Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.7 No.1, 2018, pp.55-60

DOI: https://doi.org/10.51983/ajcst-2018.7.1.1829

Security Analysis of XOR Based Ciphered Image

P.Sharma[1], R. Shrivastava[2], V.K.Sarthi[3] and P. Bhatpahri[4]
[1]Department of Computer Science, [2]Department of Physics, [4]Department of Mechanical Engineering,
ICFAI University, Raipur, Chhattisgarh, India
[3]Department of Computer Science, Government Polytechnic College, Jagdalpur, Chhattisgarh, India
E-Mail: ravi_april78@yahoo.co.in

(Received 9 January 2018; Revised 26 January 2018; Accepted 10 February 2018; Available online 20 February 2018)

***Abstract* - In the present paper, we report security analysis of an effective method of scrambling i.e. XOR technique, which may be used as an important component in visual cryptography. Histogram of scrambled or encrypted images expressed that pixel values are distributed quite uniformly. This implies that nothing can be guessed about the original image using the encrypted image. For analyzing the complexity of encrypted images, information entropy, the correlation coefficient of adjacent pixels values were also calculated. Values of horizontal correlation, vertical correlation, and information entropy reflected that the complexity and randomness of pixel values are quite high for XOR cipher. Now a day's differential attack has been very common. Keeping the same in the mind, we have calculated Unified Average Changing Intensity (UACI) and the Number of Pixels Change Rate (NPCR), to exhibit the ability of encrypted image using XOR cipher to resist the differential attack. So we can say that XOR cipher is useful for secure transmission of an image.**

Keywords: **Cryptography, Matrix Algorithms**

I. INTRODUCTION

Now a day's digital images are used extensively. So, digital security is a very important aspect in today's research area. Using visual cryptography we can encrypt an important message in such an unintelligible format that no one can identify the original image from that format and sender can send the original image or message securely to the receiver, because unauthorized access to that original message may create disastrous security issue **[1].** Therefore it is important to convert the original message into random like cipher using a secret key, in such a way that the original message can be recovered again. Image scrambling is a very important aspect of visual cryptography technique. There are various methods of scrambling technique, such as block-based scrambling, pixel scrambling etc. Using these scrambling techniques many researchers had reported many algorithms to create cipher images. It is observed that using XOR cipher we can encrypt an original image into a scrambled image which cannot distinguish. In this scrambling process, we use a secret key. We use the same secret key to unscramble the encrypted image.

Digital revolution has changed the lifestyle of a common man. We are moving towards complete digitalization. Most importantly, transactions done using the digital system have saved our time and efforts. We use different forms of data such as audio voice and images to communicate from one end to another end. These data may carry plenty of important information especially for defense or any other ministry. Thus secure data transmission is a major area of concern for many researchers. Visual encryption is one of the techniques to hide the original message for unwanted persons. There are many techniques reported for visual encryption such as sub-image encryption method [2], Multilevel encoding [3], R prime shuffle technique [4], Block-based Scrambling [5], Random Grid technique [6], Arnold Cat map [7], etc. Our article deals with one of the methods to do the same. We have developed a new algorithm to scramble the image to provide security while sending the information to an individual. We performed various testing on the scrambled image to judge its capability to handle different types of attack. Result found expressed that, the method used for encryption can be very useful in this regards. Recently, various chaos-based permutation-diffusion architecture image encryption schemes have been proposed, which operate at the pixel-level [8-14].

II. ALGORITHM

A. Encryption Algorithm

1. Take an image of m x m dimension**.**
2. Select a secret key of the same dimension as per the image dimension such as [X_{11}, X_{12}, x_{13} ….x_{mm}]
3. Converted each element of image and key matrix in binary format
4. Apply bitwise XOR operation between an element of image matrix and the corresponding element of the key matrix
5. After step 4 we will get the encrypted image

B. Decryption Algorithm

1. Take the encrypted image.
2. Select the same secret key which was used to encrypt the image.
3. Converted each element of encrypted image and key matrix in binary format.
4. Apply bitwise XOR operation between an element of encrypted image matrix and the corresponding element of the key matrix.
5. After step 2 we will get the decrypted image which will be same as original one.

III. MATRIX REPRESENTATION OF ENCRYPTION TECHNIQUE

In this technique, we had used XOR Cipher to encrypt a greyscale image. The algorithm mentioned above is explained using 5 x 5 matrixes which are shown below in Figure 1. A sample key is used which is of 5 x 5 dimensions. In this process, we will perform XOR operation between every element($X_{11,}$ X_{12}, x_{13},…….x_{mm}) of image matrix to every element of the secret key matrix (Y_{11}, Y_{12}, Y_{13},……..Y_{mm}). Thereafter scrambling will be completed. For descrambling, we have to select the same secret key used to encrypt the image. Now for decryption, we have to perform XOR operation between every element of encrypted image matrix to every element of the secret key matrix. In this process, we are performing XOR operation with the same secret key. So the security is also increased.

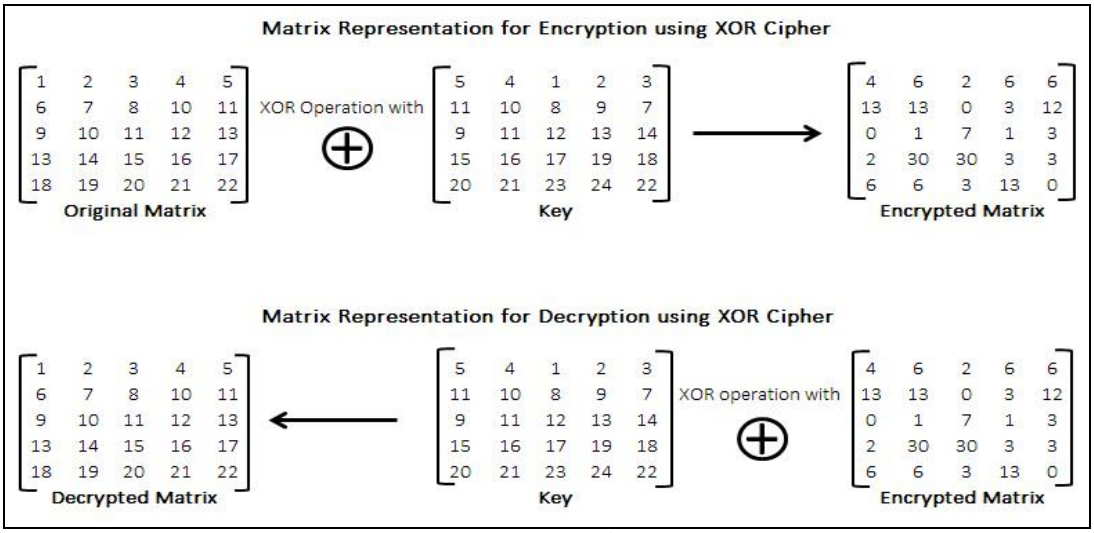

Fig. 1 Matrix representation of algorithm used

A. Scrambling of Image

Five images are used to analyze their suitability of scrambling technique. Original images along with their scrambled images are shown in Figure 2. It is analyzed from Figure 2 that using XOR operation we got complex scrambled images. To support the above statement we have done histogram, horizontal and vertical correlation.

B. Histogram Analysis

The histogram shows the distribution of pixel values in an image. Histogram of five original images with their encrypted images is shown in Figure 3. Histogram of an image shows an estimation that how the pixels are distributed. By seeing different histograms it can analyze that pixel value of encrypted images are uniformly distributed than original and decrypted images. If randomness of an encrypted image is high then it is very difficult to descramble that image. So by seeing histograms of Figure 3, it is clear that scrambled an image using XOR operation is very useful to secure a particular image.

C. Adjacent Pixel Values

The adjacent pixel values of a meaningful image always carry nearby values. So when we scramble an image we always expect those nearby pixel values to be scattered. More scattering of points of an encrypted image shows the better level of scrambling. We have calculated horizontal and vertical correlation to support the above statements in Table I. We have selected 1000 pairs of randomly selected horizontally and vertically adjacent pixels and then calculated horizontal and vertical correlation coefficient [15]. The graphical representation of horizontal and vertical correlation is shown in Figure 4 (a) and 4 (b).

By analyzing Table I it can be observed that original images have high correlation values for both horizontal and vertical correlation which is nearby the value 1, whereas in scrambled images have lower correlation values for both horizontal and vertical correlation. Minimum correlation indicates the better level of scrambling. So we can conclude that by using XOR operation we can encrypt an image which is next to impossible to decrypt.

D. Information Entropy Analysis

Entropy is a process of measure randomness of pixels in an image. If the random distribution of pixel is low then we can say that the image is meaningful. But if the random distribution of an image is high then we can say that the image is less meaningful. We have calculated randomness of different original images and their cipher images. The information entropy can be calculated by using the following formula [16]

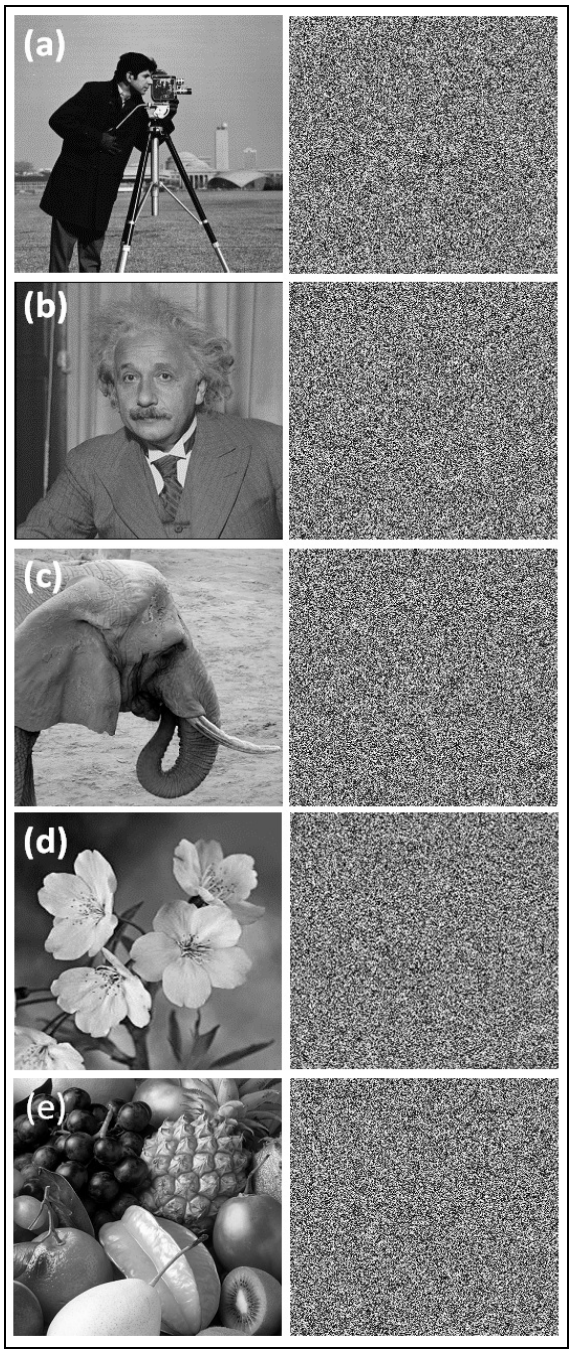

Fig. 2 Original and Encrypted images of (a) Cameraman.jpg (b) Einstein.jpg (c) Elephant.jpg (d) Flower.jpg (e) Fruit.jpg

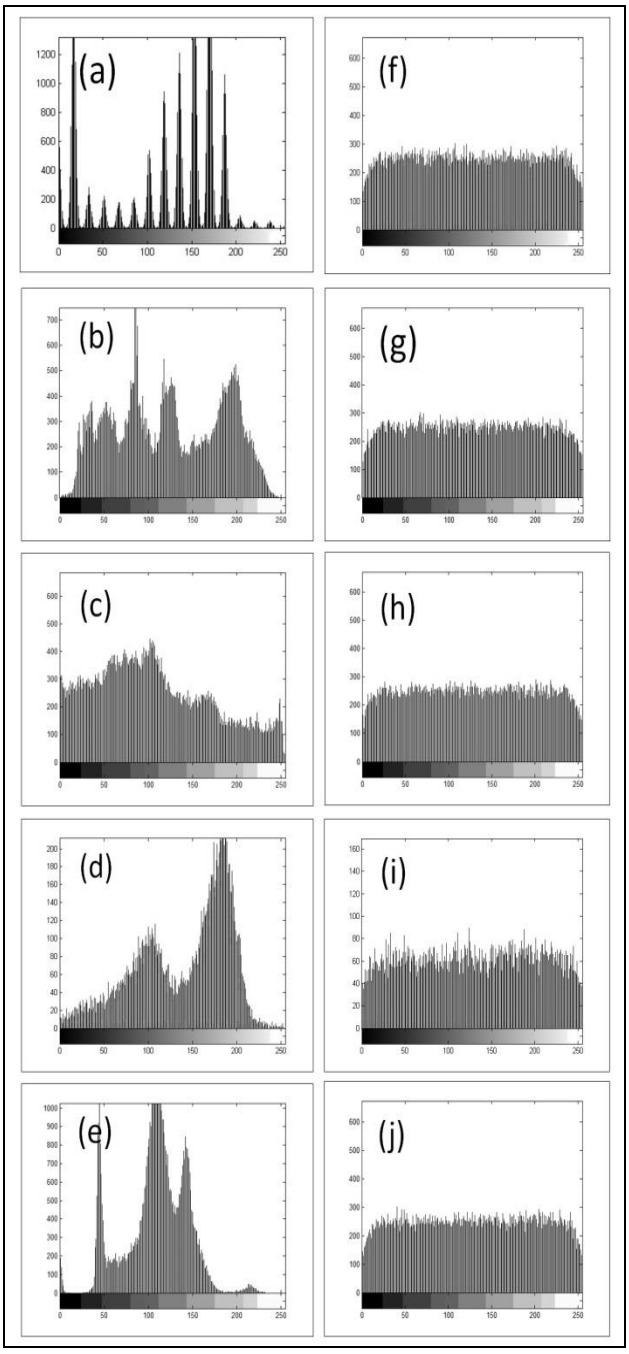

Fig. 3 Histogram of Original and Encrypted images of (a) Cameraman.jpg (b) Einstein.jpg (c) Elephant.jpg (d) Flower.jpg (e) Fruit.jpg

TABLE I CORRELATION COEFFICIENT OF DIFFERENT IMAGES

Correlation Type	Images				
	Cameraman	**Einstein**	**Elephant**	**Flower**	**Fruit**
Scrambled Horizontal Correlation	-0.000875596	-0.047685284	-0.056015606	0.004210166	0.017469877
Scrambled Vertical Correlation	-0.010266216	-0.032270861	0.004008881	-0.035814629	0.004323797
Original Horizontal Correlation	0.921535794	0.922625171	0.956745302	0.958615321	0.955184281
Original Vertical Correlation	0.914560952	0.934368277	0.954380702	0.951956276	0.952037232

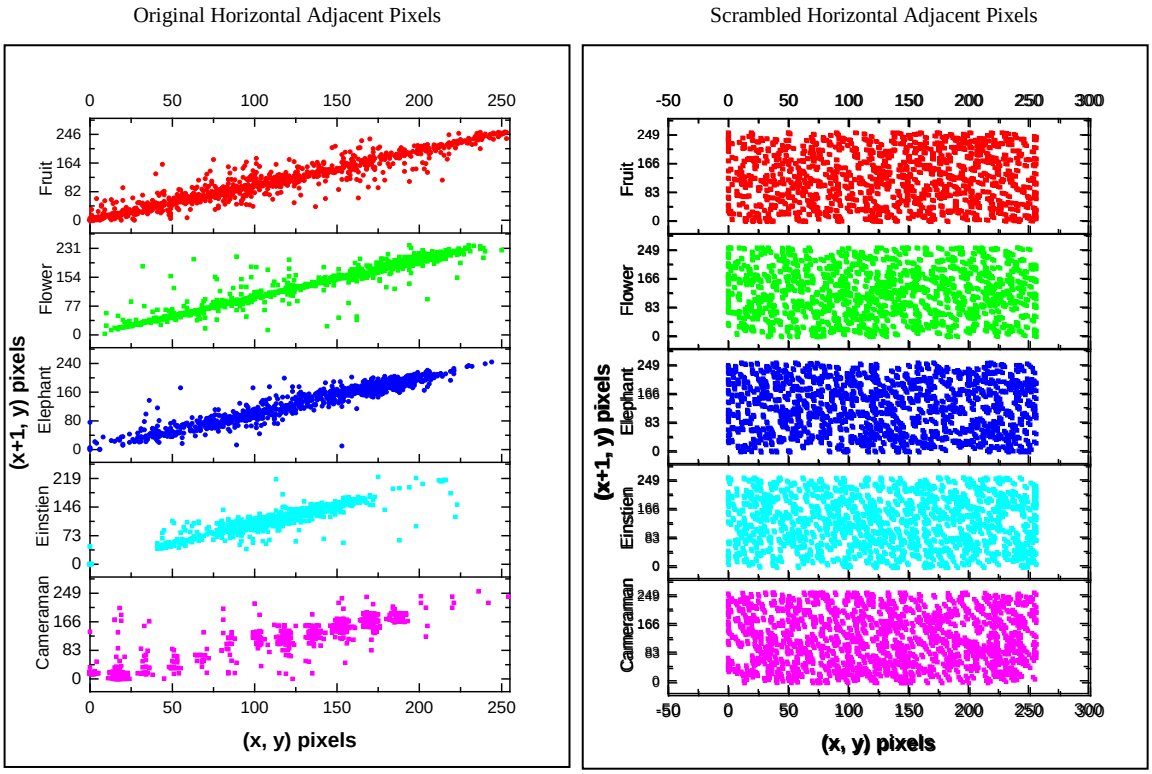

Fig. 4 horizontal correlations of original and encrypted images

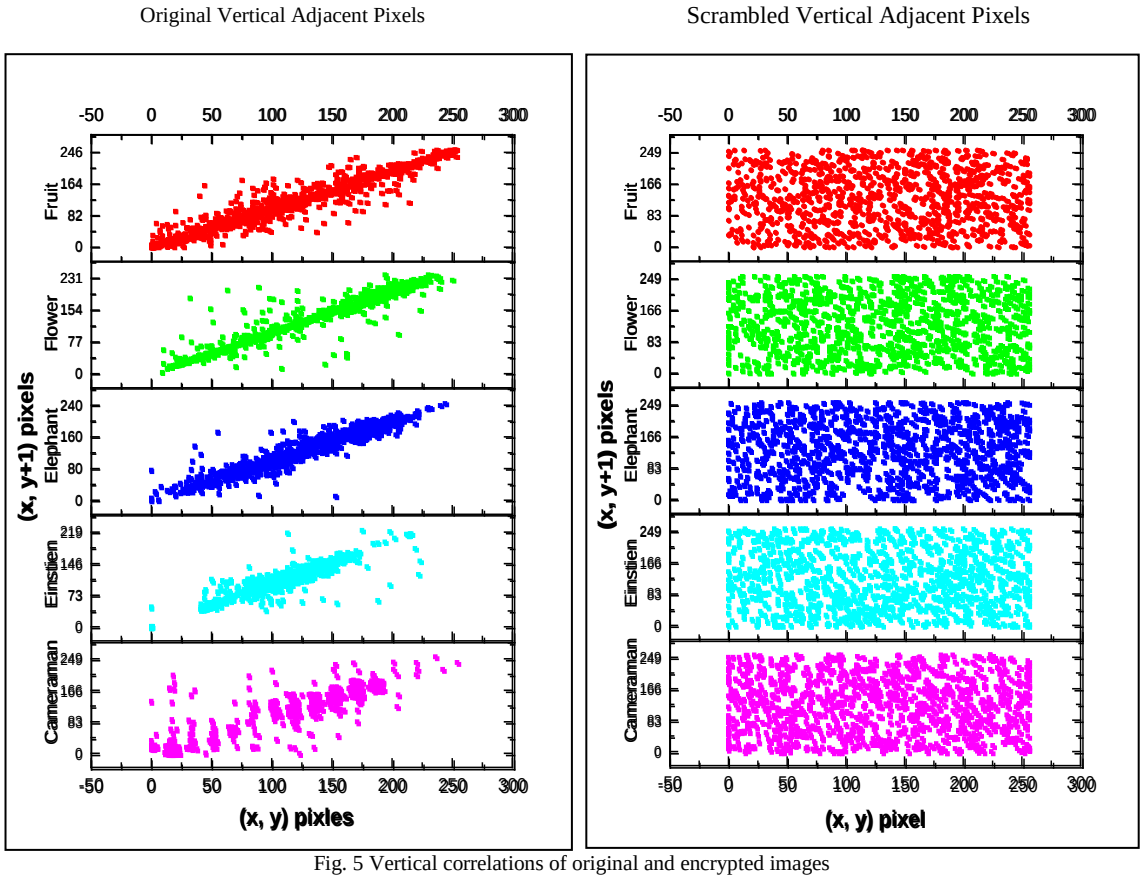

Fig. 5 Vertical correlations of original and encrypted images

E. Differential attack analysis

$$H(s) = \sum_{i=0}^{2^N-1} p(S_i) log_2 \frac{1}{p(S_i)} \ldots\ldots\ldots\ldots (1)$$

TABLE II INFORMATION ENTROPY

Original Image	Entropy Value	
	Original	Encoded
Cameraman	6.4373	7.9541
Einstein	6.8938	7.9528
Elephant	7.4715	7.9579
Flower	7.6931	7.9545
Fruit	7.8905	7.9561

In the above formula $p(S_i)$ denotes the probability of symbol S_i. When a source producing 2L symbols, the entropy should be L. Take 256- greyscale image for an instance, the entropy of the image should be nearby 8. The entropies of the original image and ciphered images are shown in Table II. According to entropy analysis done in Table II, we can see that the entropy value for the original images is less than the entropy values of ciphered images so by this point we can conclude that the ciphered images are secure.

The differential attack, as a type of chosen-plaintext attack, investigates how the difference between plain-images may affect the corresponding cipher-images in an encryption scheme. It traces the differences and tries to find the connections between plain-images and cipher-images [16-19]. The number of pixel change rate (NPCR) and Uniform average change intensity (UACI). Commonly, the Unified Average Changing Intensity (UACI) and the Number of Pixels Change Rate (NPCR) and can be used to define as the ability to resist the differential attack. Minor changes in the plain image should create substantially different cipher-images in order to provide high security. Adding this feature makes the system invulnerable to differential attacks. In order to test the effect of one – bit change on the plain image, two common measures are used, namely number of pixel change rate (NPCR) and unified average changing intensity (UACI). [16-19].

Their definitions are as follows:

$$NPCR = \sum_{i,j} \frac{d(i,j)}{h \times w} \quad (2)$$

$$d(i,j) = \begin{cases} 1 & c_1(i,j) \neq c_2(i,j) \\ 0 & otherwise \end{cases} \quad (3)$$

$$UACI = \frac{1}{h \times w} \sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255} \quad (4)$$

Here, 'h' and 'w' are the height and width of the image, respectively. C_1 (i, j) and C_2 (i, j) are the corresponding pixels of two images. If C_1 (i, j) = C_2 (i, j), then D (i, j) = 0, otherwise D (i, j) = 1. The ideal values of UACI and NCPR are 0.3346 and 0.9961, respectively.

The results of NPCR and UACI values are shown in Table III. It can be observed that the values of NPCR for different images range in 0.99477 to 0.99640 which is close to 0.9961 (ideal value) and UACI ranges in 0.29075 to 0.34359 which is again close to 0.3346 (ideal value). These results are indicative that the difference in the single bit of the plain image can diffuse to the entire cipher image, and we may conclude that the algorithm is good enough for resisting various differential attacks.

TABLE III NPCR & UACI VALUES

Image	NPCR Value	UACI Value
Cameraman.jpg	0.99637	0.34359
Einstein.jpg	0.99539	0.33836
Elephant.jpg	0.99504	0.32489
Fruit.jpg	0.99477	0.29075
Flower.jpg	0.99640	0.32131

IV. CONCLUSION

In this paper, we found that XOR cipher is an important tool to encrypt an image. When, we use XOR cipher to encrypt an image then the randomness of pixels of an original image increase. If randomness is more, we can say that the image is more secure. By analyzing histogram, horizontal and vertical correlation, information entropy it can be concluded that after scramble different images the randomness increases in their ciphered images, it means the ciphered images are more secure that it is not possible to decrypt.

The security keys which are used to encrypt and decrypt the original images are same. In this process to encrypt an image XOR operation is performed between original image and security key. Then to decrypt the image again XOR operation is performed between encrypted image and Security key. So decryption using security key is totally dependent on the result after encryption. So we can conclude that this process increases security of an image.

Informational entropies of encrypted images were found more than 7.9, which is an indication of large randomness. The values of correlation between horizontal pixels of encrypted images were very close to zero, which expressed that there are very small relationships between the nearby

pixel values. This implies that the encrypted images are of high complexity. Calculated UACI and NCPR values were closed to 0.3346 and 0.9961. This ensures the existence of capability of encrypted images to resist the differential attacks.

REFERENCES

[1] P. Sharma, D. Mishra, V.K. Sarthi, P. Bhatpahri and R. Shrivastava, "Visual Encryption Using Bit Shift Technique", *International Journal of Scientific Research in Computer Science and Engineering*, Vol. 5, No. 3, pp. 57-61, June 2017.

[2] XY Wang, YQ Zhang and LT Liu, "An enhanced sub-image encryption method", *Optics and Laser in Engineering*, Vol. 86, pp. 248-254, November 2016

[3] CC Lee, HH Chen, HT Liu, GW Chen and CS Tsai, "A new visual cryptography with multi-level encoding", *Journal of Visual Languages and Computing*, Vol. 2,No. 3, pp. 243-250, June 2016.

[4] HB Kekre, T Sarode and P. Halarnkar, "Image Scrambling using R-Prime Shuffle", *International Journal of Advanced Research in Electrical Electronics and Instrumentation Engineering*, Vol. 2, No. 8, pp. 4070 – 4076, August 2013.

[5] Z. Hua and Y. Zhou, "Design of image cipher using block-based scrambling and image filtering", *Information Sciences*, Vol. 396, pp. 97-113, August 2017.

[6] T Guo, F Liu and C. Wu, "k out of k extended visual cryptography scheme by random grids", *Signal Processing*, Vol. 94, pp. 90-101, January 2014.

[7] A. Soleymani, M. J. Nordin and E. Sundarajan, "A Chaotic Cryptosystem for Images Based on Henon and Arnold Cat Map", *The Scientific World Journal*, 2014. DOI:-http://dx.doi.org/10.1155/2014/536930.

[8] X.Y. Wang, F. Chen and T. Wang, "A new compound mode of confusion and diffusion for block encryption of image based on chaos", *Communications in Nonlinear Science and Numerical Simulation*, Vol. 15,No. 9, pp. 2479-2485, September 2010.

[9] L. Sui and B. Gao, "Single-channel color image encryption based on iterative fractional Fourier transform and chaos", *Optics & Laser Technology*, Vol. 48, pp. 117-127, June 2013.

[10] H. Li, Y. Wang, H. Yan, L. Li, Q. Li and X. Zhao, "Double-image encryption by using chaos-based local pixel scrambling technique and gyrator transform", *Optics and Lasers in Engineering*, Vol. 51, No. 12, pp. 1327-1331, 2013.

[11] A. Kanso, M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map", *Communications in Nonlinear Science and Numerical Simulation*, Vol. 17, No. 7, pp. 2943-2959, July 2012.

[12] C.Y. Song, Y.L. Qiao and X.Z. Zhang, "An image encryption scheme based on new spatiotemporal chaos", *Optik*, Vol. 124, No.18, pp. 3329-3334, September 2012.

[13] N. Singh and A. Sinha, "Optical image encryption using improper Hartley transforms and chaos", *Optik*, Vol. 121, No. 10, pp. 918-925, June 2010.

[14] A. Akhshani, S. Behnia, A. Akhavan, H.A. Hassan and Z. Hassan, "A novel scheme for image encryption based on 2D piecewise chaotic maps", *Optics Communications*, Vol. 283, No. 17, 3259-3266, September 2010.

[15] X. Y. Wang, Y.Q Zhang, and L.T. Liu, "An enhanced sub-image encryption method", *Optics and Laser in Engineering*, Vol. 86, pp. 248-254, November 2016.

[16] B. Stoyanov, and K. Kordov, "Image Encryption Using Chebyshev Map and Rotation Equation", *Entropy*, Vol. 17, pp. 2117-2139, April 2015.

[17] X. Tong, Y. Liu, M. Zhang, H. Xu and Z. Wang, "An Image Encryption Scheme Based on Hyperchaotic Rabinovich and Exponential Chaos Maps", *Entropy*, Vol. 17, pp. 181-196, January 2015.

[18] Yue Wu, Student Member, IEEE, Joseph P. Noonan, Cyber Journals: Multidisciplinary *Journals in Science and Technology*, *Journal of Selected Areas in Telecommunications (JSAT)*, April Edition, 2011

[19] https://en.wikipedia.org/wiki/Differential_cryptanalysis, accessed on 16 June 2017.