iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VII **Month of publication:** July 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

Implementation of Digital Image Scrambling Encryption Technique

Dhananjay Santosh Waghulde[1], Dr. P. M. Mahajan[2]
[1]*Department of Electronics & Telecommunication, North Maharashtra University, Jalgaon*
[1]*P.G.Student,* [2]*Associate Professor, J. T. Mahajan college of Engineering, Faizpur, Maharashtra,India*

Abstract*: *Digital image scrambling encryption technology is a way of securing digital image information. With the use of transformation techniques, it can change the original image into a disordered one beyond recognition, making it difficult for those who get the image in unauthorized manner to extract information of the original image from the scrambled images. In this paper two different techniques (Digital Image Scrambling Encryption using Arnold Transform and Random Permutation) are implemented .Performance and Security parameters of scrambled images are evaluated and compared. We define set of measures of effectiveness for comparative performance and security analysis and then used on proposed algorithms that have been applied on different sets of images.

Keywords*: *Digital Image, Image Scrambling Encryption, Arnold Transformation, Random Permutation

I. INTRODUCTION

Image scrambling encryption disarrange pixel position or pixel color in order to make it unrecognizable and finding the algorithm to rebuild the original image. With the use of transformation techniques, it can change the original image into a disordered one beyond recognition, making it hard for those who get the image in unauthorized manner to extract information of the original image from the scrambled images [3]. Scrambling a digital signal in the spatial or the frequency domain corresponds to modify that signal in such a way that the original semantic media loses its meaning and become hard to be viewed (the inverse of scrambling is descrambling). Refer to transforming the digital image into another completely different digital image. The users only know the algorithm and keys; this allows them to restore the original image. Also image scrambling can be seen as encryption. The plain text is the original image and the cipher text is meaningless noises for unauthorized users [2].

The scrambling encryption process of digital image is essentially a process of coding and decoding of a class of image. When the third capture confusing image, since the parameters of scrambling algorithm are confidential, even in the case that the algorithm is known it is also difficult to decipher. The image scrambling requires that the image has a lower intelligibility after scrambling; the scrambling image should have a certain degree of security after scrambling, and can withstand a certain degree of attack. Digital image scrambling cannot change the resolution of images; the images that remove the scrambling have undifferentiated or little difference with original image, and can be able to accurately express the content or meaning of the original image. Figure 1.1 shows generalized block diagram of image scrambling [4].

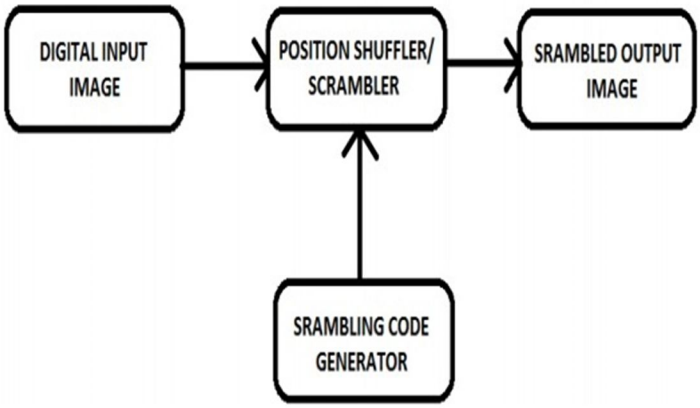


Fig. 1.1: Block Diagram of Image Scrambling

Compared with traditional cryptography, digital image has a large amount of data, thus it has a lot of clear space, and also has a great cipher text space, and the most important is the autocorrelation of the digital image visually manifested direction of perpendicular and direction of various tilt angles. Therefore, when considering the scrambling encryption algorithm we should fully consider the impact of algorithm on the image autocorrelation, the worse the autocorrelation the better the scrambling, the poorer the intelligibility of the image after scrambling. Therefore, the conventional cryptography encryption algorithm has a strong security, but the effect of encrypting image is not necessarily the best [4].

II. PROPOSED SCRAMBLING ENCRYPTION METHODOLOGY

A. Arnold Transformation Based Image Scrambling Encryption

The Arnold transform is an image scrambling technique that can be used to encrypt and decrypt image data. The transform is area preserving and invertible without loss of information. It is also known as cat map. The mapping can be done successively several times to completely obscure the image beyond recognition. Alice has the information about the number of times the transform is applied and can successfully recover the original image [13].

Following steps include in encryption by Arnold transformation

1) Input original image.

2) Resize the original image into nxn matrix.

3) apply the Arnolds transformation to nxn matrix by using the equation

$$T\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x+y \\ x+2y \end{bmatrix} mod\ n$$

where mod is modulo of $\begin{bmatrix} x+y \\ x+2y \end{bmatrix}$

a) Shear in x- direction by factor of 1.

b) Shear in y- direction by factor of 1.

c) Evaluate modulo

4) Reassemble the image.

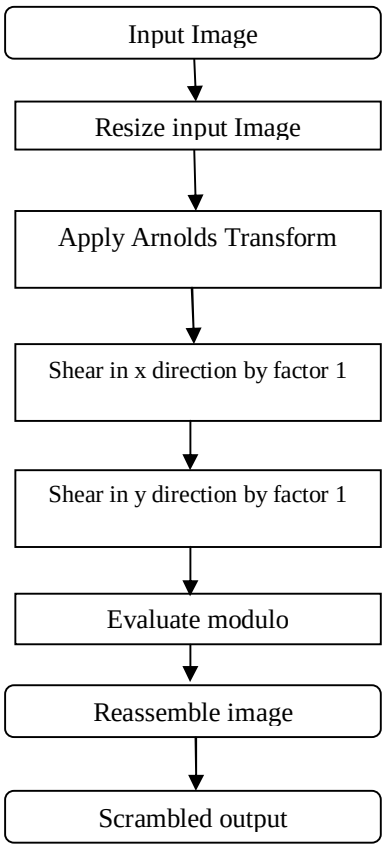


Fig.2.1: Workflow of Arnold Transformation

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

B. Scrambling Encryption Using Random Permutation

The development of image encryption using chaotic random permutation is attracted in recent year. The basic permutation can be performed in three ways such as bit, pixel and block permutation. The permutation of bits is effective in significantly reducing the correlation thereby decreasing the perceptual information, whereas the permutation of pixels and blocks are good at producing higher level security compared to bit permutation [16].

A pixel in a digital image is collection of 8 bits therefore maximum available key of bit permutation is equal to 8! (40320) .The pixel permutation can be performed by shuffling the pixel position according to the encryption key. The encryption key size can be one dimensional (1-D) or two dimensional (2-D) for pixel permutation. 2-D key has more number of encryption key as compare to 1-D key. The encrypted image can be decrypted only if attacker has knowledge of key and large numbers of possible key spaces make it infeasible to extract the original information.

The encryption algorithm includes following steps:

1) Input original image.
2) Find the size of original image (m*n)
3) Reshape the m*n matrix whose elements are taken column wise sequence.
4) Convert the sequence of decimal values into binary bits (unit 8).
5) Apply random permutation (p) to sequence.
6) Convert the sequence of binary bit values to decimal.
7) Reconstruct the sequence into image size (m*n).
8) End.

C. The Decryption Algorithm includes following steps

1) Input scrambled image
2) Reshape the m*n matrix whose elements are taken column wise sequence.
3) Convert the sequence of decimal values into binary bits (unit 8).
4) Reconstruct the random permutation by using value (p).
5) Convert the sequence of binary bit values to decimal.
6) Reconstruct the sequence into image size (m*n).
7) End.

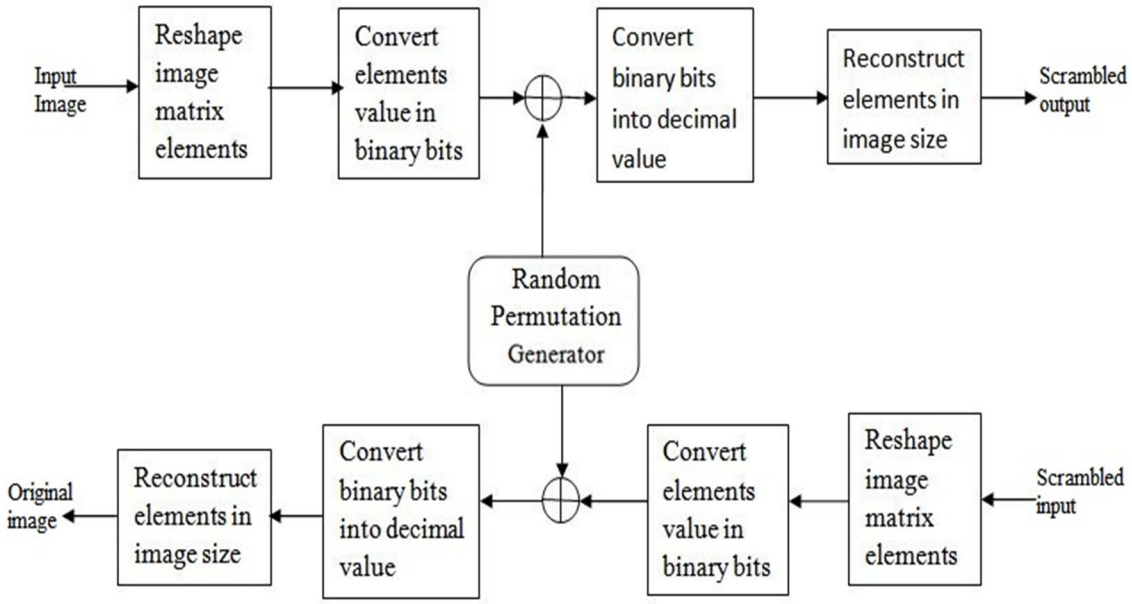


Fig. 2.2: Workflow of Random permutation scrambling encryption

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

III. PERFORMANCE AND SECURITY PARAMETERS

Following parameters are used to assess the performance and security of scrambled image.

A. Uniform Image Histogram

Histogram provides information about the frequency distribution of continuous pixels and density estimation. So a cipher image should have a uniform histogram to be secure from the known plain-text attack. For example, figure 3.1.1 is the histogram of the original image and figure 3.2 is the histogram of the encrypted image. Figure 3.1.2 shows the more uniform histogram that is highly desirable.

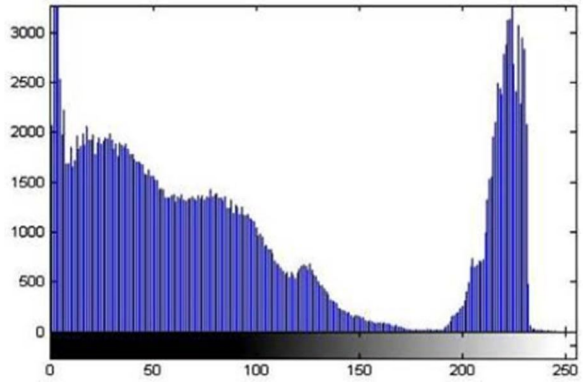


Figure 3.1.1 Histogram of Original Image

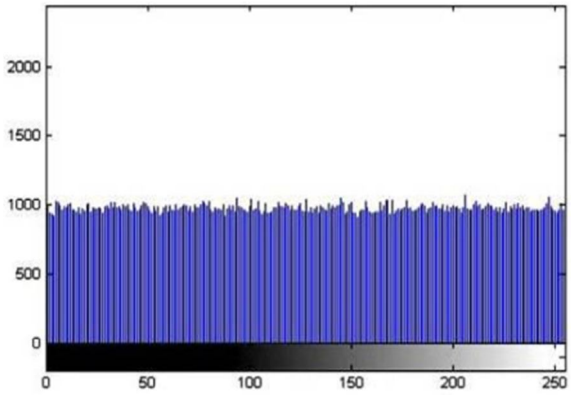


Figure3.1.2 Histogram of Cipher Image

B. Information Entropy

It identifies the degree of uncertainty and uniform distribution in the system. Thus, an encryption technique should show randomness and uniform distribution in the encryption process. Information entropy is calculated by the following formula.

$$H(m) = -\sum_{i=0}^{2^N-1} P(m_i)\log_2[P(m_i)] \qquad (1)$$

Where p (mi) defines the probability of a pixel and N is the number of bits in each pixel. For a gray level image, each pixel has 8 bits, so the probability of a pixel is 1⁄28. Hence, information entropy of the gray level image is H (m) = 8. However, practically it is intricate to obtain ideal entropy; so slight difference is also tolerable.

C. Correlation Analyses

It assesses the correlation between two adjoining pixels of the plain-image and the cipher image [17]. An encrypted image should have low correlation between two abutting pixels. For example, xi and yi are two pixel pair then the correlation coefficient can be calculated by equation (5)

(2)

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \ ,$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 , \quad (3)$$

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))\,(y_i - E(y)) \ , \quad (4)$$

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \ , \quad (5)$$

where $\sqrt{D(x)} \neq 0$ and $\sqrt{D(y)} \neq 0$

Where xi and yi are gray level value of two adjacent pixels, N is the number of pairs (xi, yi) and E(x) is the mean of xi and E(y) is the mean of yi.

D. Differential Analyses

NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) measures the invulnerability of an algorithm against the differential attacks on image. NPCR evaluates the pixels change rate in the coded image after modification in one pixel of a prime image, consequently, high NPCR value is effective. Furthermore, UACI computes the variation in intensity of the corresponding pixel of the plain image and the encrypted image. If C1 and C2 are the two cipher image after and prior to 1 bit change in the original image, then NPCR and UACI can be calculated by following formula (6) and (7) respectively.

$$NPCR = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \ \times 100\ \% \ , \quad (6)$$

With if C1 (i, j) = C2 (i, j), then D (i, j) = 0 else D (i, j) = 1,

$$UACI = \left[\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C1(i,j) - C2(i,j)|}{255}\right] \times \frac{100\ \%}{M \times N}, \quad (7)$$

Where, M and N are the dimension and (i, j) is the coordinates of the image.

E. Mean Square Error (MSE)

The mean square error (MSE) is the squared norm of the difference between the data and the approximation divided by the number of elements. The mean square error between a signal or image, X, and an approximation, Y, is the squared norm of the difference divided by the number of elements in the signal or image:

$$\frac{||X - Y||^2}{N} \quad (8)$$

F. Peak Signal to Noise Ratio (PSNR)

PSNR is the peak signal-to-noise ratio in decibels (dB). The PSNR is only meaningful for data encoded in terms of bits per sample, or bits per pixel. For example, an image with 8 bits per pixel contains integers from 0 to 255.

The following equation defines the PSNR:

$$20\log_{10}\left(\frac{2^B - 1}{\sqrt{MSE}}\right) \quad (9)$$

Where MSE represents the mean square error and B represents the bits per sample.

G. MaxErr

Maximum absolute squared deviation of original and decrypted image.

H. L2RA

Ratio of squared norm of the original and decrypted image.

IV. RESULTS AND DISCUSSION

To validate the effectiveness of the algorithm and in order to compare and evaluate both the techniques, which each technique consider as independent scrambling encryption technique, the same digital images will be used. The proposed techniques tested over 50 different database images of different classes. The table I shows some test images used in this paper for evaluation.

Table 4.1: Test images used in this paper

Test Images (Class)	Image format	Image size (KB)	Pixels
Test image 1(Class of Birds)	TIFF	118	384x256
Test image 2 (Class of Fruits)	JPEG	511	768x576
Test image 3 (Grayscale images)	JPEG	17.1	256x256

The performance and security parameters such as Entropy, Correlation, Peak signal to noise ratio, Mean square error, a Maximum absolute squared deviation of original and decrypted image, Ratio of squared norm of the original and decrypted image are calculated. The results of few different database images are shown below.

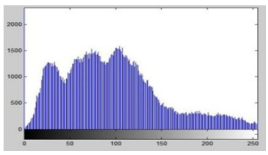
Figure 4.1 to figure 4.3 shows various test images used for experimental analysis of digital image scrambling encryption. Each test image contains part I (a) original image, (b) scrambled image, (c) decrypted image, (d) histogram of original image (e) histogram of scrambled image (f) histogram of decrypted image results for Arnold transformation, and part II (g) original image, (h) scrambled image, (i) decrypted image, (j) histogram of original image (k) histogram of scrambled image (l) histogram of decrypted image results for random permutation. Comparson can be done visually as well as quantitatively.

I. Results for Image Scrambling Encryption using Arnold Transformation

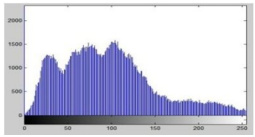
(a) Original Image

(b) Scrambled Image

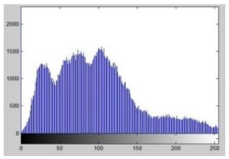
(c) Decrypted Image



(d) Histogram of original Image



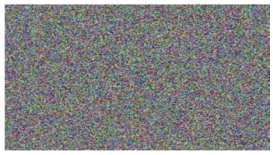
(e) Histogram of Scrambled Image



(f) Histogram of Decrypted Image

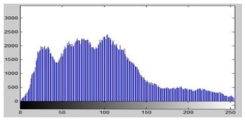
II. Results for Image Scrambling Encryption using Random Permutation

(g) Original Image

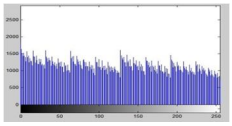


(h) Scrambled Image

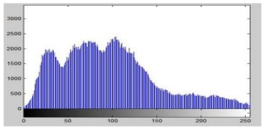
(i) Decrypted Image



(j)Histogram of Original Image



(k)Histogram of Scrambled Image



(l)Histogram of Decrypted Image

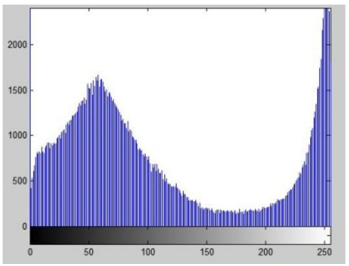
Figure 4.1: Test Image: Bird 1.tif

I. Results for Image Scrambling Encryption using Arnold Transformation

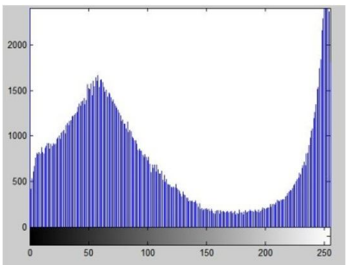
(a) Original Image

(b) Scrambled Image

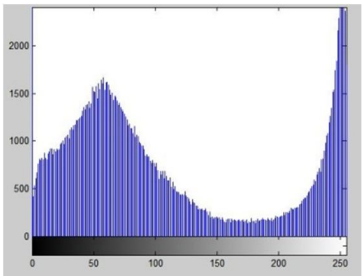
(c) Decrypted Image



(d) Histogram of original Image



(e) Histogram of Scrambled Image



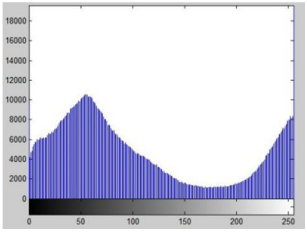
(f) Histogram of Decrypted Image

II. Results for Image Scrambling Encryption using Random Permutation

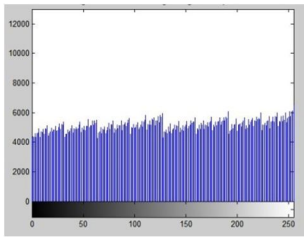
(g) Original Image

(h) Scrambled Image

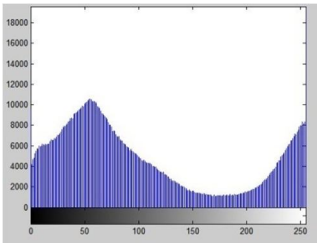
(i) Decrypted Image



(j)Histogram of Original Image



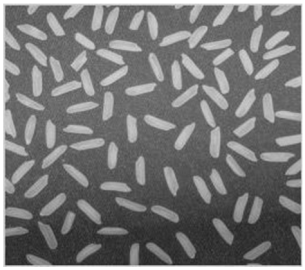
(k)Histogram of Scrambled Image



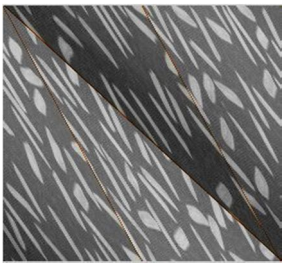
(l)Histogram of Decrypted Image

I. Results for Image Scrambling Encryption using Arnold Transformation

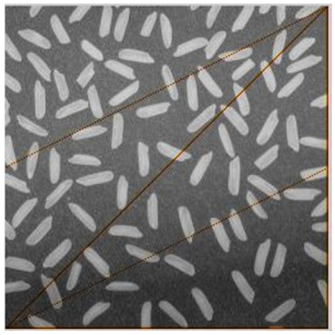
Figure 4.2: Test Image: Fruit 2.jpg



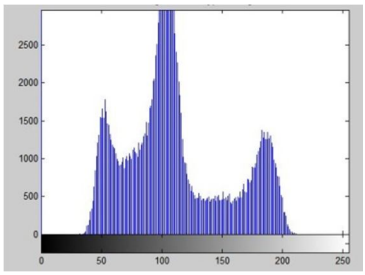
(a) Original Image



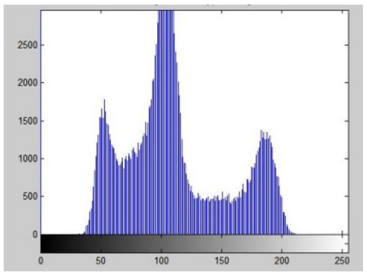
(b) Scrambled Image



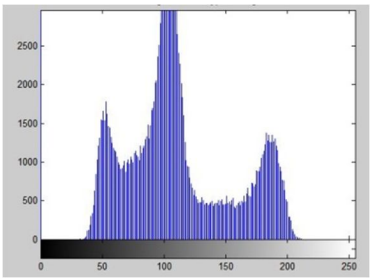
(c) Decrypted Image



(d) Histogram of original Image

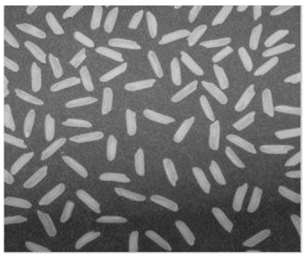


(e) Histogram of Scrambled Image

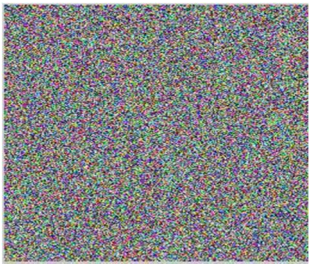


(f) Histogram of Decrypted Image

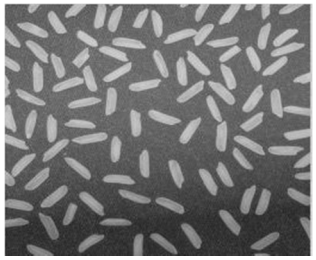
II. Results for Image Scrambling Encryption using Random Permutation



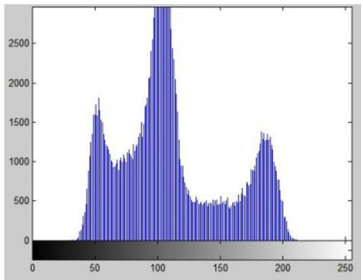
(g) Original Image



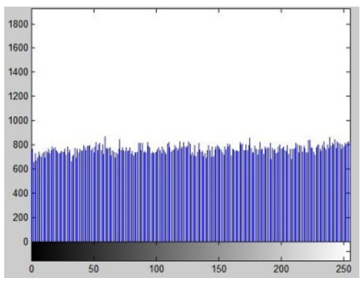
(h) Scrambled Image



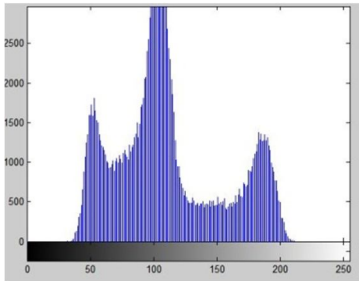
(i) Decrypted Image



(j)Histogram of Original Image



(k)Histogram of Scrambled Image



(k)Histogram of Decrypted Image

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

Figure 4.3: Test Image: Rice.jpg

By visually observing the entire test images viz. Bird 1.tif (figure 4.1), Fruit 2.jpg (figure 4.2), Rice.jpg (figure 4.3), it is clearly observed that the scrambled image and decrypted image of random permutation scrambling encryption is good as compared with Arnolds transformations scrambled image and Decrypted image respectively. By comparing the histograms of scrambled image of both techniques we observed that the Arnold transform histogram of scrambled image is not uniform as random permutation scrambled image histogram which is initial security parameter of scrambling encryption.

Table 4.2 to table 4.4 gives performance and security characterization results for each respective test image. Each table reflects assessment parameters as information entropy (original and cipher), correlation (original and cipher), mean square error, peak signal to noise ratio, number of pixels change rate, unified average changing intensity, maximum absolute squared deviation of original and decrypted image, ratio of squared norm of the original and decrypted image for Arnolds transform, random permutation scrambling encryption. These performance values obtained in both of the techniques are compared with each other and a comparative analysis of both of the techniques is derived.

Table 4.2: Performance & Security Parameter Results for Image: Bird1.tif

Parameters		Arnold Transform	Random Permutation
Entropy	Original	7.6541	7.6552
	Scrambled	7.6603	**7.9821**
Correlation	Original	0.9013	0.9321
	Scrambled	0.7814	**0.0027**
PSNR (db)		26.3690	**Inf.**
MSE		150.0277	0.00
Maxerr.		237	0.00
L2rat		0.9877	1.00
NPCR (%)		99.49	**99.58**
UACI (%)		24.22	**30.37**

Experimental results obtained in table 4.2 (for Bird 1.tif) shows that entropy of scrambled image of Arnolds transform is less than the Scrambled image of random permutation, the correlation coefficient of random permutation is near to zero. Peak signal to noise ratio of decrypted image of random permutation are greater than decrypted image of Arnold transform. Also mean square error, maximum absolute squared deviation of original and decrypted image is less in random permutation scrambling encryption. Ratio of squared norm of the original and decrypted image is satisfactory in random permutation. Computed Number of pixels change rate and unified average changing is grater and acceptable in random permutation scrambling encryption.

Table 4.3: Performance & Security Parameter Results for Image: Fruit 2.jpg

Parameters		Arnold Transform	Random Permutation
Entropy	Original	7.6222	7.5637
	Scrambled	7.6221	**7.9959**
Correlation	Original	0.8896	0.9235
	Scrambled	0.8133	**0.0003**
PSNR (db)		28.7542	**Inf.**
MSE		86.6270	0.00
Maxerr.		223	0.00
L2rat		0.9955	1.00

NPCR (%)	98.86	**99.60**
UACI (%)	17.23	**36.41**

In table 4.3 (for Fruit 2.jpg) all the parameters show good results for random permutation scrambling encryption. The entropy, correlation, peak signal to noise ratio is greater in random permutation. Mean square error maximum absolute squared deviation of original and decrypted image is less in random permutation scrambling encryption. Number of pixels change rate and unified average changing intensity is good in Arnold's transformation but is not better than random permutation scrambling encryption. Ratio of squared norm of the original and decrypted image is satisfactory in random permutation.

Table 4.4: Performance & Security Parameter Results for Image: Rice.jpg

Parameters		Arnold Transform	Random Permutation
Entropy	Original	7.0574	7.0574
	Scrambled	7.0662	**7.9983**
Correlation	Original	0.7082	0.7082
	Scrambled	0.3845	**0.0017**
PSNR (db)		25.8838	**Inf.**
MSE		167.7621	0.00
Maxerr.		204	0.00
L2rat		0.9881	1.00
NPCR (%)		98.98	**99.61**
UACI (%)		18.63	**28.28**

In table 4.4 (for Rice.jpg) the entropy, peak signal to noise ratio is greater in random permutation. Mean square error maximum absolute squared deviation of original and decrypted image is less in comparison with Arnold's transformation scrambling encryption. Number of pixels change rate and unified average changing intensity is good in Arnold's transformation but is not better than random permutation scrambling encryption. Ratio of squared norm of the original and decrypted image is satisfactory in random permutation.

Table 4.5: Performance & Security Parameter Results Database Images for random permutation

Parameters		Class of Birds	Class of fruits	Grayscale Images	Class of Flowers	Class of House
Average Entropy	Original	7.72815	7.08655	7.07845	7.08655	7.50395
	Scrambled	7.9855	7.6612	7.98675	7.6612	7.97485
Average Correlation	Original	0.914	0.9467	0.7668	0.9467	0.93625
	Scrambled	0.0005	0.00175	0.0019	0.00175	0.00135
Avg. PSNR (db)		Inf.	Inf.	Inf.	Inf.	Inf.
Avg. MSE		0.00	0.00	0.00	0.00	0.00
Avg. Maxerr.		0.00	0.00	0.00	0.00	0.00
Avg. L2rat		0.95	1.00	0.91	1.00	0.86
Avg. NPCR (%)		99.6	99.54	99.60	99.37	99.59
Avg. UACI (%)		34.59	32.89	29.67	31.48	33.68

Table 4.5 shows the average calculated values of performance and security parameters viz. Average Entropy, Average Correlation, Average Peak signal to Noise Ratio, Average mean square error, average Maxerr., Average L2rat, average number of pixel change

rate and average unified average changing intensity for the random permutation scrambling encryption technique. The table 4.5 shows the calculated values for the different database images of classes of images viz. Class of Birds, class of fruits, class of flowers, grayscale images and class of house. The entropy of the Scrambled image of random permutation is near to 8 bits, the correlation coefficient of random permutation is near to zero. Peak signal to noise ratio of decrypted image of random permutation is good. Also mean square error, maximum absolute squared deviation of original and decrypted image is less in random permutation scrambling encryption. Ratio of squared norm of the original and decrypted image is satisfactory in random permutation. Computed Number of pixels change rate is above 99.31% and unified average changing is above 32.89% and which is acceptable.

Table 4.6: Comparison of Image Scrambling Techniques

Criteria	Arnolds transformation	Random permutation
Basic process unit	Pixel	Can be pixel or small block or macro cells
Area	Can be done only on square images	Can be done to image of any shape
Scrambling times	Depends on the number of pixels of the image	Can be scrambled any number of times
Image reassembly	Can be done by continuing the same process of scrambling	Can be done by reversing the scrambling process
Key space	Small	Large
Key sensitivity	Low	High
Security	Low, as the number of scrambling depends on the number of pixels used	High, as the different number of scrambling can be done on the different parts of image

V. CONCLUSIONS

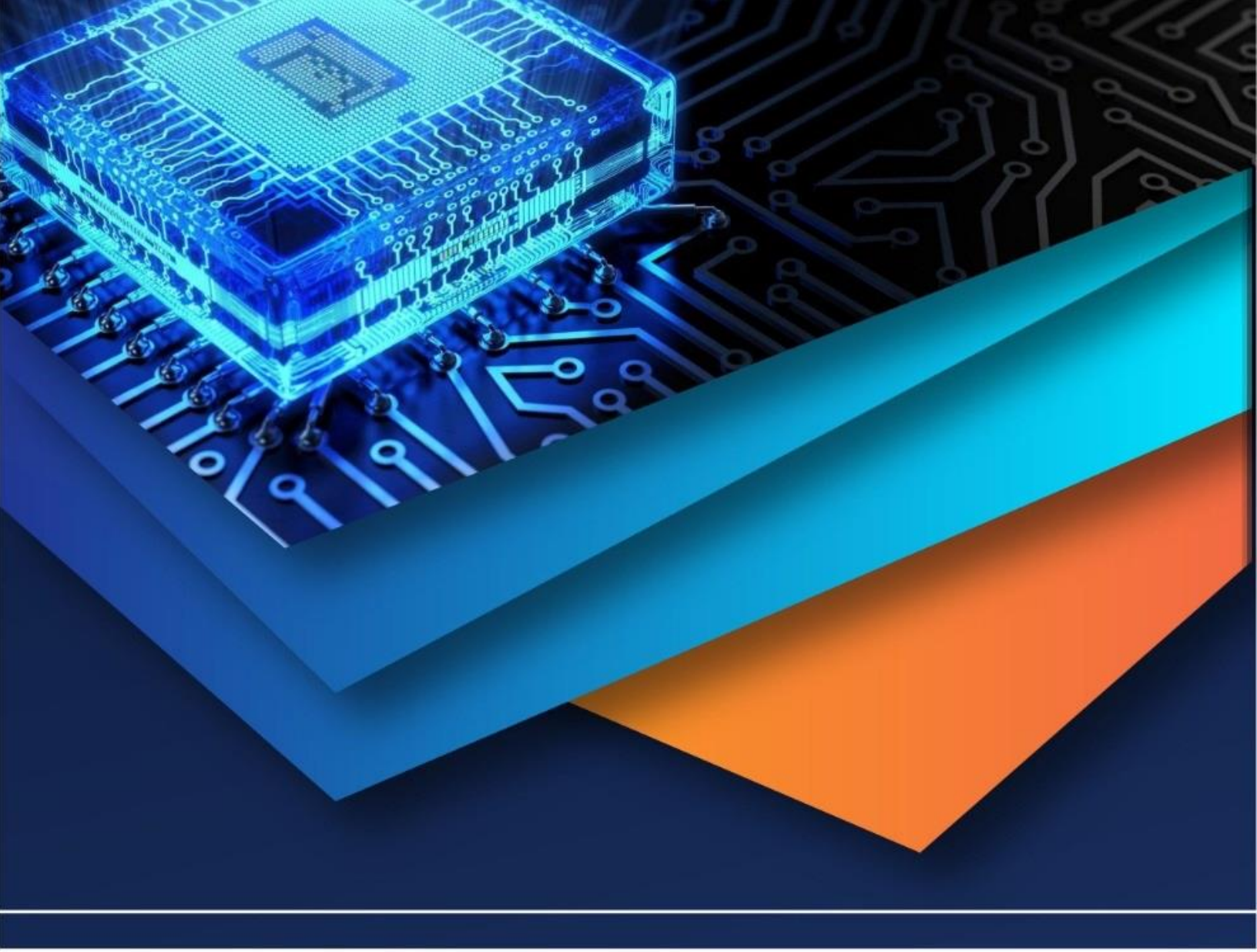
In this paper, we have presented digital image scrambling encryption techniques viz. Image scrambling encryption using Arnold's transformation and random permutation. Experimental studies were conducted by applying both scrambling encryption techniques. The effectiveness of proposed method is validated by statistical analysis, visual testing, entropy analysis, and differential analysis which have been presented in previous section.

It is found that the correlation between adjacent pixels of encrypted image is very close to zero. The obtained entropy value is approximately matches with the standard value 8 bits. The computed PSNR value for proposed method is also greater than Arnolds Transformation. The computed NPCR value is acceptable and is greater than 99.5%. The UACI value is greater than 33% for random permutation scrambling encryption. The random permutation scrambling encryption minimizes the possibility of statistical, differential and entropy attacks. The proposed method Scrambling Encryption using Random Permutation is suitable for real time data transmission. The decryption process is performed to confirm the reception of original image.

REFERENCES

[1] Gonzalviz Woods " Digital Image processing book".
[2] Yan, WeiQi, and Jonathan Weir, Fundamentals of Media Security. Bookboon, 2010.
[3] Zhao Xue-feng, "Digital image scrambling based on the baker's transformation". Journal of Northwest Normal University (Natural Science),vol.39, pp26-29, February .2003.
[4] Wenquing Chen, Tao wang and Bailing Wang, "Design of Digital Encryption Algorithm Based on chaotic Sequences" International Journal on smart Sensing and Intelligient Systems Vol. 7, no. 4,December 2014.
[5] P. Premaratne and M. Premaratne, "Key-based scrambling for secure image communication," in Emerging Intelligent Computing Technology and Applications, P. Gupta, D. Huang, P. Premaratne and X. Zhang, Ed. Berlin: Springer, 2012, pp.259-263.
[6] Zhenwei Shang, Honge Ren, Jian Zhang. "A Block Location Scrambling Algorithm of Digital Image Based on Arnold Transformation". The 9th International Conference for Young Computer Scientists, 2008.
[7] Shiva Shankar S., A Rengarajan, "Data Hiding In Encrypted Images Using Arnold Transform," ICTACT Journal On Image And Video Processing, Volume: 07, Issue: 01, August 2016.
[8] Vineeta Singh, Vipin Dubey, "A Two Level Image Security based on Arnold Transform and Chaotic Logistic Mapping," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 2, February 2015.
[9] Jiancheng Zou , Rabab K. Ward , Dongxu Qi, "A New Digital Image Scrambling Method Based on Fibonacci Number," Proceeding of the IEEE Inter Symposium On Circuits and Systems,Vancouver ,Canada ,Vol .03 , PP .965-968 , 2004.
[10] Shao Z. Qin, B. Liu J. Qin and H Li., "Image Scrambling Algorithm Based on Random Shuffling Strategy", in ICIEA 2008, pp. 2278-2283.

[11] Makera M Aziz, Dena Rafa Ahemad "Simple Image Srambling Algorithm Based on Random Number Generation" IJARCSSE, volume 5, issue 9,September 2015.
[12] Shuqun Zhang and Mohammed A. Karim, "Color image encryption using double random phase encoding", Microwave and Optical Technology Letters Vol. 21, No. 5, 318-322 , June 5 1999.
[13] W.Chen, C.Quan and C.J.Tay. "Optical Color Image Encryption based on Arnold Transform and Interference Method", Optics Communications, Vol. 282, No. 18, pp. 3680-3685, 2009.
[14] S.Liping,Qin, Z. Liu Bo, Q. Jun, L.Huan," Image Scrambling Algorithm Based on Random Shuffling Strategy" 3rd IEEE Conference on Industrial Electronics and Applications, 2008,pp. 2278 – 2283.
[15] Ravi Praksh Devangan et.al, " Image Encryption using Random Permutation by Different Keys" International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 10, October 2015.
[16] T. Shivakumaar and R. Venkateshan,"A New Image Encryption Method Based on Knights Travel Path and True Random Number" Journal of Information Science and Engineering 32, 133-152 (2016) .
[17] Khalid Hamdnaalla, Abubaker Wahaballa, Osman Wahballa, " Digital Image Confidentiality Depends upon Arnolds Transformation and RC4 Algorithms" International journal of Video & Image Processing and Network Security IJVIPNS-IJENS volume 13, No. 04. August 2013.
[18] K s tamilkodi and dr. (mrs) n rama,"a comprehensive survey on performance analysis of chaotic colour image encryption algorithms based on its cryptographic requirements" international journal of information technology, control and automation (ijitca) vol.5, no.1/2, april 2015.
[19] Shrija Somaraj and Mohammed Ali Hussain "Performance and Security Analysis for Image Encryption using Key Image" Indian Journal of Science and Technology**,** Vol 8(35), DOI: 10.17485/ijst/2015/v8i35/73141, December 2015.
[20] Osama M. Abu Zaid , Nawal A. El-Fishawy , and E. M. Nigm**,"** A PROPOSED PERMUTATION SCHEME BASED ON 3-D CHAOTIC SYSTEM FOR ENCRYPTING THE COLORED IMAGES" IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 2, July 2013ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784.
[21] Chandel, Gajendra Singh, and Pragna Patel. "Image Encryption with RSA and RGB randomized Histograms." Image 3, no. 5 (2014).
[22] H.Yuan and L.Jiang " Image Scrambling based on Spiral Filling of Bits" International Journal of Signal Processing, Image Processing and Pattern Recognition , vol.8, pp.225-234 , March. 2015.
[23] L.Anguan, W. Sheng, Z. lie" A New Method for Image Information Hiding Based on Image Scrambling and LSB Technology" International Conference on Computer Application and System Modeling 2010 ,pp 349-355.
[24] B.Radu, D. Cristina, P.Iustin and F. Cristina "A New Fast Chaos-Based Image Scrambling Algorithm" 10th international conference on communication , 2014, , pp 1-4.
[25] A. A. Abd El-Latif, L. Li, N. Wang, X. Niu, "Image encryption scheme of pixel bit based on combination of chaotic systems," in Proceedings of 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP'11), pp. 369-373, 2011.
[26] Yang Zou, Xiaolin Tian, Shaowei Xia, and Yali Song. "A Novel Image Scrambling Algorithm Based on Sudoku Puzzle," Proceedings of the Fourth International Congress on Image and Signal Processing, Vol. 2, October 2011.
[27] Yunpeng Zhang, 2Peng Sun, 1Liang Yi, 1Yongqiang Ma and 1Ziyi Guo, "Analysis and Improvement of Encryption Algorithm Based on Blocked and Chaotic Image Scrambling" Research Journal of Applied Sciences, Engineering and Technology 4(18): 3440-3447, 2012.
[28] M. Al-Husainy " A Novel Encryption Method for Image Security" International Journal of Security and Its Applications",vol. 6 ,January. 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY