, we conclude that the performance of the proposed image encryption method is perfect and suitable to use for image encryption in a wide range of application.

References

[1] Petkovic, M., Jonker, W. Preface, "Special issue on secure data management," *Journal of Computer Security*, 17(1), pp.1-3 **(2009)**

[2] Bernstein, D.J., Chen, T.R., Cheng, C.M., Lange, T. & Yang, B.Y. "ECM on graphics cards". *In A. Joux (Ed.), Advances in Cryptology - Eurocrypt 2009 (28th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Cologne, Germany, April 26-30, 2009. Proceedings) Vol. 5479. Lecture Notes in Computer Science (pp. 483-501). Berlin: Springer **(2009)**

[3] Bernstein, D.J., Lange, T., Peters, C.P. & Tilborg, H.C.A. van. "Explicit bounds for generic decoding algorithms for code-based cryptography". *In International Workshop on Coding and Cryptography (WCC 2009, Ullensvang, Norway, May 10-15, 2009. Pre-proceedings)* (pp. 168-180). Bergen: Selmer Center, University of Bergen **(2009)**

[4] Stevens, M., Sotirov, A., Appelbaum, J., Lenstra, A.K., Molnar, D., Osvik, D.A. & Weger, B.M.M. de. "Short chosen-prefix collisions for MD5 and the creation of a 18 rogue CA certificate". *In S. Halevi (Ed.), Advances in Cryptology - CRYPTO 2009 (29th Annual International Cryptology Conference, Santa Barbara CA, USA, August 16-20, 2009. Proceedings)* Vol. 5677. Lecture Notes in Computer Science (pp. 55-69). Berlin: Springer **(2009)**

[5] Kahate A., "CRYPTOGRAPHY AND NETWORK SECURITY", *Tata-McGraw-Hill*, 2nd edition **(2008)**

[6] H. El-din. H. Ahmed, H. M. Kalash, and O. S. Farag Allah, "Encryption quality analysis of the RC5 block cipher algorithm for digital images," Menoufia University, Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menouf-32952, Egypt **(2006)**

[7] D.R. Stinson, "Cryptography Theory and Practice," CRC Press, Inc. **(2002)**

[8] Arnold EA, Avez A, "Ergodic Problems of Classical Mechanics", *Benjamin, W. A., New Jersey*, Chap. 1, pp.6 **(1968)**

[9] Cheng-Hung Chuang, Zhi-Ye Yen, Guo-Shiang Lin, et al, "A Virtual Optical Encryption Software System for Image Security", *JCIT*, Vol. 6, No. 2, pp.357-364 **(2011)**

[10] Brahim Nini, Chafia Melloul, "Pixel Permutation of a Color Image Based on a Projection from a Rotated View", *JDCTA*, Vol. 5, No. 4, pp.302-312 **(2011)**

[11] Li. Shujun, X. Zheng "Cryptanalysis of a chaotic image encryption method," Inst. of Image Process. Xi'an Jiaotong Univ., Shaanxi, This paper appears in: *Circuits and Systems, ISCAS 2002. IEEE International Symposium* on Publication Date: 2002, Vol. 2, pp.708-711 **(2002)**

[12] Wei Ding, Wei-qi Yan, and Dong-xu Qi, "A Novel Digital Hiding Technology Based on Tangram Encryption", *IEEE Proceedings of on NEWCAS 2005*, and Conways Game", Proceeding of 2000 International Conference on Image Processing, Vol. 1, pp. 601-604 **(2000)** September.

[13] Zhao Xue-feng, "Digital Image Scrambling Based on the Baker's Transformation", *Journal of Northwest Normal University (Natural Science)*, Vol. 39, No. 2, pp. 26-29 **(2003)** February.

[14] Bao Guan-jun, Ji Shi-ming, and Shen Jian-bin, "Magic Cube Transformation and Its Application in Digital Image Encryption", Computer Applications, Vol. 22, No. 11, pp. 23-25 **(2002)** November.

[15] Zhu Guibin, Cao Changxiu, Hu Zhongyu, et al., "An Image Scrambling and Encryption Algorithm Based on Affine Transformation", *Journal of Computer-Aided Design & Computer Graphics*, Vol. 15, No. 6, pp. 711-715 **(2003)** June.

[16] Li Chang-Gang, Han Zheng-Zhi, and Zhang Hao-Ran, "Image Encryption Techniques: A Survey", *Journal of Computer Research and Development*, Vol. 39, No. 10, pp. 1317-1324 **(2002)** October.

[17] Scharinger J, "Fast Encryption of Image Data Using Chaotic Kolmogorov Flows", *Journal of Electronic Imaging*, Vol. 7, No. 2, pp.318-325 **(2009)**

[18] Behnia S, Akhshani A, Mahmodi H, et al, "A Novel Algorithm for Image Encryption Based on Mixture of Chaotic Maps", *Chaos Solutions & Fractals*, Vol. 35, No. 2, pp.408-419 **(2008)**

[19] Patidar V, Pareek NK, Sud KK, "A New Substitution-diffusion Based Image Cipher Using Chaotic Standard and Logistic Maps", *Communications in Nonlinear Science and Numerical Simulation*, Vol. 14, No. 7, pp.3056-3075 **(2009)**

[20] Wong KW, Kwok BSH, Yuen CH, "An Efficient Diffusion Approach for Chaos-based Image Encryption" *Chaos Solutions & Fractals*, Vol. 41, No. 5, pp.2652-2663 **(2009)**

Author

Mohammed Abbas Fadhil Al-Husainy received the M.Sc. and Ph.D. degrees in 1996 and 2002, respectively. From 1997 to 2002, he was a lecturer in the Department of Computer Science, Al-Hadba University of Mosul. Since 2002 he has been an assistant professor in the Departments: Computer Science and Multimedia Systems, Faculty of Science and Information Technology, Al-Zaytoonah University of Jordan. He lectures in the areas of microprocessors, data structures, algorithm design and analysis, digital design systems, operating systems, cryptography, computer organization, programming languages. His research interests are in the broad field of algorithm design, including multi-media data processing, scheduling algorithms, and cryptography algorithms.