International Journal of Scientific Research in Computer Science and Engineering
Vol.5, Issue.3, pp.57-61, June (2017)

Research Paper

E-ISSN: 2320-7639

Visual Encryption Using Bit Shift Technique

P. Sharma[1], D. Mishra[2], V.K. Sarthi[3], P. Bhatpahri[4], R. Shrivastava[5*]

[1]Department of Computer Science & Engineering, ICFAI University, Kumhari, Durg, India
[2]Department of Mechanical Engineering, ICFAI University, Kumhari, Durg, India
[3]Department of Computer Science & Engineering, Govt. Polytechnic College, Jagdalpur, India
[4]Department of Mechanical Engineering, ICFAI University, Kumhari, Durg, India
[5*]Department of Physics, ICFAI University, Kumhari, Durg, India

Corresponding Author: ravishrivastava95@gmail.com, Tel.: +919893726504

Available online at: www.isroset.org

Received 14th May, 2017 Revised 25th May 2017, Accepted 20 Jun 2017, Online 30th Jun 2017

***Abstract*—** In present paper we report an effective method of scrambling an image, which can be used as one of the important tool in visual cryptography. A sample image is scrambled using bit shift technique using specific algorithm. The considered algorithm was explained using a matrix representation, taking an 8 x 8 sample matrix. Intensity distribution and toner distributions of scrambled images were studied using their histograms. The results of histogram of an image, in which, each pixel was shifted 4 places left, using bit shift technique, expressed that the toner distribution is uniform throughout. In order to judge the complexity level of scrambling, horizontal and vertical correlation of adjacent pixels and of 4 bit shifted scrambled images were also calculated. Values of horizontal and vertical correlation coefficients were also calculated, which reflected that the complexity and randomness of pixels increases with increasing stages of scrambling which supports the result obtained in histogram. This technique of encryption can be used as a very useful tool in digital security system.

***Keywords*—** Cryptography, Matrix Algorithms, Scrambling, Horizontal and Vertical Correlation

I. INTRODUCTION

Digital images play a vital role in today's digital technology. Digital security has been the most intensive area of research because of increasing use of digital communication and digital money transactions. Apart from the digital security, Visual cryptography is also useful in encrypting the secret message to be sent, related to defense systems of the country and other important cyber data, because the unauthorized access to these data may create severe issues of national security. To prevent important from being theft and misuse, the original message is needed to convert into random-like cipher message using a specific secret code, called key in such a way that, original message can be recovered, only after the use of correct secret key **[1-5]**. Visual cryptography plays an important role in accomplishment of the same. Image scrambling is a part of visual cryptography and it is a very powerful approach to encrypt the image into unintelligible format. There are number of ways possible to scramble an image like Relative prime shuffling **[6]**, Block based scrambling **[3]**, Pixel scrambling **[7-9]** etc. Many researchers have reported different algorithms to create cipher image. We have tried a bit-shift algorithm to get the encrypted image. It was observed that, the randomness of the pixels increases with increasing number of bits shifted towards left.

II. ALGORITHM

A. Encryption algorithm

(1) Take any greyscale image of m x m dimension.
(2) Select a digit between 1 to 7, which will be used as a key to shift number of bits towards left of each pixel value.
(3) Shifting n bit left, multiplies pixel value by 2^n.
(4) Pixel values after shift different places, exceeds the greyscale range 0-255.
(5) For getting the pixel values within the defined range for a greyscale image, we managed to create two different matrices of same dimensions carrying quotient and remainder when the each element shifted matrix was divided by 256.
(6) The remainder matrix is used as encrypted image.

B. Decryption algorithm

(1) Take encrypted image.
(2) We need to have quotient matrix with us to get the original image back because the encrypted image is

nothing but the remainder when each element of shifted image is divided by 256.

(3) We can use dividend=quotient*divisor + remainder to get the dividend matrix, i.e. left shifted matrix.

(4) We need to apply right bit shift operation on dividend matrix to get the original image back.

If we shift an 8 bit binary data by 'n' places, we get a data, whose decimal equivalent is 2^n times, the initial value. This property is utilized in this encryption technique. Matrix representation for the technique used for encryption and decryption is elaborated in Figure **1**. We have used a square matrix of dimension 8 x 8 to explain the method for encryption and decryption.

III. SCRAMBLING OF IMAGE

An image, elephant.jpg is used for analyzing the suitability of scrambling technique used. Original image along with different scrambled images are shown in Figure **2**. Figures show that complexity of images is increasing with increasing number of left shifts. It can easily be observed that image found after four bits left shift, level of scrambling is complex. For discussing about the security of scrambled images, we have studied histogram and correlation between adjacent pixels. This entire process was carried out in Software MATLAB ver. R2009b.

IV. HISTOGRAM ANALYSIS

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 **[10-12]**. Histogram of "elephant.jpg" Gy-Scale image with the histogram of original and 4 bit left shifted ciphered images are shown in **Figure 3**. It can easily be predicted that pixels of different values are distributed uniformly for an image when a left shift of 4 is incorporated in each pixels and remainder matrix is used as an encrypted matrix. This shows that the randomness is high in cipher image and it is difficult to descramble.

V. ADJACENT PIXEL VALUES

Two adjoining pixels in a regular image are strongly correlated in horizontal and vertical positions **[8-9, 12-13]**. 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 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 **[8-9, 12-13]**. The graphical representation of horizontal correlation between adjacent pixel values for different images, are shown in **Figure 4**. Correlation coefficients were calculated for original image and 4 bit left position shifted ciphered image by using equation 1. These calculated values are shown in Table 1. For original image the value of correlation coefficients are much closer to 1.0, which is the maximum possible value of correlation coefficient. When these coefficients were calculated for ciphered images its value decreased drastically, the values found are very low and closed to 0.

$$r_{x,y} = \frac{\Sigma(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\Sigma(x_i - \bar{x})^2 (y_i - \bar{y})^2}} \quad \cdots\cdots\cdots \quad (1)$$

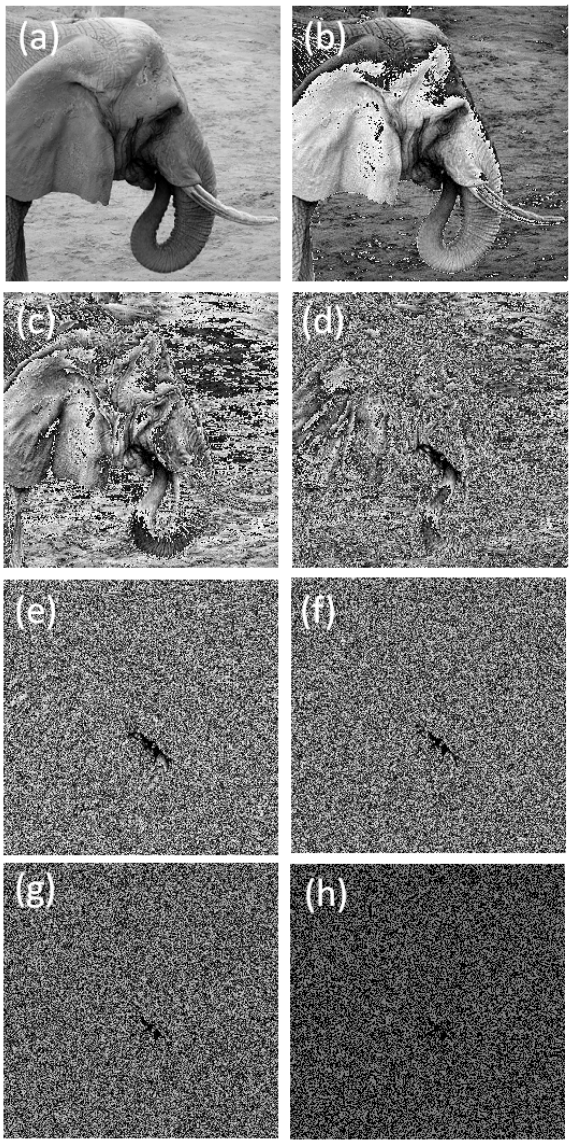

Figure 2 (a) Original Image (b) 1 bits shifted image (c) 2 bits shifted image (d) 3 bits shifted image (e) 4 bits shifted image (f) 5 bits shifted image (g) 6 bits shifted image (h) 7 bits shifted image

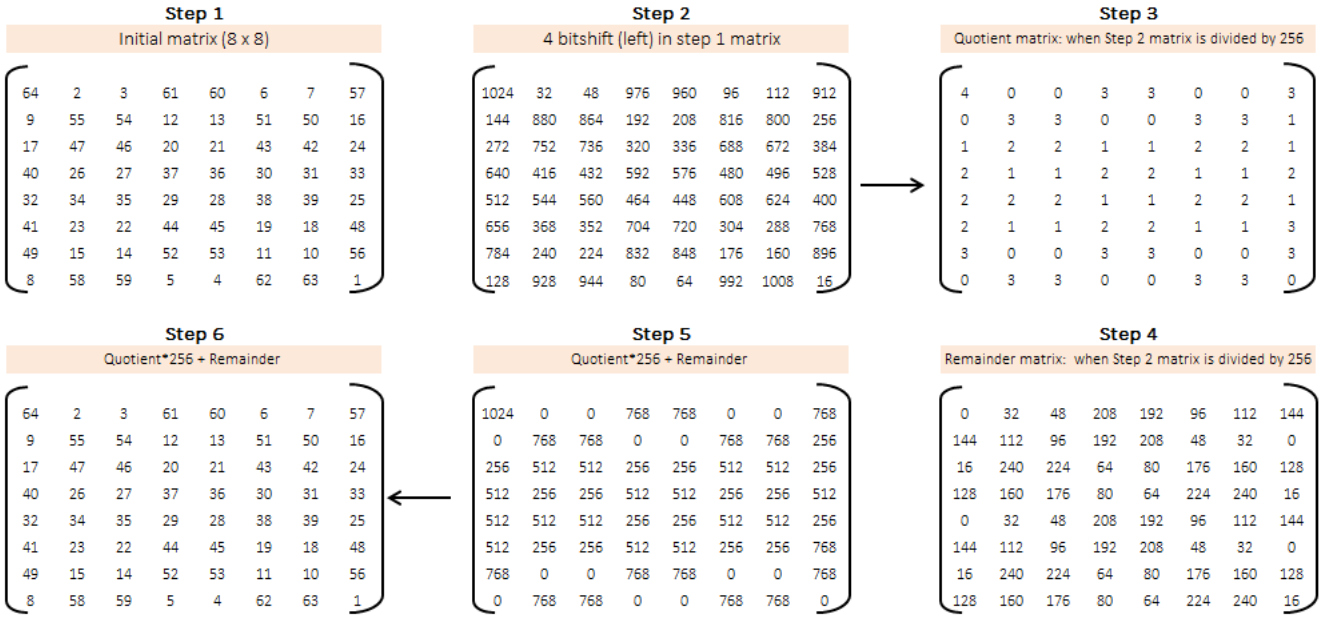

Figure 1 Matrix representation of algorithm used

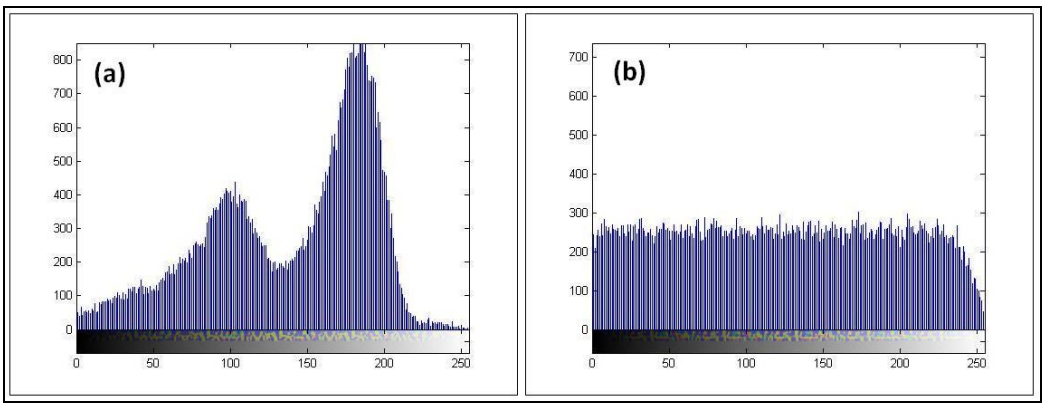

Figure 3 Histogram of (a) Original Image (b) 4 bit shifted image

Table 1 Correlation Coefficient at different stages of Scrambling for elephant.jpg

Not of bit(s) shifted	0	1	2	3	4	5	6	7
Horizontal Correlation (x+1, y)	0.9493	0.6060	0.3122	0.1123	-0.0363	0.0047	0.0043	-0.0064
Vertical Correlation (x, y+1)	0.9601	0.6932	0.4477	0.1255	0.0186	-0.0117	0.0013	-0.0485

VI. CONCLUSION

In this paper, we have performed bit-level left shifting to modify the image matrix. For converting the pixel values of the modified image within the ranges specified for images i.e. (0-255), we divided these pixel values by 256 and created a remainder matrix. This remainder matrix is used as ciphered image. We got different matrices by shifting 1, 2, 3, 4, 5, 6, and 7 places towards left positions using above mentioned method. If we go for 8 places left bit shift, pixel value of original image is multiplied with 2^8, which is 256. As a result, all the elements of modified matrix become multiples of 256 hence we get 0 remainder for every elements. In this method, we are using single key as shift number but we require having remainder matrix with us to decrypt the ciphered image. This increases the security level by a good extent. In all we may conclude that this Image scrambling method can be an important tool to encrypt an image. Histogram of encrypted image expressed that there is uniform distribution of pixels, which makes it difficult for hackers to decrypt.

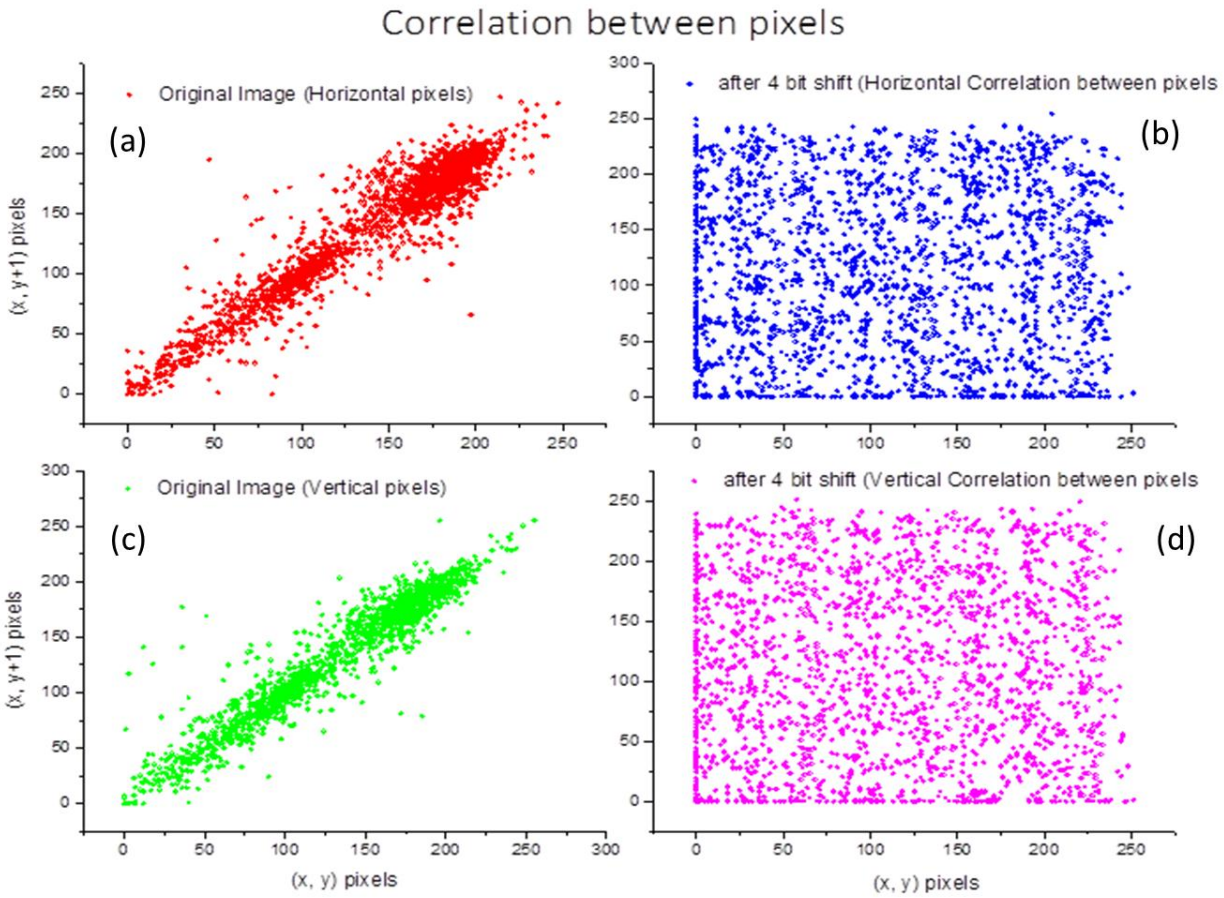

Figure 4 (a) Horizontal pixels correlation of Original Image (b) Horizontal pixel correlation of the 4 bit shifted image (c) Vertical pixels correlation of Original Image (d) Vertical pixel correlation of the 4 bit shifted image

REFERENCE

[1] X. Chai, Z. Gan, Y. Change, Y. Zang, "*A visually secure image encryption scheme based on compressive sensing*", Signal Processing, Vol. 134, Issue.5, pp. 35-51, 2017.

[2] Y. Zang, L.Y. Zhang, "*Exploiting random convolution and random subsampling for image encryption and compression*", Electron Letters, Vol. 51, Issue. 20, pp. 1572-1574, 2017.

[3] Z. Hua, Y. Zhou, "*Design of image cipher using block-based scrambling and image filtering*", Information Science Vol. 396, Issue.7, pp. 97-113, 2017.

[4] C. Ling, X. Wu, S. Sun, "*A general efficient method for chaotic signal estimation*", Transactions on Signal Processing, Vol. 47, Issue. 5, pp. 1424–1428, 1999.

[5] T. Guo, F. Liu, C. Wu, *"k out of k extended visual cryptography scheme by random grids"*, Signal Processing, Vol. 94, Issue.1, pp. 90-101, 2014.

[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, Issue. 8, pp. 4070-4075, 2013.
[7] G. Ye, "*Image scrambling encryption algorithm of pixel bit based on chaos map"*, Pattern Recognition Letters, Vol. 31, Issue.5, pp. 347–354, 2010.
[8] 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, Issue.11, pp. 248-254, 2016.
[9] 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, Issue.7, pp. 1-21, 2014.
[10] 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, Issue. 3, pp. 1-5, 2015.
[11] 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, Issue.4, pp.1-6, 2013.
[12] C. Li, K. T. Lo, "*Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks"*, Signal Processing, Vol. 91, Issue. 4, pp. 949–954, 2011.
[13] X. Liao, S. Lai, Q. Zhou, "*A novel image encryption algorithm based on self-adaptive wave transmission"*, Signal Processing, Vol. 90, Issue. 9, pp. 2714–2722, 2010.

Authors Profile

Ms. Piyali Sharma is MCA from Dibrugarh University, Assam. She is Faculty member in Department of Computer Science at ICFAI University, Kumhari, Durg. She has 02 years of overall experience. Recently she is working in the field of Cryptography.

Mr. Dilip Mishra is working as Faculty Member in the Department of Mechanical Engineering at ICFAI University, Raipur. He is B.E. (Mechanical) and M.E. (Thermal). He has 12 publications. His area of expertise is non-conventional energy sources and area of interest is Thermal Engineering, Cryptography etc. He is having membership of two professional educational bodies of India, i.e. LMC-Indian Section, IIT madras & LMISTE and a member of IRD, India.

Mr. Vijay Kumar Sarthi is M.Tech. in Computer Science from NIT Rourkela, he has qualified UGC-NET and CG SET. He is currently working as Assistant professor in the department of Computer Science at Govt. Polytechnic College, Jagdalupur.

Mr. Pramay Bhatpahri is B.E. 2013 (Mechanical Engineering) CSVTU, Bhilai and M.Tech 2016 (Machine Design) NIT, Raipur, He has done an internship of 1 years at TATA Steels, Jamshedpur. Currently, he is teaching at ICFAI University, Kumhari, Durg as a faculty member in the Department of Mechanical Engineering.

Mr. Ravi Shrivastava is working as Faculty Member in the Faculty of Science & Technology. He is M.Sc. in Physics with specialisation in Electronics from Govt. VYT PG Autonomous College Durg, B.Ed. from Kalyan College, Bhilai, PGDCSc from Kalyan College, Bhilai & Ph.D. in Physics from Pt. Ravi Shankar Shukla University, Raipur. He has approximately 10 years of experience in teaching. He has published more than 42 articles in different natioanl and international journals. He is life time member of Luminescence Society of Indian and Member of International Journal of Computer Sciences and Engineering.

