International Journal of Sciences: Basic and Applied Research (IJSBAR)

ISSN 2307-4531
(Print & Online)

http://gssrr.org/index.php?journal=JournalOfBasicAndApplied

H.A.F Technique for Documents and Archaeologist Images Encryption

Hind Shaaban[a*], Ali Alramahi[b], Farah Sari[c]

[a,b,c] *Computer science Department , Kufa University, Iraq*

[a]*Hindrustum.shaaban@uokufa.edu.iq*

[b]*alia.alramahi@uokufa.edu.iq*

[c]*faraa.altaee@uokufa.edu.iq*

Abstract

The Encryption important Images like documents and archaeologist images area became extremely important now days , so that is why proposed new technique called H.A.F(Hind ,Ali and Farah) to encrypt image with complex steps to make it hard on hackers to hacked it , which need to reverse the block exchange then should be try to decrypt image by inverse math module use specific keys , these keys created using many probability with specific criteria . in this paper have twice keys with shifting blocks of images , in additional encryption method will apply on parts not the entire image . Experimental result and security analysis indicates the robustness and advantages of the new proposed algorithm. Technique is possible to reproduce the original image with no loss of information for the encryption and decryption process. It is fast and simple enough to be comparable to other recent methods, and it has passed all the security requirements and it is fast and secure to be used in very broad range of documents and archaeologist images encryption applications.

Keywords*:* Encryption images; Mathematics Module; Encryption algorithms; Encryption Decryption algorithm; Encryption Exchange blocks.

---

* Corresponding author.

1. Introduction

In some cases image applications require to satisfy their own needs like real time transmission and processing. One of the main goals that must be achieved during the transmission of information over the network is security. Cryptography is the technique that can be used for secure transmission of data. This technique will make the information to be transmitted into an unreadable form by encryption so that only authorized persons can correctly recover the information. The security of image can be achieved by various types of encryption schemes. Different chaos based and non-chaos based algorithms have been proposed. Among this the chaotic based methods are considered to be more promising. The chaotic image encryption can be developed by using properties of chaos including deterministic dynamics and unpredictable behavior [1].

Data Encryption is one of the widely used techniques for data protection. In Data Encryption, data is converted from its original to other form so that information cannot be accessed from the data without decrypting the data i.e the reverse process of encryption. The original data is usually referred as plain data and the converted form is called cipher data. Encryption can be defined as the art of converting data into coded form which can be decode by intended receiver only who poses knowledge about the decryption of the ciphered data. Encryption can be applied to text, image, and video for data protection [2].

Encryption of images is different from that of textual data, as images are intrinsically bulky and have high correlation among pixels and higher redundancy which is difficult to be handled by the traditional encryption schemes. Hence the DES, AES, IDEA, Blowfish, RC6 and RSA etc. do not suite for modern image transmission requirements [3].

Many researchers have tried to innovate better solutions for secured image transmission. In particular, application of chaos theory in multimedia encryption is one of the important research directions [4].

Image Encryption Using Affine Transform and XOR Operation , Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar and Partha Pratim Sarkar [9] introduced a new algorithm using affine transform and was based on shuffling the image pixels. It was two phase encryption decryption algorithm. Firstly using XOR operation they encrypted the resulting image and then using the affine transformation, the pixel values were redistributed to different locations with 4 bit keys. The transformed image then divided into 2 pixels x 2 pixels blocks and each block is encrypted using XOR operation by four 8-bit keys. The result proves that the correlation between pixel values was significantly decreased after the affine transform.

Image Encryption Using Block-Based Transformation Algorithm ,Mohammad Ali Bani Younes and Aman [8] introduce a block-based transformation algorithm based on the combination of image transformation and a well-known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, and using the transformation algorithm it was rearranged, and then the Blowfish algorithm is used for encrypting the transformed image their results showed that the correlation between image elements was significantly decreased. Their results also show that increasing the number of blocks by using smaller block sizes resulted in

a lower correlation and higher entropy.

The paper is organized as follows; Section 2 deals with **H.A.F(Hind ,Ali and Farah) method** , section3 the proposed method with results is introduced , in section4 Experimental Results, and the conclusion of this study is given in section 5.

2. H. A.F (Hind, Ali and Farah) technique

The proposed technique called H.A.F (Hind ,Ali and Farah) encryption method involves two stages (The encoding, decoding) images Model encryption method and the exchange of blocks. The encoding, decoding algorithms and the schemes are given in the following sections.

a. Algorithm for encoding

The Algorithm for encoding in H.A.F(Hind ,Ali and Farah) encryption method is:

1-Start

2- Input image in any size

3- Scaling of image in order to be balanced size (512 * 512)

4- Segmentation image into blocks of 8 * 8 so fragmentation of images to Block 64 and each one is a 64-element (8 * 8)

5- Switch blocks with some of them (the first block with the last block) and the block before the final with the second block, and so on.

6- Encrypted image bytes. Until step 4 there are no prominent effect on image , so that is why need to mathematical module which close to some extent affine algorithm which work on string or char only but with special keys became (H.A.F) algorithm and work on bytes .

C=a*p+3 mod 256 ……(1)

Where a is special coprime between a and 256, ideal value is 3 and p is byte to be encrypt.

This method needed to test set of values, without causes too much influence to image, until find suitable coprime value

7- The result kept in the same folder.

8- End.

b. Algorithm for decoding

The Algorithm for decoding in H.A.F(Hind ,Ali and Farah) encryption method is:

1- Start

2- Download Encrypted image

3- Split of Block to the image size 8 * 8

4- Appling of the equation in reverse

$P = c\text{-}3 * a^{-1} \bmod 256$ … (2)

Where a^{-1} is the inverse of the correct number and that no common denominator to account between him and the 256, which is applied in Euclid algorithm.

Where using java program to find GCD between two numbers

5- Remained image is not clear after the decryption

6- Re blocks to their places of origin reverse the work of the previous **(a)** Algorithm for decoding.

7- End.

(a)

(b)

(c)

Figure 1: (a) Sample Data Base for documents images. (b) Sample Data Base for archaeologist images. (c) image with its number Appling in paper.

3. Proposed method Database

The proposed method has been applied using any type for images with any format and size detailed experimental comparison of the above stated study has been presented. We have used image databases. Figure (1) shows sample database for astronomical images, which are used in this paper. Data base for paper contain 50 documents and archaeologist images applied.

Use of time complexity makes it easy to estimate the running time of H. A.F technique . Performing an accurate calculation of H. A.F technique operation time is a very accurate and sensitive process. Complexity can be viewed as the maximum number of primitive operations that a F technique may execute.

4. Experimental Results

In this section, the results are presented which are obtained by applying and evaluation H.A.F (Hind ,Ali and Farah) method.

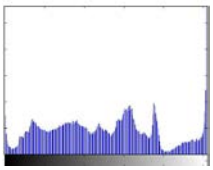
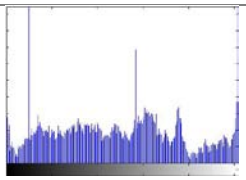
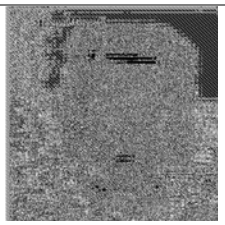
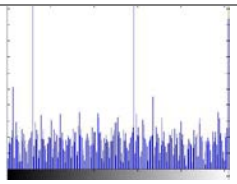
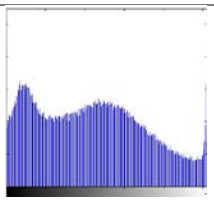
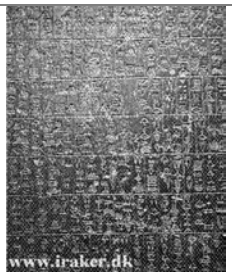
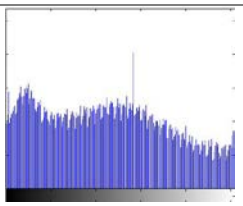
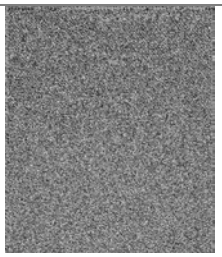
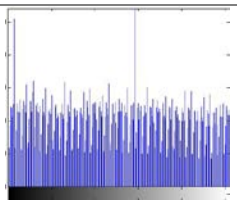
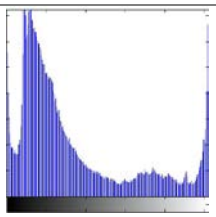
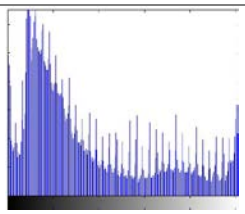
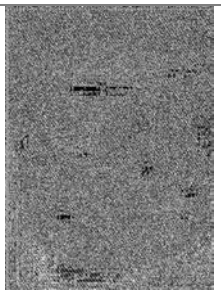
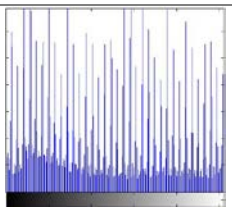
Histogram equalization is a spatial domain method that produces output image with uniform distribution of pixel intensity means that the histogram of the output image is flattened and extended systematically [5, 6].

And when we discriminate input image histogram with the processed image histogram we found that the gray

level intensities are stretched and depressed systematically. Consequently, we obtain that the histogram of the output image is systematically distributed. Yet, this accords the over enhancement in images above the actual gray scale span. During histogram equalization approach the mean brightness of the processed image is always the middle gray level without concerning of the input mean. This procedure is not very convenient to be enforced in consumer electronics, such as television, by the reason of that the method tends to introduce irrelevant visual deterioration like the concentration effect. The particular explanation for this issue is to conquer this weakness is by perpetuating the mean brightness of the input image indoor the output image [7].

Table (1) showed H.A.F(Hind ,Ali and Farah) technique encryption method for archaeologist images and Table (2) showed H.A.F(Hind ,Ali and Farah) technique encryption method for documents images.

Table 1: H.A.F (Hind, Ali and Farah) technique Encryption method for documents and archaeologist

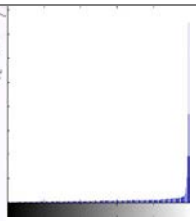
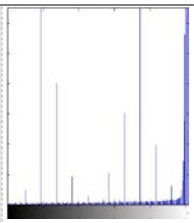
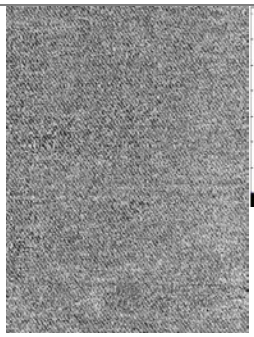
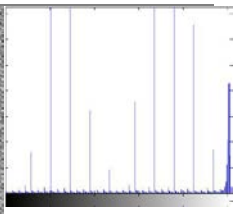
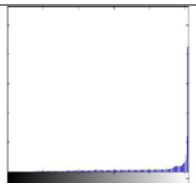
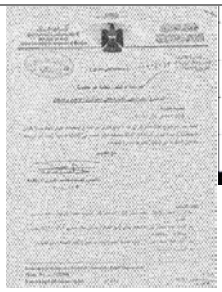
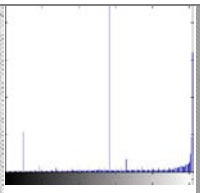
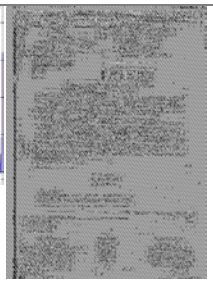
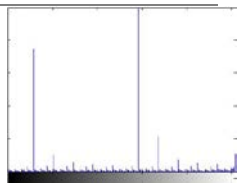
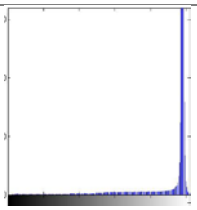
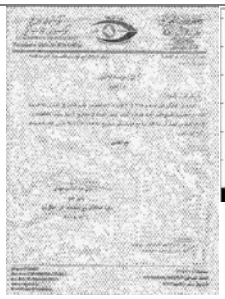
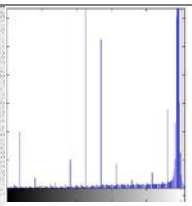
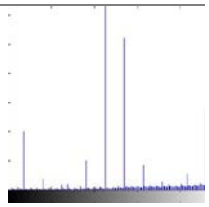
Original Image	**Image Hist**	**Encrypted Image (Diagonals)**	**D- Hist**	**Cipher Image (Blocks Shifting)**	**B-Hist**
					
					
					

As show in table (1) we note that, the encrypted image using chipper elements in upper and lower of main diagonal that the components of the histogram are cover a broad range of the gray scale and , further, that the distribution of pixels is not too far from uniform, with a lot of vertical lines being much higher than the others.

Intuitively, it is reasonable to conclude that an image, whose pixels tend to occupy the entire range of possible gray levels and, in addition, tend to be distributed uniformly, nevertheless the component of histogram of the encrypted image using scatter elements in the main diagonal are very close to the original image where the

histogram have few vertical lines . This means that there is little change compared with the original image.

Table 2: H.A.F (Hind, Ali and Farah) technique encryption method for documents and archaeologist

Original Image	Image Hist	Encrypted Image (Diagonals)	D- Hist	Cipher Image (Blocks Shifting)	B-Hist
					
					
					

As it is clear from the above figure , the encrypted image in the first method there are no high-impact image where it is suffering just a little noise and the ratio of read text or watch is high image and the human eye can distinguish the features of the image , from another side when apply second method which that makes the entire image damaged , no face no text can detected in encrypted image .

Table (3) Shows sample of execute time for each image by H.A.F(Hind ,Ali and Farah) technique encryption method for archaeologist images. Figure 3 exhibit the differences among images rely on executing time and size.

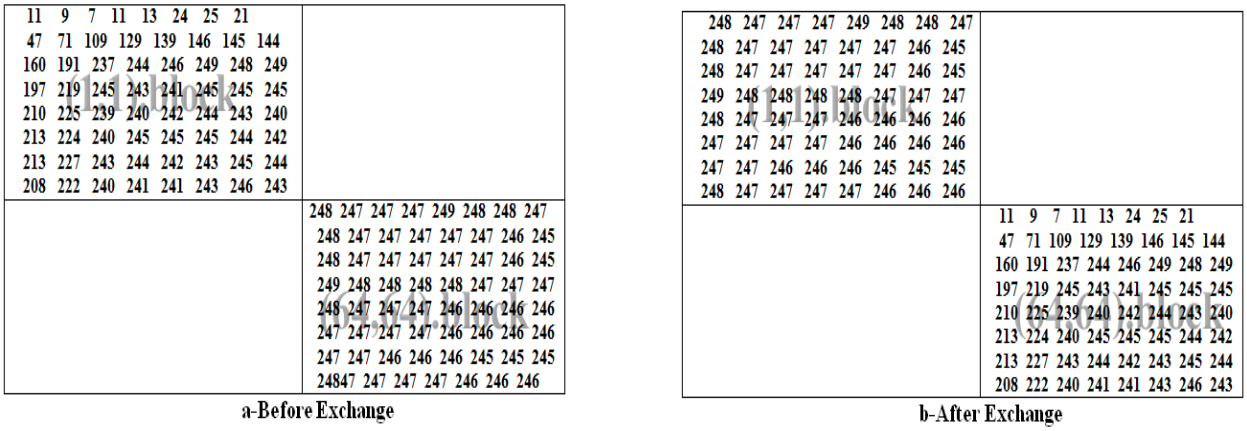


Figure 2: Sample of blocks Exchange values by H.A.F(Hind ,Ali and Farah) technique encryption method for archaeologist images.

Table 3: Sample of execute time for each image

Serial	Image	Size	Execute time
1	IM1	210 KB	6.709061 seconds.
2	IM2	256 KB	6.775735 seconds.
3	IM3	247 KB	7.185439 seconds.
4	Doc1	210 KB	6.698708 seconds.
5	Doc2	103 KB	6.633191 seconds.
6	Doc3	178 KB	6.658208 seconds.

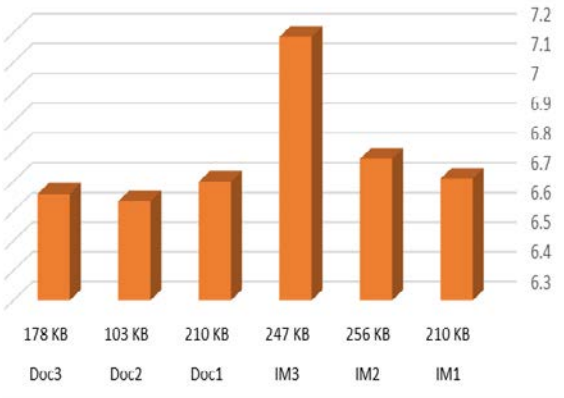


Figure 3: levels of executing time

Figure (4) Showed sample of blocks exchange shapes for image by H.A.F (Hind, Ali and Farah) technique encryption method for archaeologist images.

Figure 4: sample of image before block Exchange

Table (4) shows encryption images using main diagonal elements and secondary elements.

Encryption diameter main elements of the way of the image without switching places blocks

1. split the image into blocks of 8 * 8

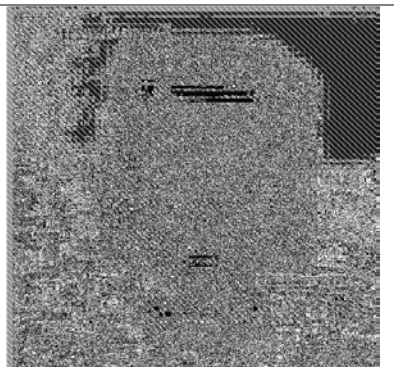
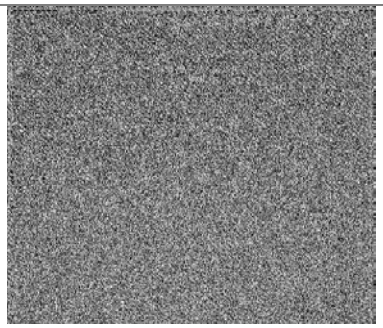
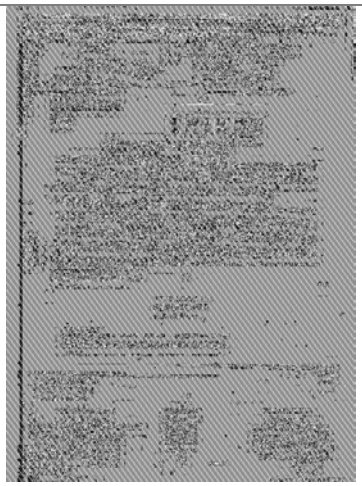
2. Encrypt the main elements in the country all the same Block Model Sports

3. Save Image

Decryption: unlike the model in each block (8 * 8)

The second way that any destruction of the image does not occur except for the white line and one diagonal image as well as in the secondary diameter.

Table 4: show encryption images using main diagonal elements and (upper - lower (main diagonal elements))

Original Image	Encryption Using (main diagonal elements)	Encryption Using Secondary elements
		
		
		

5. Conclusion

We conclude in this paper, encryption the main diagonal elements and without exchange blocks make slight effect on image , in the other hand the encryption upper and lower of main diagonal elements distort complete image . Exchange blocks with each other make the encryption process more complex, finally, we have select coprime key no one can expect and give good results

References

[1] Lini Abraham, Neenu Daniel," Secure Image Encryption Algorithms: A Review", International Journal of Scientific & Technology Research volume 2, issue 4, april 2013.

[2] V.V.Divya, S.K.Sudha and V.R.Resmy ," Simple and Secure Image Encryption", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 3, November 2012.

[3] K. Gupta and S. Silakari, “New Approach for fast color image encryption using chaotic map”, Journal of Information Security, vol. 2, no. 2, 2012.

[4] Kamlesh Gupta , Ranu Gupta , Rohit Agrawal and Saba Khan, "An Ethical Approach of Block Based Image Encryption Using Chaotic Map", International Journal of Security and Its Applications Vol.9, No.9 2015.

[5] R. C. Gonzalez and R. E. Woods, “Digital image processing,” Third Edition, Prentice Hall.

[6] A. K. Jain,“Fundamentals of Digital Image Processing Englewood Cliffs,” NJ: Prentice Hall, (1989).

[7] Ravindra Pal Singh and Manish Dixit, "Histogram Equalization: A Strong Technique for Image Enhancement", International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.8, No.8 ,2015.

[8] Wang Ying, Zheng DeLing, Ju Lei, et al., “The Spatial-Domain Encryption of Digital Images Based on High-Dimension Chaotic System”, *Proceeding of 2004 IEEE Conference on Cybernetics and Intelligent Systems, Singapore, pp. 1172-1176, December . 2004*

[9] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar Partha Pratim Sarkar, “Image Encryption Using Affine Transform and XOR Operation ”,*International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011).*