Asian Journal of Computer Science and Technology
ISSN: 2249-0701 Vol.7 No.1, 2018, pp. 40-45

Visual Encryption Using Multilevel Scrambling Followed by Affine Encryption Technique

Piyali Sharma[1], Pramay Bhatpahri[2], Ravi Kiran Patnaik[3] and Ravi Shrivastava[4]
[1&3]Department of Computer Science, [2]Department of Mechanical Engineering, [4]Department of Physics,
ICFAI University, Raipur, Chhattisgarh, India
E-Mail: ravishrivastava95@gmail.com

Abstract **- In the present paper, we report an effective method of multilevel scrambling followed by affine encryption, which may be used as one of the useful tools in visual cryptography. A sample image is scrambled for six times using a specific algorithm. Toner distributions of scrambled images were studied using their histograms. The results of histogram expressed that the effectiveness of scrambling increased with its increasing stages and it becomes almost ideal when the image after affine encryption is taken. In order to judge the complexity level of scrambling, horizontal & vertical correlation of adjacent pixels and Information Entropy of different scrambled images were also calculated. Values of horizontal & vertical correlation and information entropy reflected that the complexity and randomness of pixels increase with increasing stages of scrambling. It also indicated that the randomness doesn't change much after the fifth stage of scrambling and affine encryption enhanced the level of security by a large extent.**

Keywords: **Cryptography, Matrix algorithms, Scrambling, Horizontal Correlation, Vertical Correlation**

I. INTRODUCTION

In the era of digitalization, internet is used quite a lot by the people for sending and receiving information. It is really a tough task to protect our data, which is to be sent and to keep the important information in the safe hands. Text ciphers are comparatively easier to decrypt in comparison to image ciphers as the complexity level is quite higher in visual cryptography (VC). For this reason, Visual cryptography is replacing text cryptography. An encryption technique can be evaluated by level of security, precision in reconstruction, complexity of computation, storage requirement. In recent past years, the importance of image security has been enhanced rapidly. This is because; many researchers are working towards developing different algorithms with aim to provide high security [1-2]. In addition to the basic capability of sharing secrets, some other VC-based techniques including image encryption [3], visual authentication [4], digital watermarking [5], to name a few, are also developed to enrich the applications of VC. We have tried a multilevel scrambling algorithm to get the encrypted image. It was observed that, the randomness of the pixels increases with increasing number of stages of scrambling till its fourth stage than the result looked stagnant. We have also used different keys for scrambling and unscrambling of images. The key used for scrambling is the key of sender's choice and the unlock key or key for unscrambling the images can be retrieved using the key used in scrambling process. The histogram and adjacent pixel correlation curves of these scrambled images suggested that the scrambling was good but not good enough as far as its security issues are concerned. Keeping this in mind, we decided to go for chaos-based permutation diffusion technique. Recently, a number of chaos-based permutation–diffusion architecture image encryption schemes have been proposed. Most of them operate at the pixel-level and based on ordinary chaos. We used Affine Ciphering technique to alter each pixels of the image, which we had got after sixth stage of circular shifting. The result after applying affine cipher technique expressed quite satisfactory results.In this paper, we mainly propose an encryption scheme with circular shift operation on image matrix using a key matrix of dimension 1x n, followed by a diffusion process using the affine cipher, which enhances the security of circular shift encryption.

II. ALGORITHM

A. Encryption algorithm

1. Take any greyscale image of m x m dimension.
2. Select a secret key of dimension of 1 x m dimension such as [x1, x2, x3,……..xm]
3. Shift different columns of the image matrix by the respective numbers, corresponding to different columns of a secret key.
4. Step 3 gives first stag scrambled image. Transpose first scrambled image. (Note:- to interchange the column and row position)
5. Repeat step 3 on the transposed image of the first scrambled image. We will get the Second stage Scrambled image. We may go for repeating the process 3-5 using the image got in step 5 for getting multiple stages scrambled images.

B. Decryption algorithm

1. Take the encrypted image.
2. If all elements of the key used for encryption are less than or equal to m then select the secret key of dimension 1 x m, with the value of the elements [m-x1, m-x2, m-x3,……..m-xm].
3. If the values of elements are greater than elements of encryption key then select the secret key of 1 x m, with the values of the elements, [y1,y2…….yn] considering

the following:- [n1m+y1, n2m+y2, n3m+y2, n4m+y3…….nm+yn], where n1, n2,……nn, are integers and values of y1, y2…. Yn are less than m.

4. Shift the columns of the transposed encrypted image using keys generated using step 3. This step gives first scrambled image.
5. By circular shifting first scrambled image using the key mentioned in step 3, we get decrypted image.
6. If the scrambling is done for four stages, step 2-5 is required to be repeated for getting the final decrypted image.

III. MATRIX REPRESENTATION OF ENCRYPTION TECHNIQUE

In this method, the multilevel scrambling technique is used. The entire above mentioned algorithm is explained using a sample of 8 x 8 matrix, which is shown in Figure 1. A sample key [1 2 3 4 5 6 7 8] is used to express the process of scrambling. We may choose any random key matrix of the order of 1 x 8. We can apply the same key to the transpose of first stage scrambled image. This key can be used 'n' number of times for scrambling process for increasing the level of scrambling. For the process of descrambling, we require generating a new key, which will be generated using the key used in the scrambling process. The detailed process of generating the new key is illustrated in decryption algorithm. In this process, we are using separate keys for encryption and decryption process. This increases the security of encryption. Steps 1, 2, & 3 belong to encryption and Steps 4, 5, & 6 belong to decryption process.

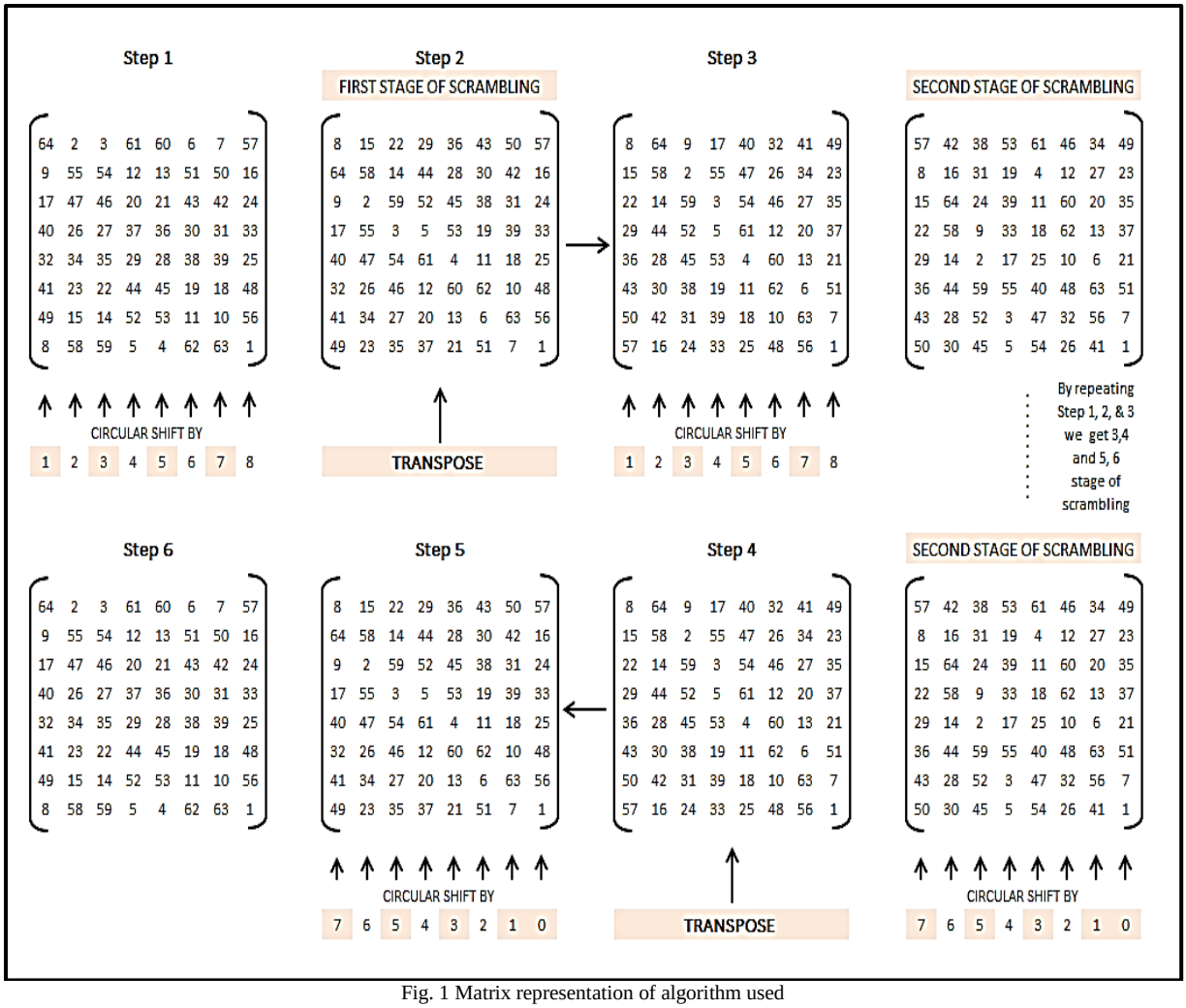

Fig. 1 Matrix representation of algorithm used

IV. SCRAMBLING OF IMAGE

An image, flower.jpg is used for analyzing the suitability of scrambling technique used. The original image along with different scrambled images is shown in Figure 2. Figures show that complexity of images is increasing with increasing level of scrambling. It can easily be observed that image found after the fifth level of scrambling is most complex amongst all other images. We have done histogram and horizontal correlation analysis in support of the above-mentioned statement.

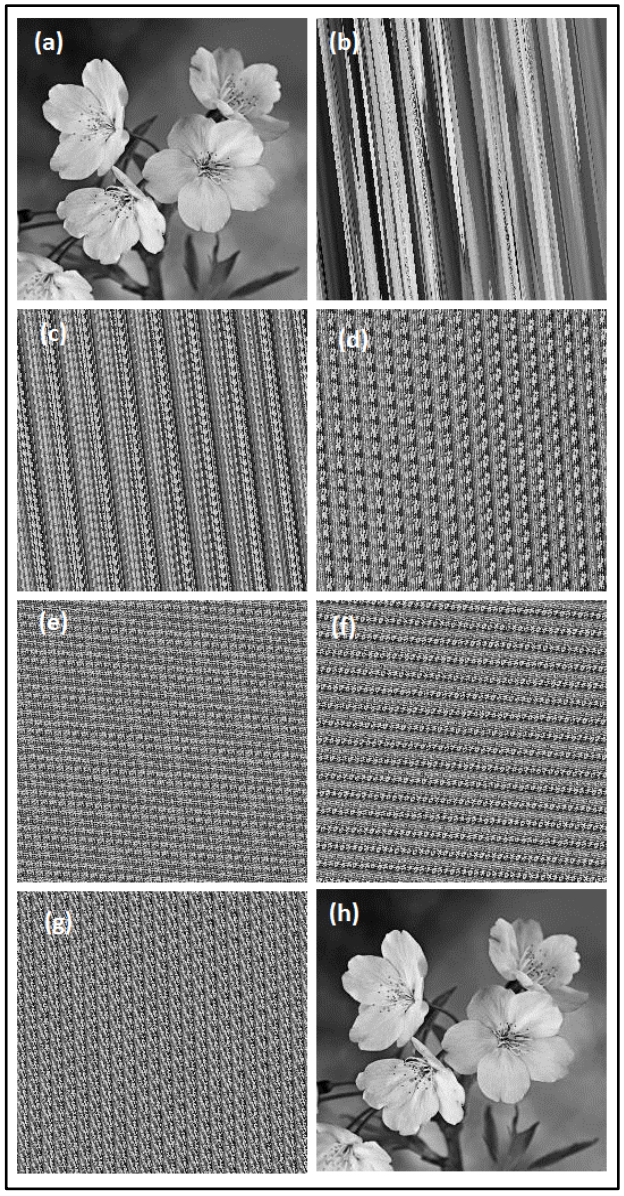

Fig. 2 **(**a) Original Image (b) First Stage Scrambled (c) Second Stage Scrambled (d) Third Stage Scrambled (e) Fourth Stage Scrambled (f) Fifth Stage Scrambled (g) Sixth Stage Scrambled (h) Decrypted image

V. HISTOGRAM ANALYSIS

The image histogram is a graphical representation of toner distribution of a digital image. Histogram of an image gives us an estimation that how the pixels are distributed by number at each level. Histogram of "flower.jpg" Gy-Scale image with the histogram of different cipher images are shown in [7-10] Figure 4. It can easily be predicted that pixels of different values are distributed uniformly in comparison to original image and uniformity is highest for fifth and sixth stage scrambled image. This shows that the randomness is high in cipher image and it is difficult to descramble.

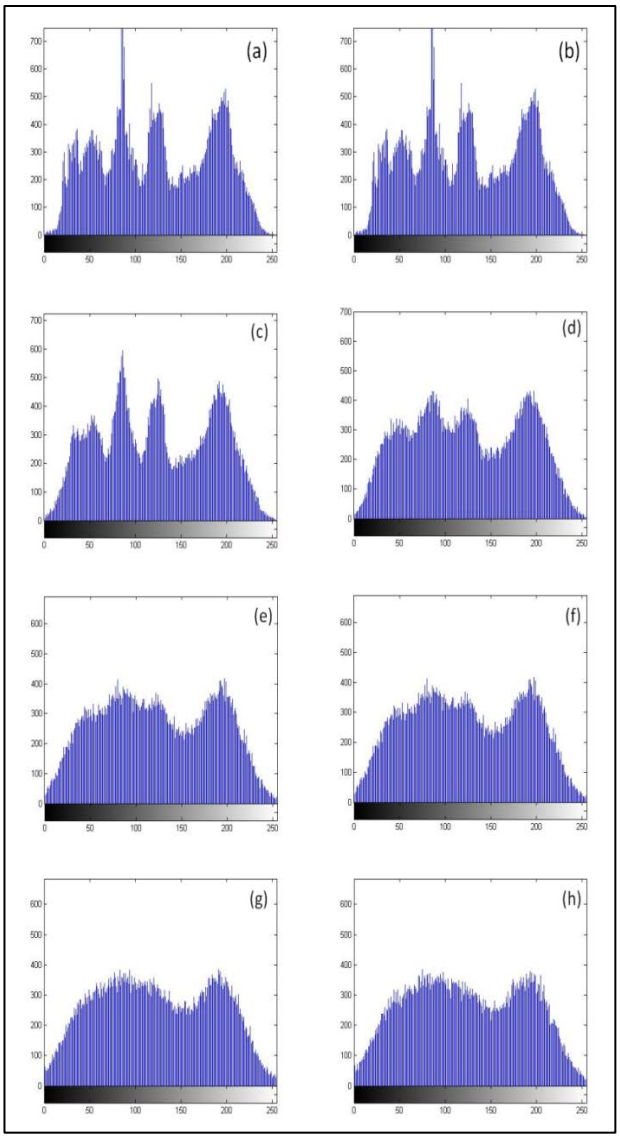

Fig. 3 Histogram of (a) Original Image (b) Decrypted image (c) First Stage Scrambled (d) Second Stage Scrambled (e) Third Stage Scrambled (f) Fourth Stage Scrambled (g) Fifth Stage Scrambled (h) Sixth Stage Scrambled

VI. ADJACENT PIXEL VALUES

If an image is meaningful, it should have nearby values between the adjacent pixels. When we start scrambling, we expect those pixel values to be scattered. More scattering of the points expresses the better level of scrambling. We also have calculated the horizontal correlation between pixel values. We have selected 1000 pairs of randomly selected horizontally adjacent pixels and then calculated correlation coefficient [6]. The graphical representation of the horizontal correlation between adjacent pixel values for different images is shown in Figure 5.

Correlation coefficients for original and different stages scrambled images are shown Table 1. It can be observed from the table that the correlation between the pixel values of the original image is quite high and close to 1. When we

scrambled the images it goes on decreasing and its minimum absolute value is found in the sixth stage of scrambling. So we may conclude that pixel correlation in ciphered images is lower.

TABLE I CORRELATION COEFFICIENT AT DIFFERENT STAGES OF SCRAMBLING FOR FLOWER.JPG

Original Image	Correlation at Different stages of Scrambling					
	First Stage	Second Stage	Third Stage	Fourth Stage	Fifth Stage	Sixth Stage
0.9566	0.7054	0.0158	-0.0453	0.1862	0.3342	0.0151

VII. INFORMATION ENTROPY ANALYSIS

Entropy in Mechanical Engineering is the measure of randomness of the uncertainty of any state. Similarily in the case of Image processing, it expresses the degree of random distribution of pixel values in any of the image. If the randomness is more, we may conclude that the image is less meaningful. We have calculated the information entropy of original as well as ciphered images. The randomness is calculated using following formula [6]

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

TABLE II INFORMATION ENTROPY FOR FLOWER.JPG

Original Image	Information Entropy					
	First Stage	Second Stage	Third Stage	Fourth Stage	Fifth Stage	Sixth Stage
7.6931	7.753	7.8095	7.8479	7.8494	7.8713	7.8712

Where p (S_i) denotes the probability of symbol S_i. When a source producing 2L symbols, the entropy should be L. Take 128- 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 image is less than the entropy values of ciphered images. We can also see that entropy value is increasing from first ciphered image to second ciphered image (i.e., randomness is increasing) and accordingly so on. But after fifth stage entropy value is decrease than the fifth stage. So we can say that after the fifth stage of scrambling the randomness of the ciphered image cannot increase. So we have done scrambling up to the sixth stage.

A. Applying affine cipher technique in encrypted images

In order to increase the security measures, or to make the encryption even more difficult for the attackers to decrypt, we have implemented affine cipher in each and every pixel. This adds to the security. Affine cipher is an example of substitution cipher, where each alphabet of any text message is mapped to the numeric equivalent of the same. A mathematical expression is used to encrypt a text message and another mathematical expression is used to decrypt it back. In this cipher, every single alphabet is encrypted individually [1, 14].

B. Function used for encryption

E(x) = (ax + b) mode m, where m is the size of the alphabet and a & b are the key of the cipher. 'a' must be chosen in such a way that m and a are co-prime [1, 14].

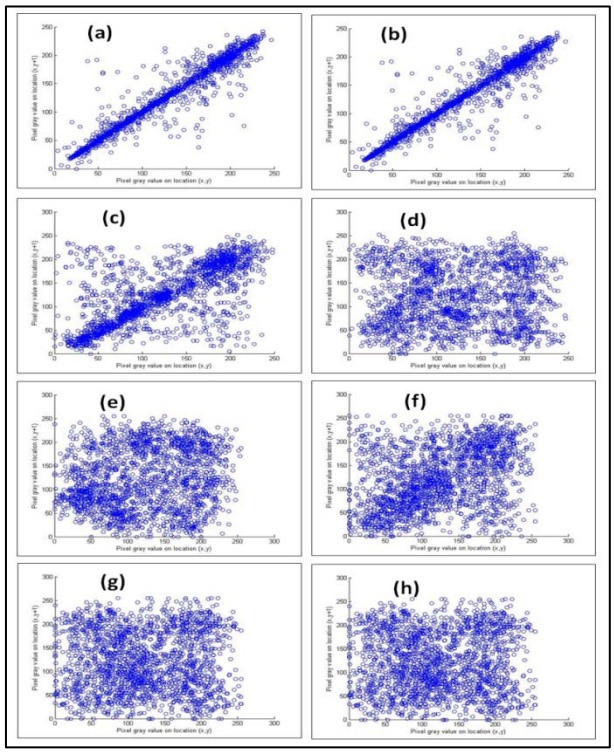

Fig. 4 Horizontal correlation of (a) Original Image (b) Decrypted image (c) First Stage Scrambled (d) Second Stage Scrambled (e) Third Stage Scrambled (f) Fourth Stage Scrambled (g) Fifth Stage Scrambled (h) Sixth Stage Scrambled

C. Function used for decryption [1, 14]

D (E(x)) $= a^{-1}$ (E(x) – b) mod m
$= a^{-1}$ (((ax + b) mod m) – b) mod m
$= a^{-1}$ (ax + b – b) mod m
$= a^{-1}$ (ax) mod m
= x mod m

In figure 5, it can be observed, if we apply affine cipher algorithm on the 'sixth stage scrambled images' (figure 5 (b)), the randomness of the pixel increases significantly. The images after applying affine cipher are shown in figure 5 (c). In order to analyze the randomness of these ciphered images, we have plotted its histogram (figure 5 (d)). Histogram of each figure showed that the distribution of pixel values of ciphered images are uniform and attacker may not get any information by these histograms. Apart from these histograms, horizontal pixel relationship graph is also plotted which is shown in figure 5 (e). All the scattered graph of horizontal pixels relationship expressed that the distribution of pixel values are scattered and randomness is very high. The correlation coefficients for different images are shown in Table III.

TABLE III CORRELATION COEFFICIENTS (HORIZONTAL PIXELS) OF DIFFERENT SCRAMBLED IMAGES

Image Name	(x+1, y) Vs (x, y) Horizontal Correlation Coefficient		
	Original	6th Stage scrambled	After affine cipher
Boat	0.8450	0.0737	-0.0190
Elephant	0.8773	0.0569	-0.0139
Flower	0.8744	0.1694	0.0360
Fruit	0.9186	-0.1191	-0.0172
Peppers	0.8963	0.0937	-0.0195

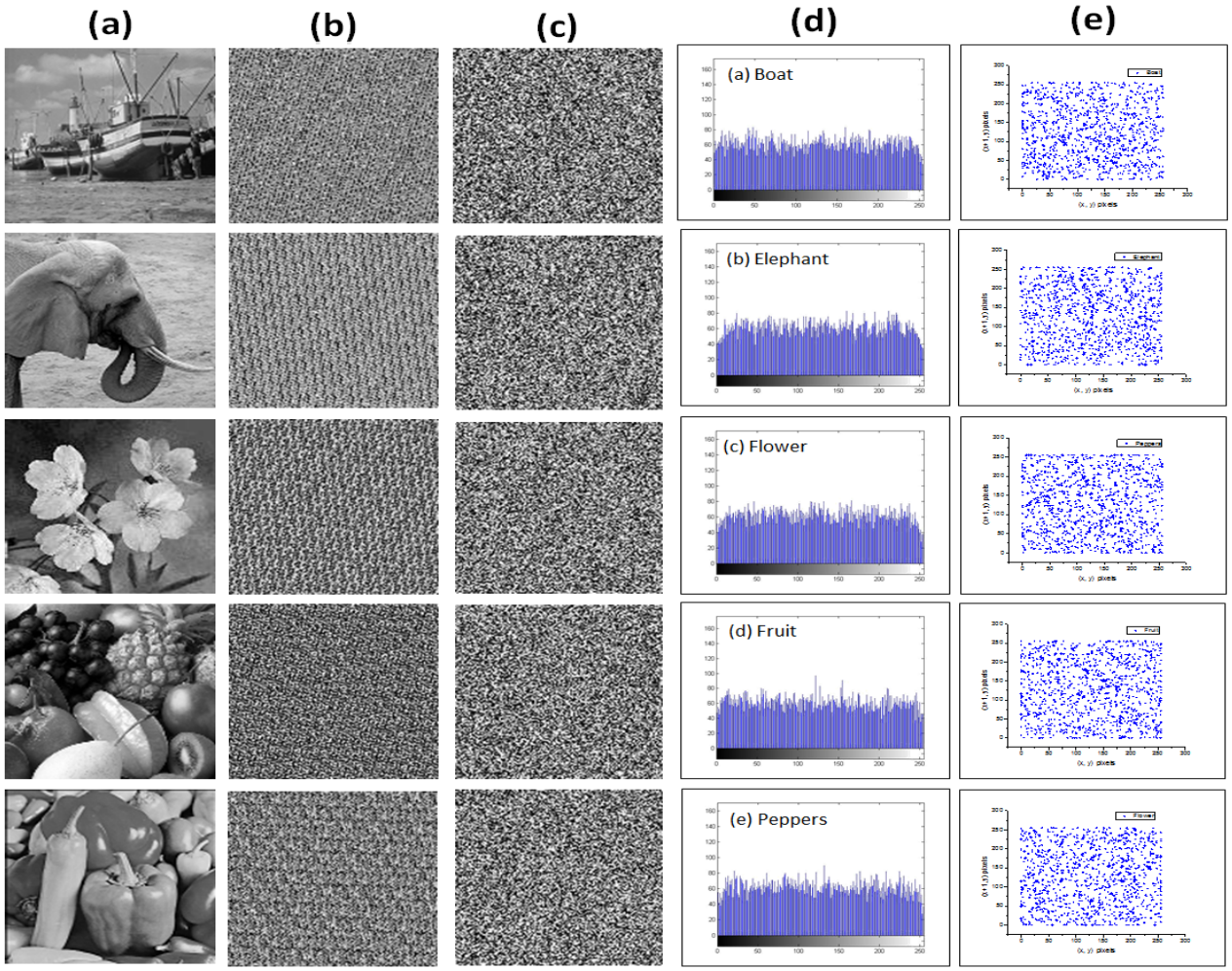

Fig. 5 (a) original images, (b) sixth stage scrambled images, (c) images after applying affine cipher algorithm, (d) histogram of images in 'c', (e) horizontal correlation between pixels.

D. Differential attack analysis

Differential attack/cryptanalysis is a common name of attacks which is basically applicable to the block ciphers working on binary sequences. The discovery of differential cryptanalysis is usually attributed to Eli Biham and Adi Shamir [11-12, 15]. They gave information about this type of attacks to different ciphers, which also includes theoretical weakness of Data Encryption Standard (DES) [13]. Since then, it has been a very general attack and this needs to be considered while thinking about various encryption techniques. The differential attack, as a kind of chosen – plaintext attack, investigates how the variations in plain – images can affect the corresponding cipher – images is an encryption system. It traces the differences and puts its efforts towards finding the connections between plain-

images and cipher – images. The attacker may seek to observe variations of the ciphertext in the tiny variations of the plaintext to find the correlation between the plaintext and the ciphertext. If a tiny change in the original image can lead to a great change in the cipher image, then the algorithm can effectively resist these differential attacks [11-13]. 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). [11-13].

Their definitions are as follows:

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

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

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

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 33.46% and 99.61%, respectively. A pixel is selected from the original image randomly. The corresponding cipher texts of this new plain image and the original image can be obtained by the proposed algorithm, respectively. Likewise, 500 tests are done and the corresponding values of UACI and NPCR can be found. Thus we can attain the average values of NPCR and UACI. The results of NPCR and UACI values are shown in Table IV It can be observed that the values of NPCR and UACI are near to the ideal values. This indicates that single bit difference of the plain image can diffuse to the whole cipher image, and we can conclude that the algorithm is capable of resisting differential attacks.

TABLE IV NPCR AND UACI VALUES

Image	NPCR	UACI
	Score	Score
Boat	0.980164	0.304611
Elephant	0.995422	0.340185
Flower	0.995178	0.341624
Fruit	0.994812	0.3445
Peppers	0.996094	0.341645

VIII. CONCLUSION

In this paper, it was found that a multilevel image scrambling followed by affine encryption can be an important tool to encrypt an image. It was also found that randomness of the encrypted image was increased when we increased security level by increasing the scrambling stage, but after fifth stage randomness started decreasing. Applying affine cipher randomness increases abruptly. There are two algorithms i.e. circular shift & affine algorithms were used. We have the liberty to have more numbers of keys i.e. keys for both algorithms separately. Firstly, we used circular shift algorithm where the security keys used to encrypt and decrypt the image were different, but the key which was used to decrypt the image was dependent on the key, used to encrypt the image. It can be concluded that overall process used for encryption and decryption may be useful in application world.

REFERENCES

[1] H. Zhua, C. Zhao, X. Zhanga, and L. Yang, "An image encryption scheme using generalized Arnold map and affine cipher", *Optik*, Vol. 125 No. 22, pp. 6672-6677, November 2014.

[2] R. Z. Wang, Y. C. Lana, Y. K. Lee, S. Y. Huang, S. J. Shyu, and T. L. Chia, "Incrementing visual cryptography using random grids, Optics Communications", Vol. 283, No. 21, pp. 4242-4249, November 2010.

[3] R. Lukac, K.N. Plataniotis, "Bit-level based secret sharing for image encryption", *Pattern Recognition*, Vol. 38, pp. 767-772, May 2005.

[4] M. Naor and B. Pinkas, "Visual authentication and identification, advances in cryptography", Lecture Notes in Computer Science, Springer-Verlag, New York, Vol. 1294, pp. 322–336, August 1997.

[5] D.C. Lou, H.K. Tso, and J.L. Liu, "A copyright protection scheme for digital images using visual cryptography technique", *Computer Standards and Interfaces*, Vol. 29, pp. 125-131, January 2007.

[6] 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.

[7] https://en.wikipedia.org/wiki/Image_histogram, (18 April 2017)

[8] C. Li and K. T. Lo, "Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks", *Signal Process*, Vol. 91, No. 4, pp. 949-954, June 2011.

[9] X. Liao, S. Lai, Q. Zhou, "A novel image encryption algorithm based on self-adaptive wave transmission", *Signal Process*, Vol. 90, No. 9, pp. 2714-2722, September 2010.

[10] https://en.wikipedia.org/wiki/Image_histogram, accessed on 17 June 2017.

[11] 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 No. 1, pp. 181-196, January 2015.

[12] B. Stoyanov, and K. Kordov," Image Encryption Using Chebyshev Map and Rotation Equation", *Entropy*, Vol. 17, No. 4, pp. 2117-2139, 2015.

[13] 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

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

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