International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT2174130

Visual Encryption Using Block based Scrambling Followed by Affine Encryption Technique

Durgesh Kumar Maurya*[1], Rajesh Kumar Pathak[2], Komal Yadav[3]
[1]Shri Rawatpura Sarkar University Raipur, Chhattisgarh, India
[2]Professor, Shri Rawatpura Sarkar University Raipur, Chhattisgarh, India
[3]Assistant Professor, Shri Rawatpura Sarkar University Raipur, Chhattisgarh, India

Article Info
Volume 7, Issue 4
Page Number: 579-583

Publication Issue :
July-August-2021

Article History
Accepted : 12 Aug 2021
Published : 23 Aug 2021

ABSTRACT

This article reports the Block based cipher concept followed by the affine cipher technique. The Image considered was grouped into squared (16, 32 and 64) pixel blocks then each column was shifted by specific values. These values were randomly generated prime numbers and worked as the key for scrambling. These images were investigated for their quality of scrambling using histogram and adjacent pixel correlation. The adjacent pixel correlations for 16, 32 and 64 pixel-based ciphered images were found as 0.7907, 0.7292, and 0.4783 respectively. The analysis gave the information that the level of scrambling was not satisfactory, therefore; the affine cipher technique was applied to each of the images. These images were converted into the matrix format and each element was transformed using the affine cipher. This transformed matrix is again converted inform of the image to visualize. The Histogram and adjacent pixel correction for these images were much improved.

Keywords : Scrambling, Visual encryption, Block level encryption.

I. INTRODUCTION

In the recent past, the use of the internet has been increased rapidly. The use of visual multimedia has also been increased with the increasing use of cybersecurity. In the recent past, visual security was a bigger concern of military application, now it has been mandatory for many sectors including the banking and finance sectors. Some of the basic features of the images like bulk data capacity and large correlation among nearby pixels; traditional encryption techniques are not very useful now a day [1]. The two-dimensional (2D) digital images play more and more important roles in modern digital technology. A 2D digital image is a type of 2D data, which carries data in a visualized and meaningful way. Then, if secret images are decrypted, used or viewed by prohibited users, devastating security issues may arise. For example, hostile country to get the detailed parameters and settings for weapons to analyze the image that is being steal by the spy. Therefore, it is quite important to protect digital images and image cipher is an efficient solution to image security issues by encrypting a digital image into a random-like cipher-image **[2-4].** Various ways are there for scrambling an image like Block based scrambling **[5]**, Relative prime shuffling **[6]**, pixel scrambling **[7-9]** etc. Many researchers have reported different algorithm

to create cipher image. For getting the ciphered image, block level scrambling technique is used. In this work, whole image was divided into desired number of sections of specific dimensions. We have used circular shift procedure to scramble the picture. We have also used a set of key of randomly generated prime numbers.

II. RESULT & DISCUSSION

2.1 Algorithm for Encryption

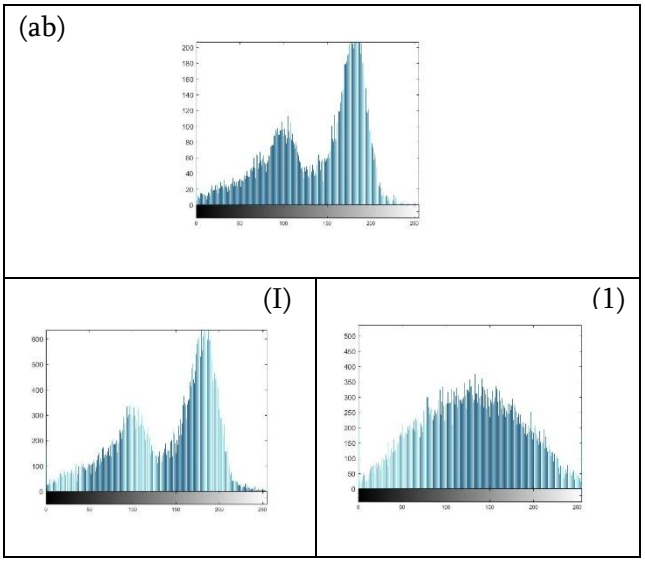
For encryption technique below is the steps shown:
Reading the image of square dimension (n x n)
Finding the dimension of the image
Converting the image in the cell of blocks of the desired dimension
(i.e. 16 x 16, 32 x 32, 64 x 64, 128 x 128……., m x m)
Generating random prime numbers to generate a set of keys of dimension 1 x m
Shifting the columns of the cell of blocks by the corresponding element of key
Transposing the shifted columns of blocks
Shifting the columns of outcome Transposed columns of blocks using the same keys
The scrambled image received from step 7 was converted into a matrix.
Each pixel of the image was considered as an element of the matrix.
Converted each element of the matrix to display the final scrambled image. The formula used for conversion was as under:-
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].

Results found from Encryption using Block based shifting followed by Affine cipher Technique

We encrypted the image using the algorithm already discussed in section 2.1. We scrambled the image by shifting the blocks of various sizes (16x16, 32x32, 64x 32, and 128x128). The scrambled images using the various block sizes are given in Figure 1 (a) – 1(d). The corresponding histograms of the encrypted images are also shown in Figure 2 (I) – 2 (IV). By observing these histograms closely, it can be concluded that corresponding histograms have non-uniform peaks which may be helpful for cryptanalysts to recover the original image. Therefore, the affine cipher technique was applied to every element to improve the quality of scrambling. Applying affine cipher technique in encrypted images.

In order to increase the difficulty level for attackers to decrypt the image, affine cipher in every pixel is employed. This adds to the security. Affine cipher is an example of substitution cipher, where each letter 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.

The histogram for the images scrambled using block ciphering followed by the affine cipher is shown in Figure 2 (1) – 2 (4). Comparing the histograms from Figure 2 (I) – 2 (IV) and Figure 2 (1) – 2 (4), we may conclude that later on, after applying the Affine Cipher technique the level of scrambling got better.



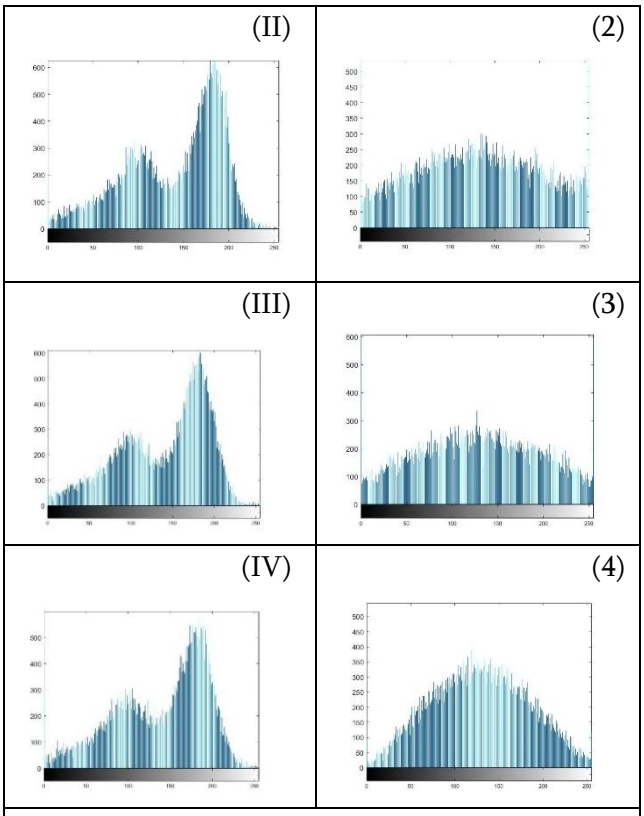
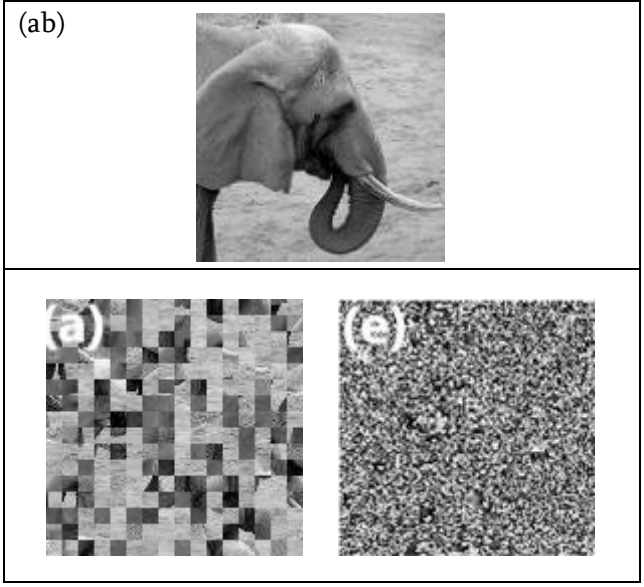


Figure 2 Histogram of- **(ab)** Original image **(I)** Elephant 16 Blocks **(II)** Elephant 32 Blocks **(III)** Elephant 64 Blocks **(IV)** Elephant 128 Blocks, After applying Affine **(1)** Elephant 16 Blocks **(2)** Elephant 32 Blocks **(3)** Elephant 64 Blocks **(4)** Elephant 128 Blocks



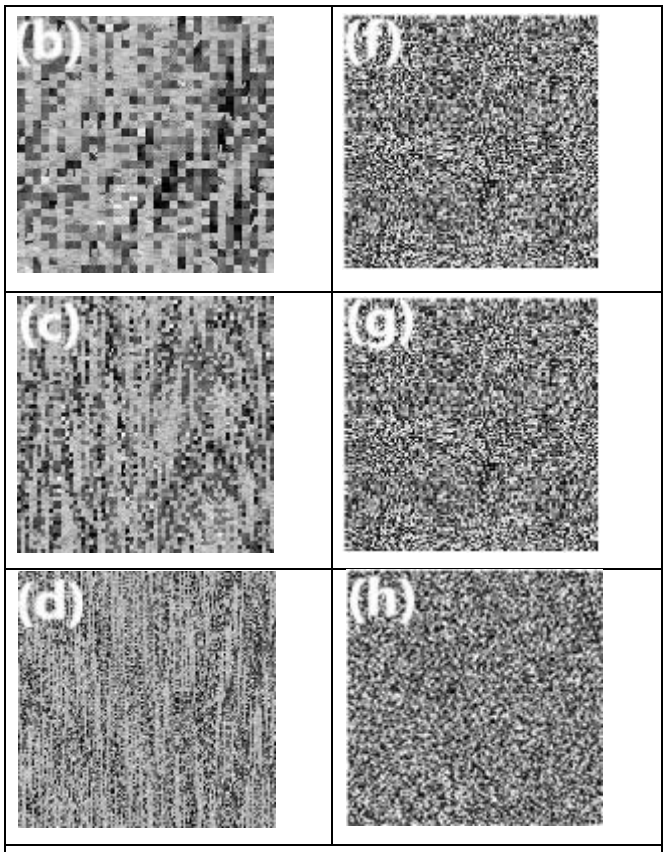


Figure 1 Scrambled images **(ab)** Original image **(a)** Elephant 16 Blocks **(b)** Elephant 32 Blocks **(c)** Elephant 64 Blocks **(d)** Elephant 128 Blocks, After applying Affine **(e)** Elephant 16 Blocks **(f)** Elephant 32 Blocks **(g)** Elephant 64 Blocks **(h)** Elephant 128

In order to find the quality of scrambling received after ciphering through Affine Cipher, some security analysis (s) such as were done.

III. ADJACENT PIXEL VALUES

If the adjacent pixels have the close by values, then the image will be meaningful. When we scramble any image, we expect the pixel value of the adjacent position to be scattered. Hence the level of scattering can be determined by the amount of scattering of the points. We have calculated the correlation between the horizontal nearby pixels. For this, we choose 1000 pairs of randomly selected horizontally adjacent pixels **[10-14].**

Figure 3 **(a – g)** indicated the amount of scattering in different images. It can be observed that for the original "Elephant.jpg" image, we don't have plenty of scattering and as we start scrambling the image using the circular shift technique, after breaking the image into the various number of blocks, we find that amount of scattering is increasing when we increase the number of blocks. The scattering of points is highest when we convert the image into the number of blocks equal to its dimension.

Original	Correlation coefficient (Only Block Shifting)		
	Block (16)	Block (32)	Block (64)
0.9459	0.7907	0.7292	0.4783
	Correlation coefficient (With Affine Cipher)		
	Block (16)	Block (32)	Block (64)
	0.4077	0.1934	0.1846

IV. CONCLUSION

The concept of the Block based cipher followed by affine cipher technique was used in this work. The Image considered was grouped into squared (16, 32 and 64) pixel blocks then each column was shifted by specific values. These values were the randomly generated prime numbers and worked like the key for scrambling. These images were investigated for their quality of scrambling using histogram and adjacent pixel correlation. The adjacent pixel correlations for 16, 32 and 64 pixel-based ciphered images were found as 0.7907 , 0.7292, and 0.4783 respectively. Considering the high correlation Affine cipher technique was applied and again adjacent pixel correlations were obtained. The values found were 0.4077 , 0.1934, 0.1846 for squared (16, 32 and 64) pixel blocks respectively after applying the affine cipher technique. In all, it may be concluded that if the hybrid techniques can be applied for encryption, it may be more powerful in terms of security parameters.

V. REFERENCES

[1]. Zhongyun Hua, Yicong Zhou, "Design of image cipher using block-based scrambling and image filtering", Information Sciences vol. 396 (2017) pp. 97–113

[2]. X. Chai, Z. Gan, Y. Chen, Y. Zhang, "A visually secure image encryption scheme based on compressive sensing" , Signal Process, vol. 134 (2017) pp. 35-51

[3]. Y. Zhang , L.Y. Zhang , "Exploiting random convolution and random subsampling for image encryption and compression", Electron. Lett. vol. 51 no. 20 (2015) pp. 1572–1574

[4]. H. Zhu , C. Zhao , X. Zhang , "A novel image encryption–compression scheme using hyper-chaos and Chinese remainder theorem", Signal Process. Image Commun. vol. 28 no. 6 (2013) pp. 670–680

[5]. Z. Hua, Y. Zhou, "Design of image cipher using block-based scrambling and image filtering", Information Science vol. 396 no.7 (2017) pp. 97-113

[6]. H.B. Kekre, T. Sarode, P. Halrnkar, , "Image scrambling using R-Prime shuffle", International Journal of Advanced Research in Electrical, Electronics, and Instrumentation Engineering, vol. 2 no. 8 (2013) pp. 4070-4075

[7]. G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map", Pattern Recognition Letters, vol. 31, no. 5 (2010) pp. 347–354

[8]. http://homepages.inf.ed.ac.uk/rbf/HIPR2/fourier.htm, (18 April 2017)

[9]. X. Y. Wang, Y.Q Zhang, L.T. Liu, "An enhanced sub-image encryption method Optics and Lasers in Engineering", Optics and Laser in Engineering, vol.86 no. 11 (2016) pp. 248-254

[10]. P. Sharma, D. Mishra, V.K. Sarthi, P. Bhatpahri, R. Shrivastava, "Visual Encryption Using Bit Shift Technique", International Journal of Scientific Research in Computer Science & Engineering, vol. 5 no. 3 (2017) pp. 57-61

[11]. A. Soleymani, M. J. Nordin, and E. Sundararajan, "A Chaotic Cryptosystem for Images Based on Henon and Arnold Cat Map", The Scientific World Journal, vol. 2014, no.7, (2014) pp. 1- 21

[12]. B. Saha, "A Comparative Analysis of Histogram Equalization Based Image Enhancement Technique for Brightness Preservation", International Journal of Scientific Research in Computer Science and Engineering, vol. 3 no. 3 (2015) pp. 1-5

[13]. C. P. Patidar and Meena Sharma, "Histogram Computations on GPUs Kernel using Global and Shared Memory Atomics", International Journal of Scientific Research in Computer Science and Engineering, vol.1 no.4 (2013) pp.1-6.

[14]. C. Li, K. T. Lo, "Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks", Signal Processing, Vol. 91 no. 4 (2011) pp. 949–954.

Cite this article as :

Durgesh Kumar Maurya, Rajesh Kumar Pathak, Komal Yadav, "Visual Encryption Using Block based Scrambling Followed by Affine Encryption Technique", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 4, pp. 579-583, July-August 2021. Available at
doi : https://doi.org/10.32628/CSEIT2174130
Journal URL : https://ijsrcseit.com/CSEIT2174130