# Image Encryption
# Using Permutation and Hill Cipher
# تشفير الصورة باستخدام التبادليات وتشفير هيل

**Ghassan Muslim Hassan** — **غسان مسلم حسن**
**Baghdad-Iraq** — **بغداد-العراق**
**Mustansiriya University** — **الجامعة المستنصرية**
**College of Sciences/Computer Department** — **كلية العلوم/قسم الحاسوب**
**E-mail: gmhalsaddi@yahoo.com**

**المستخلص**

**يستخدم التشفير لغرض نقل البيانات بصورة امنة في شبكات الحاسب. وتختلف خوارزميات التشفير باختلاف نوع البيانات (نص، صورة، صوت) لما لكل نوع من البيانات خواصه المختلفة. في هذا البحث تم اقتراح طريقة جديدة لتشفير الصور تتلخص باستخدام صورتين، احدهما تستخدم كمفتاح وتكون موجودة لدى المرسل والمستلم والاخرى هي الصورة المراد ارسالها يتم اضافة الصورتين باستخدام (XOR) بعدها يتم تجزئة الصورة الى أجزاء بحجم(n x n) جزء وتمرر هذه الاجزاء الى خوارزمية التشفير (Hill cipher) ويتم بعثرة هذه الاجزاء حسب جدول يتم توليدة.**

## Abstract

Encryption is used to securely transmit data in open networks. Each type of data has its own features; therefore different techniques should be used to protect confidential image data from unauthorized access. This paper, has been proposed new encryption algorithm using two different images, one is cover image which acts as key image which is shared by both sender and receiver and other is Informative image. As first step, XOR cover image with informative image to obtain resultant image. The resultant image is decomposed into (n x n) blocks which passed to the Hill Cipher algorithm to form encrypted blocks. The encrypted blocks are transformed into new locations using permutation table.

Keywords: Encryption, Hill cipher, permutation,

## 1. Introduction

The rapid growth of computer networks allowed large files, such as text, audio, and image, to be easily transmitted over the internet and it is important to protect the confidentiality of image data from unauthorized access [1]. Cryptography is the science of using mathematics to encrypt and decrypt data, and thus it provides a secure way to store sensitive information or transmit it across insecure networks such as the internet, so that it cannot be read by anyone except the intended recipient [2]. In general, conventional textual cryptography algorithms such as DES, Triple-DES, AES and RSA cannot be used to encrypt images directly. Images are different from texts in many aspects such as high correlation among pixels and high redundancy. Thus, a variety of new image encryption schemes have been proposed [3].

Although we may use the traditional encryption algorithms to encrypt images directly, it is not a good idea for two reasons. The **first** is the image size is often larger than text. Consequently, the traditional encryption algorithms need longer time to directly encrypt the image data, the **second**, is the decrypted text must be equal to the original text, but this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable [4].

## 2. Literature Survey:

Most of the algorithms specifically designed to encrypt digital images are proposed in the mid-1990s. There are two major groups of image encryption algorithms: (a) nonchaos selective methods and (b) Chaos-based selective or non-selective methods. Most of these algorithms are designed for a specific image format compressed or uncompressed, and some of them are even format compliant. There are methods that offer light encryption (degradation), while others offer strong form of encryption. Some of the algorithms are scalable and have different modes ranging from degradation to strong encryption [5].

Shujun Li et al. [6] have pointed out that all permutation only image ciphers were insecure against known/chosen plaintext attacks. In conclusion, they suggested that secret permutations have to be combined with other encryption techniques to design highly secured images. Mitra A et al.[2] have proposed a random combinational image encryption approach with bit, pixel and block permutations. Zhi-Hong Guan et al. [7] have presented a new image encryption scheme, in which shuffling the positions and changing the grey values of image pixels are combined to confuse the relationship between the cipher image and the plain image. Sinha A. and Singh K. [8] proposed an image encryption by using Fractional Fourier Transform (FRFT) and JigSaw Transform (JST) in image bit planes. Maniccam S.S. and Bourbakis N G. [5] proposed image and video encryption using SCAN patterns. The image encryption is performed by SCAN based permutation of pixels and a substitution rule which together form an iterated product cipher. Ozturk I. and Sogukpinar I. [9] proposed new schemes which add compression capability to the mirror-like image encryption MIE and Visual Cryptography VC algorithms to improve these algorithms. Maniccam S.S., Nikolaos G. and Bourbakis. [10] have presented a new methodology, which performs both lossless compression and encryption of binary and gray-scale images. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. Droogenbroeck M.V. and Benedett R. [11] have proposed two methods for the encryption of an image; selective encryption and multiple selective encryption. The proposed process divides the image into number of blocks with predefined maximum and minimum number of pixels (4 × 4) pixels blocks, resulting in a stronger encryption and a decreased correlation

## 3. Encryption algorithm

This paper, was implemented Hill Cipher and permutation techniques. The proposed algorithm uses two different, same size images, one is cover image which act as key image which is shared by both sender and receiver and the other is plain image as follows:

### 3.1 At the sender

**Step1:** XOR cover image and informative image (which are the same size) to obtained resultant image.

**Step2**: The resultant image from step 1 can be decomposed into blocks; each one contains a specific number of pixels (4 × 4) pixels blocks. Increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy [5,8].

**Step3:** The blocks are passed to the Hill Cipher algorithm to form encrypted blocks.

**Step4:** The encrypted blocks transformed into new locations using **permutation table**.

### 3.2 At the receiver

**Step 1**: The encrypted image after receiving by receiver transformed to new location by using **permutation table** .

**Step 2**: Apply Hill cipher to those new locations of encrypted image by using $K^{-1}$ (key inverse of Hill cipher), to obtain merged image.

**Step 3**: The merged image (XOR) with the same key image (which is shared by sender and receiver) to obtained informative image (plain image)

The detail process of encryption process is summarized in figure 1.

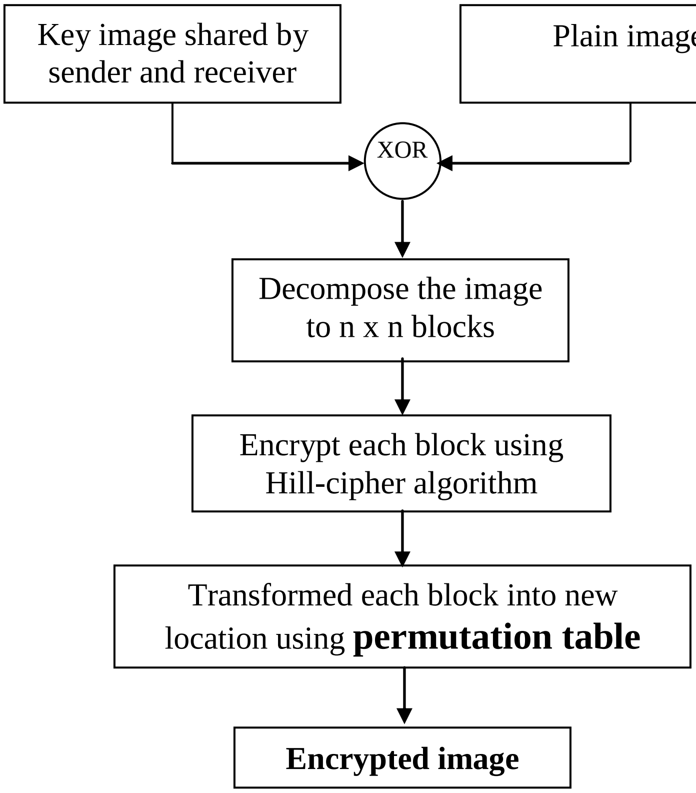
Key image shared by sender and receiver
Plain image
XOR
Decompose the image to n x n blocks
Encrypt each block using Hill-cipher algorithm
Transformed each block into new location using permutation table
Encrypted image

Fig. (1) Block diagram of the proposed algorithm

## 4. Hill Ciphering

The Hill cipher works on groups of letters in a somewhat different manner. The Hill cipher works by viewing a group of letters as a vector, and encryption is done by matrix multiplication [12]. Each letter is first encoded as a number. Often the simplest scheme is used: A = 0, B =1, ..., Z=25, but this is not an essential feature of the cipher. A block of *n* letters is then considered as a vector of n dimensions, and multiplied by an n × n matrix, modulo 26. The whole matrix is considered the cipher key, and should be random provided that the matrix is invertible (to ensure decryption is possible). A Hill cipher is another way of working out the equation of a matrix.[13]

If a message 'ACT' (for example), and the key below (or GYBNQKURP in letters):

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

Since 'A' is 0, 'C' is 2 and 'T' is 19, the message is the vector:

$$\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$$

Thus the enciphered vector is given by:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \pmod{26}$$

which corresponds to a cipher-text of 'POH', every letter has changed.[13]

## 5. Algorithm-Create-Permutation-Table

The encrypted image (plain image XOR with key) is based on the combination of encrypted block (Hill-cipher) followed by permutation process. In this case, combination of Hill-cipher followed by permutation process use the original image Fig.2(a) and Fig.2(b) to produce Fig.(c),(d) respectively. In this paper standard randomness measures was used to test the permutation complexity as followed ;

### 5.1 Statistical Tests for Randomness:

The blocks was transformed to binary form to get $\mathbf{s = s_0, s_1, s_2, \ldots, s_{n-1}}$ be a binary sequence of length n. This subsection presents four statistical tests that are commonly used for determining whether the binary sequence s possesses some specific characteristics that a truly random sequence would be likely to exhibit. If a sequence passes all four tests, there is no guarantee that it was indeed produced by a random bit generator.

- **Frequency test (mono-bit test)**

The purpose of this test is to determine whether the number of 0's and 1's in s are approximately the same, as would be expected for a random sequence. Let $n_0$ , $n_1$ denote the number of 0's and 1's in s, respectively. The statistic used is

$$X_1 = \frac{(n_0 - n_1)^2}{n} \qquad \text{eq.(1)}$$

- **Serial test (two-bit test)**

The purpose of this test is to determine whether the number of occurrences of 00, 01, 10, and 11 as subsequences of s are approximately the same, as would be expected for a random sequence. Let $n_0$, $n_1$ denote the number of 0's and 1's in s, respectively, and let $n_{00}$, $n_{01}$, $n_{10}$, $n_{11}$ denote the number of occurrences of 00, 01, 10, 11 in s, respectively. Note that

$n_{00}+n_{01}+n_{10}+n_{11}=(n-1)$ since the subsequences are allowed to overlap. The statistic used is

$$\begin{aligned} X_2 &= \frac{4}{n-1}\sum_{i=0}^{1}\sum_{j=0}^{1} n_{ij}^2 - \frac{2}{n}\sum_{i=0}^{1} n_i^2 + 1 \\ &= \frac{4}{n-1}\left(n_{00}^2 + n_{01}^2 + n_{10}^2 + n_{11}^2\right) - \frac{2}{n}\left(n_0^2 + n_1^2\right) + 1 \end{aligned} \qquad \text{eq.(2)}$$

- **Poker test**

Let m be a positive integer such that

$$\left\lfloor \frac{n}{m} \right\rfloor \geq 5 \cdot 2^m \text{, and let } k = \left\lfloor \frac{n}{m} \right\rfloor$$

Divide the sequence s into k non-overlapping parts each of length m, and let $n_i$ be the number of occurrences of the i$^{th}$ type of sequence of length m, $1 \leq i \leq 2^m$ . The poker test determines whether the sequences of length m each appear approximately the same number of times in s, as would be expected for a random sequence. The statistic used is

$$X_3 = \frac{2^m}{k}\left(\sum_{i=1}^{2^m} n_i^2\right) - k \qquad \text{eq. (3)}$$

- **Runs test**

The purpose of the runs test is to determine whether the number of runs (of either zeros or ones) of various lengths in the sequence s is as expected for a random sequence. The expected number of gaps (or blocks) of length i in a random sequence of length n is

$$e_i=(n-i+3)/2^{i+2}$$

Let k be equal to the largest integer i for which $e_i \geq 5$. Let $B_i$, $G_i$ be the number of blocks and gaps, respectively, of length i in s for each i, $1 \leq i \leq K$

The statistic used is

$$X_4 = \sum_{i=1}^{k} \frac{(B_i - e_i)^2}{e_i} + \sum_{i=1}^{k} \frac{(G_i - e_i)^2}{e_i} \qquad \text{eq. (4)}$$

**The main algorithm**

```
1: Load the plain Image
2: Input secret key
3: Get the Width and Height of the image
4.1: Lower Horizontal Number of Blocks = Integer (Image Width / 4)
4.2: Lower Vertical Number of Blocks = Integer (Image Height /4)
5: Number of Blocks = Horizontal Number of Blocks × Vertical Number of Blocks
6: Seed = | Hash value (Key) |
7: Counter of Good Keys = 0
8: For I = 0 to Number of  Blocks -1
    8.1: Get the New Location of Block .
    8.2: By Using all Tests (eq.(1), eq.(2), eq.(3), and eq.(4)) , the Good Key was Chosen.
    8.3: Save the Good Key  in a Table.
    8.4: Increase the Counter of Good Keys by One.
9: By Using Pseudo Random Generator, the Desired Key was Chosen From a Permutation
   Table
10: Set block  in its new Location
END PERFORM_PERMUTATION
Input: plain Image (BMP image file) and permutation table
Output: permuted Image.
```

The proposed combinational scheme along with individual permutations has been implemented in the **Matlab** with several test images.

## 6. Security analysis and test results

In this section, the performance of the proposed image encryption scheme is analyzed in detail. The discussion was made of security analysis of the proposed image encryption scheme including some important ones like statistical sensitivity, key sensitivity analysis, key space analysis etc. to prove the proposed cryptosystem is secure against the most common attacks.

### 6.1 Visual Testing

A number of images are encrypted by the proposed method, and visual test is performed. Two examples are shown in Fig. 2 (a) and Fig. 2 (b), where each image is in 24-bit color with 300x200 pixels. By comparing the original and the encrypted images in Fig. 2, there is no visual information observed in the encrypted image, and the encrypted images are visual indistinguishable even with a big difference in the color tone found in the original images.

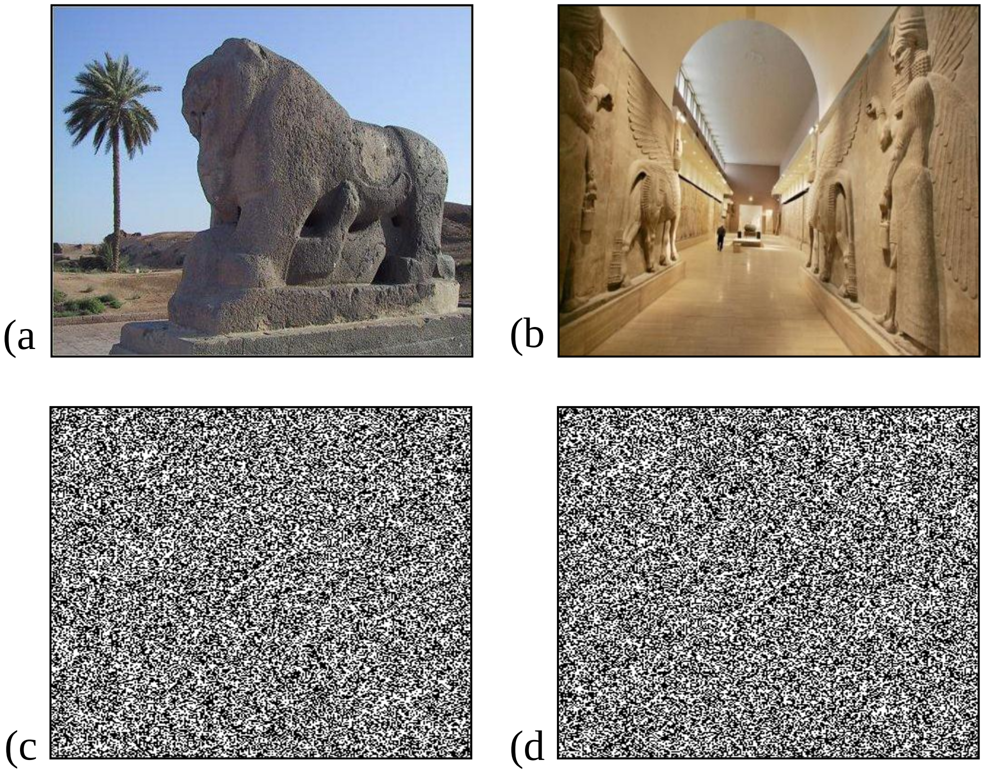

Fig. (2) Image (a) and (b) respectively, show the original images of Babylon lion and Iraqi museum. (c) and (d) respectively, show the encrypted images of the plain images shown in (a) and (b)

### 6.2 Histogram Analysis

To prevent the leakage of information to attackers, it is important to ensure that encrypted and original images do not have any statistical similarities. The histogram analysis clarifies that, how the pixel values of image are distributed. Fig. (3) shows histogram analysis on test image using the proposed algorithm.

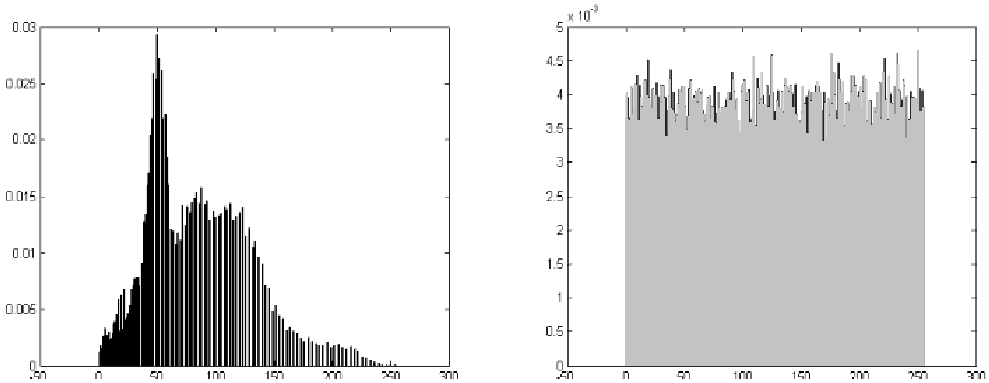

Figure 3. Histogram analysis:- shows the histograms of red channel of the plain image shown in Fig. 2 (a), and of red channel of the encrypted image shown in Fig. 2 (c). The histograms do not show any similarities.

## 7. Conclusion

Image data has visual information observed in each image. However, it is very important to disturb these information among image pixels to increase the security level of the encrypted images, if the encryption will done on each image. To make a secure image system, the proposed technique divides an image into blocks of n x n size and then perform double encryption process. In this paper the proposed algorithm uses two different images, one is cover image which act as key image which is shared by both sender and receiver and the other is plain image first we XOR the plain image and cover image and pass the resultant image to hill cipher algorithm then transformed the image using permutation table. Experimental results showed the histogram analysis of red channel for both plain and encrypted image. The histogram does not show any similarities for both images. From the results, it is observed that combined method achieved the advantages all individual permutation techniques.

## Reference

[1] W. Lee, T. Chen and C. Chieh Lee, "Improvement of an encryption scheme for binary images," *Pakistan Journal of* Information *and Technology*. Vol. 2, no. 2, 2003, pp. 191-200. http://www.ansinet.org.

[2] G. C. Kessler, "An Overview of Cryptography," published by Auerbach, 1998' (22 Desember 2007).

[3] K. Wang , Pei , Z. Liuhua ,S. Aiguo Song, H. Zhenya, "On the security of 3D Cat map based symmetric image encryption scheme," Elsevier, Physics Letters A, Vol. 343, Issue 6, 2005, pp. 432–439.

[4] S. Han, and S. Yang, "An Asymmetric Image Encryption Based on Matrix Transformat ion," e c t I transactions on computer and information technology vol . 1, no. 2 , 2010 .

[5] S.S. Maniccam, N.G. Bourbakis, "Image and video encryption using SCAN patterns," Journal of Pattern Recognition Society, vol. 37, no. 4, pp.725–737, 2004.

[6] 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: 2009, Vol. 2, 2002, pp. 708,711.

[7] G. Zhi-Hong, H. Fangjun, and G.Wenjie , "Chaos - based image encryption algorithm," Department of Electrical and computer Engineering, University of Waterloo, ON N2L 3G1, Canada. Published by: Elsevier, 2009, pp. 153-157.

[8] A. Sinha, K. Singh, "Image encrypt ion by using fractional Fourier trans form and Jigsaw transform in image bit planes," Source: optical engineering, spie-int society optical engineering, vol. 44, no. 5 , 2005, pp.15-18.

[9] I. Ozturk, and I.Sogukpinar, "Analysis and comparison of image encryption algorithm," International Journal of Information Technology, Vol. 1, no.2, pp. 64-67. http://www.waset.org.

[10] S . S . Manic c am. , G . Nikolaos , and Bourbakis, "Lossless image compression and encryption using SCAN," Journal of: Pattern Recognition, vol. 34, no. 6, 2001, pp.1229–1245.

[11] M. Van Droogenbroeck and R. Benedett, "Techniques for a selective encryption of uncompressed and compressed images," In ACIVS'02, Ghent, Belgium, Proceedings of Advanced Concepts for Intelligent Vision Systems, 2007.

[12] Scott Sutherland, "An Introduction to Cryptography", October 14, 2005

[13] Lester S. Hill, Concerning Certain Linear Transformation Apparatus of Cryptography, The American Mathematical Monthly Vol.38, 1931, pp.135–154.