International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

A Substitute Method for Color Image Enciphering based on Cell Shuffling and Scan Pattern

Chandra Prakash Singar, Jyoti Bharti, R.K. Pateriya

Abstract*: *In today's world, we use multimedia technologies in various daily applications to send vital information from one end to another side. However, security is a prime concern when data is sent over a public channel. There are various multimedia techniques to transfer data using sound, video, and images. However, these methods are not effective in security and performance. Therefore, we propose an advanced substitute method using cell shuffling and scanning methodology for image encryption. The suggested scheme contains two processes as (1) divide an image into many blocks, and then, its pixel position is rearranged, and (2) the scan pattern is applied to get a more complex image. After that, we do performance and security analysis for the proposed method using the correlation coefficient, information entropy, PSNR, MSE, SNR, number of pixels change rate, average intensity, and unified average change intensity.

Keywords: Scanning Technique, Image Encryption, Scan Pattern, Cell splitting, cell shuffling.

I. INTRODUCTION

Due to the increment of various vision applications, it is essential to preserve the security of information. Generally, encryption techniques are used to ensure secure communication between two parties over a public channel, and thus, unauthorized users are not able to understand transmitted information from one side to another end. Further, encryption achieves highly conceivable outcomes due to its advanced research innovation. In this method, the system does changes into the original images by over cryptic image, and thus, it is hard to retrieve information from these encrypted images without knowing the private key [9]. There are various applications (e.g., web correspondence, communication, teleconferencing, military communication, video broadcasting, etc.) in which image and video encryption mechanism are used to protect vital information from attackers using some cryptographic techniques [5],[19].

Cryptography is a process to preserve information and communications by using the concept of some coding, and thus, only legitimate users can understand it to proceed further. Moreover, it performs encryption and decryption operations to convert the original message into the cipher text and to get back the plain text from the encrypted message respectively [17]. There are well-known public and private key cryptography techniques, e.g., Data Encryption Standard (DES), Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), Diffie–Hellman (DH) key exchange, etc[7] [9].

A. Image Encryption

An image stores different property (i.e., access, a high correlation among the pixels, size, etc) inside it and it can be extracted after performing some operations. Therefore, image encryption is especially a useful process to store data securely and it makes information as unreadable to unauthorized users. After that, an encrypted image (encoded a plain message) is sent to the receiver party over an insecure medium. Then, the receiver does the decryption to get back the original plain-text message. In this, the decryption procedure is the exact reverse step-by-step process when the system uses symmetric key cryptography [16].

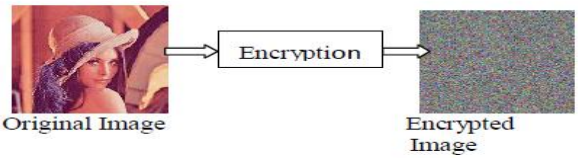


Fig.1.Image Encryption [19]

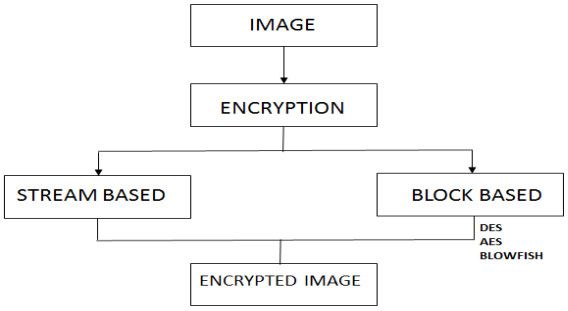


Fig.2. Encryption methods [27]

Manuscript published on November 30, 2019.
* Correspondence Author
***Chandra Prakash Singar**, Ph.d Schollar in Department of computer science and Engineering, MANIT Bhopal, 462003 India. E-mail: chandraprakash.singar@gmail.com
Dr. Jyoti Bharti, Assistant professor in Department of computer science and Engineering, MANIT Bhopal, 462003 India. E-mail: jyoti2202@gmail.com
Dr.R.K.Pateriy, Associate professor in Department of computer science and Engineering, MANIT Bhopal, 462003 India. E-mail: pateriyark@gmail.com

Fig.1 shows an encrypted image (of original image) after applying cryptographic technique. Due to the usage colourful images, the concept of colour image encryption is widely used in the market to preserve significant information.

Further, colour images contain more pixels rather than black and white images and this helps in the encryption system to enrich the security level. When colour image encryption technique can be performed in two steps as stream based and block based encryption [25]. Fig.2 displays a chart diagram to get an encrypted image from a normal image. The stream based encryption is applied bit by bit on the image. The image transformation procedure is carried out based on blocks [18].

B. Scanning Techniques

An image is formed of pixels in a two dimensional array and it is produced in a different state of pixels. Scanning is a formal language using two-dimensional spatial-accessing procedure to represent and generate a picture of different sequences [22]. This exploring process is known as SCAN and it is a special purpose context-free language. Mostly, the system uses SCAN in the encryption and compression methods for images [15].

C. Scan

An image is a collection of pixels to arrange it in a matrix form and then, it is represented as a 2-D array. Scanning of a 2-D array is defined as the sequential representation of an image element, and SCAN is used to compose a 2-D array. Further, this system uses the recursive decomposition of a picture based on the hierarchical levels [27]. A 2-D array scanning process is described using a mathematical equation as follows.

$$P_{m\times n} = \{p(i,j): 1 \le i \le m, 1 \le j \le n\} \quad (1)$$

Pictorial Representation of SCAN technique

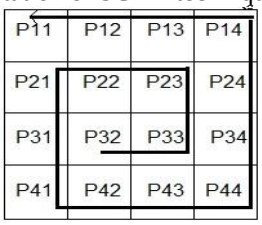


Fig.3.Spiral out scanning

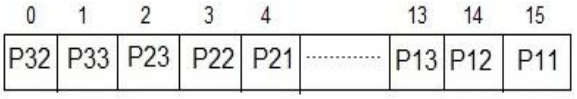


Fig.4. Array representation of Spiral out scanning

Fig.3 dictates the pictorial representation of "Spiral Out" scanning and here, pixels are denoted by P. Fig.4 shows a 1-D array representation of Fig.3. The paper is discussed in a following manner: Section 2 discuss different features and issues of various encryption techniques. We propose a novel encryption- based scanning system in Section 3. After that, we analyze and do the comparison of the proposed system with existing techniques in Section 4. Finally, our conclusions are described in Section 5.

II. LITERATURE SURVEY

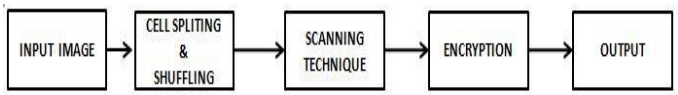
M.Zeghid and Machhout analyzed the AES algorithm, and then they proposed an image encryption scheme by using a key stream generator (A5/1, W7) to AES for the security enhancement [1]. Mohammed and Bani Younes introduced a block-based change algorithm by changing images and this method is known as Blowfish. In this scheme, the first image is isolated into blocks to improve into a transformed picture based on a transformation algorithm. Moreover, the processed image is encoded using the Blowfish method. However, the outcome of this process is reduced the correlation between image components. Further, they noticed that when the block quantity is expanded using smaller block sizes, it achieves higher entropy, but lower correlation [2]. Saroj Kumar and Panigrahy came up with an image encryption based scheme on the Hill cipher and in this method; a self-invertible matrix is generated for Hill cipher estimation. Moreover, they used this key matrix to encode gray scale and color images. The performance result is preferable of this system for gray scale images, but it produces blur images in the case of color images [3]. Amitava Nag designed a two stage method to perform encryption/decryption operations for images and in this approach, the system does rearrangement of picture pixels using affine transform and then, they apply an XOR operation for the subsequent picture. Moreover, the resultant image is processed by distributing pixels again to different parts of an image [17]. Reza Moradi et al suggested an efficient image encryption mechanism by using the XOR operation and scanning pattern at three different stages. Moreover, they use the symmetric key cryptography in this mechanism, and thus, the decryption process is the same as the encryption procedure, but it is applied in a reverse manner [20]. T.Sivakumar and R.Venkatesan designed a new image encryption method using based on framework reordering and XOR operation to encode images using the Matrix Reordering (MR) system. The primary motivation of behind the MR system and XOR operation is to fix pixel positions correctly and to diffuse the pixel esteems, respectively [21]. In 2014, T.Sivakumar suggested an image encryption scheme using random nonce and z-order bend to enhance the security level of images. This scheme achieves a certain security level due to the addition of noise during the process, and thus, this system can withstand differential and statistical attacks [24]. Seyed mohammad et.al suggested the algorithm is to use one half of image data for encryption of the other half of the image reciprocally that is based on hash function [6].

After that, T.Sivakumar and R.Venkatesan came up with a different image encryption protocol using a genuine irregular number and light of knight's travel way (based on pixel scan and travel path). Here, the Knight's travel path is used to identify the pixel spots of the primary image to a blended image. After that, an XOR operation is performed of this blended image and random key numbers to get the cipher image [26].

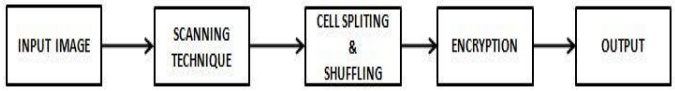
H.T. Panduranga suggested a cross-breed image encryption scheme using a scan pattern and carrier image. However, this method is feasible for image encryption [8]. In this work a novel advanced HILL encryption method has been proposed for an involuntary key matrix. This method is a fast encoding scheme which overcomes problems of encrypting the images with homogeneous background [4]

III. PROPOSED WORK

The fundamental thought of our new mechanism is to encode the original image using a block rearranging process and scan pattern. Here, the position of pixels position is changed based on spiral wave and raster spiral scanning patterns. Fig.5 shows the working process of the suggested method. The proposed method performs two alternate ways. In the first part, the original picture is separated into N number of blocks; and the image structure is changed after shuffling of blocks; and after that, the scan pattern is applied. In a second way, the scan pattern is performed before doing cell splitting and shuffling.



(a) Block diagram of process 1



(b) Block diagram of process 2

Fig.5. Proposed block diagram of (a) process 1 and (b process 2

In general, scanning algorithms are used to generate more disturbing images so that unauthorized users cannot understand from images. Next, the position of pixels is changed after doing the rearrangement based on a specific pattern, and this gives an intricate image, which is generally not the same as the original image. Fig. 6 and Fig. 7 display the original matrix of spiral wave scan pattern and raster spiral scan respectively. Fig.8 dictates the cell splitting and shuffling process for images.

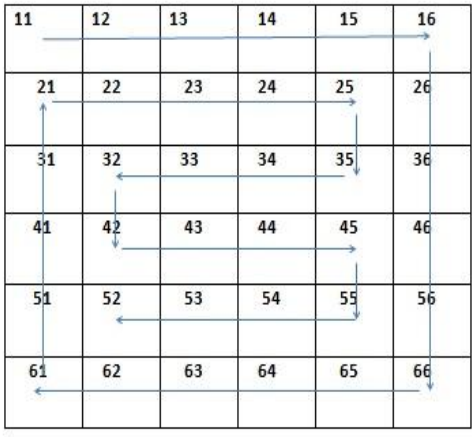


Fig.6. Spiral wave scan pattern

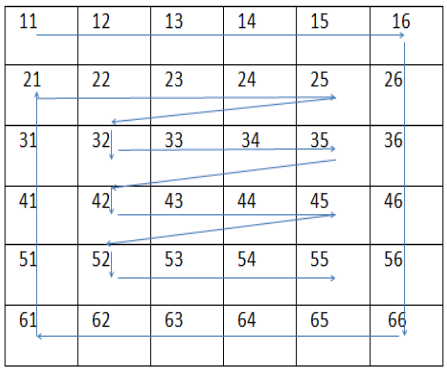


Fig.7.Raster spiral scan pattern

Our proposed scheme uses two different scanning techniques (i.e., spiral wave scan and raster spiral scan). We use these two techniques to change the pixel position, and this is shown in Fig.6 and Fig.7 sequentially. The scanning position is interchanged with cell splitting in raster spiral scan. We can state from these figures that encrypted images are totally different, and it is hard to get from these encrypted images.

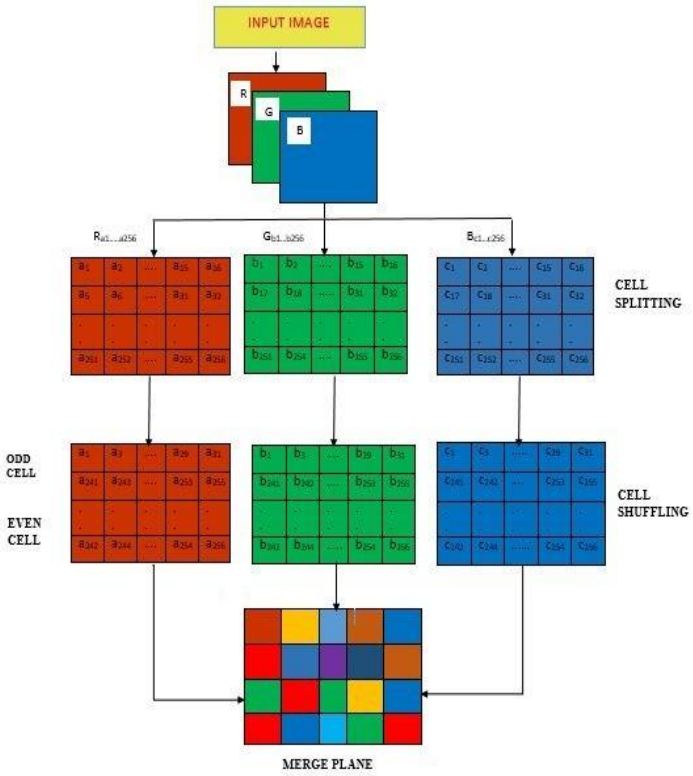


Fig.8.Cell splitting and cell shuffling

Proposed Methodology

Step1: Take RGB image as input of size M*N
Step 2: Separate RGB image into three separate plane R,G and B then split each plan into 16 *16 block, so size of each block will be 16 * 16 there index will be a0 – a15.

// a0 –a15 is block indexing after cell splitting in fig.8

$R = M_R * N_R$ // Size of the red plane
$G = M_G * N_G$ // Size of the green plane
$B = M_B * N_B$ // Size of the blue plane

Step 3: Cell Splitting
3.1. Get the width and height of the plane
3.2. Horizontal number of block (H_n) = image width / [X]
3.3. Vertical number of block (V_n) = image height / [X]

3.4. Find Total number of block (N)

$$N = \frac{Hn * Vn}{[X]}$$

3.5. The size of each plane is 512*512(W*H) dividing the image plane into 'n' equal number of blocks.
3.6. Size of each block is [X] and the blocks generated are as follows:

$$N = \frac{Hn * Vn}{[X]}$$

// Hn is number of horizontal block
// Vn is number of vertical block
// Where [X] = Size of each block

So calculate X

$$256 = (512 * 512) / X$$
$$X = 32 * 32$$

So we get 256 equal blocks of size 32 * 32.
3.7. The plane contain 16*16 block both in horizontal and vertical direction.
3.8. Repeat steps 3.1 to 3.7 to all Red, Green and Blue planes.
3.9. Merge the Red, Green and Blue planes.

Step 4: Apply Scanning techniques according to process 1 and process 2
Step 5: Apply Encryption algorithm according to process 1 and process 2
Encryption algorithm:

- Pick any of the images from subset that will be an input image for the next step.
- Input an image.
- To encrypt the image three keys (key1, key2, key3) are required .This will be created randomly using function "rand ()".
- Convert the input image matrix img1 into double precision image matrix "pic".
- Divide the image matrix pic obtained by key1.
- Calculate element by element for product of the above matrix with key 2.
- Add key 3 to the resultant image matrix and then there will get new encrypted image as Crypt Pic.
- Again convert the final image matrix value into 8 bit unsigned integer.
- Finally, we get an encrypted image.

IV. IMPLEMENTATION AND RESULTS ANALYSIS

The proposed method is executed on the system, which is configured as 2.80 GHz P-IV Processor, 2 GB RAM, 180 GB HDD. Moreover, we have used Matlab 2013 on Windows 7 (64-bit) operating system. We have implemented the proposed encryption scheme for three color images (e.g., "Lena", "Peppers", and "Baboon") of 512 x 512 sizes. Performance results are shown in Table 1, 2, 3, and 4. Specifically, encrypted and decrypted images (of the first process) are shown in Table 1 and 3 for spiral wave scan and raster spiral scan. Similarly, Table 2 and 4 show encrypted and decrypted images (of the second process) for spiral wave scan and raster spiral scan. Table 5 and 6 describe different results for spiral wave scan and raster spiral scan respectively.

Table- I: Process 1 encrypted image and decrypted image

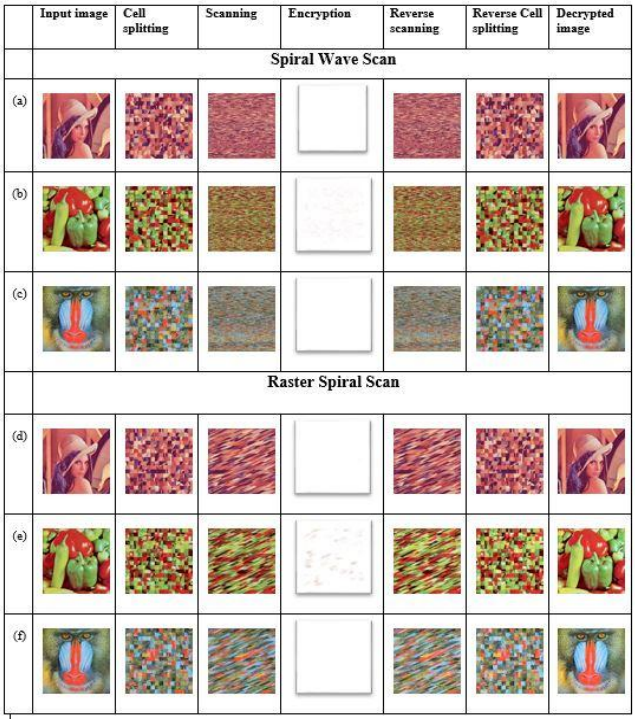


Table- II: Process 2 encrypted image and decrypted image

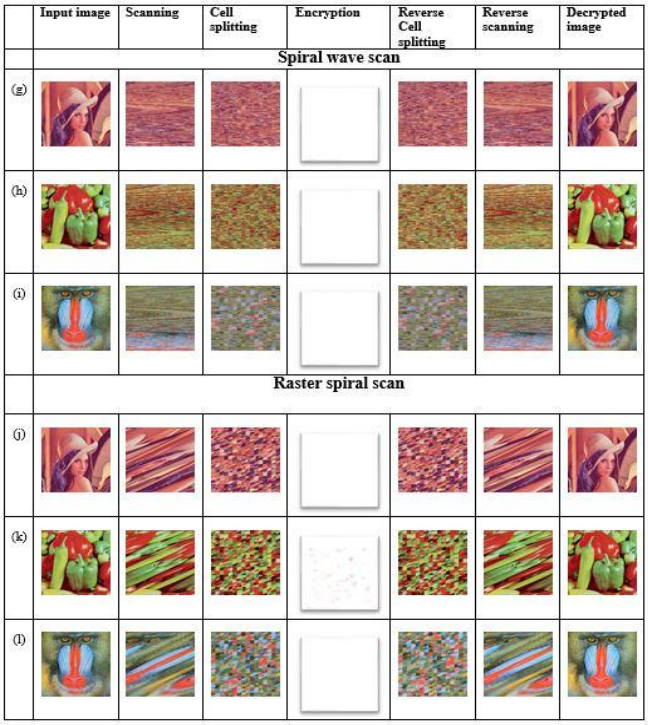


Table- III: Process 1 histogram analysis

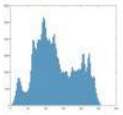
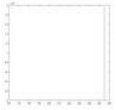
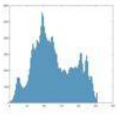
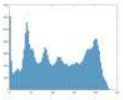
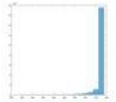
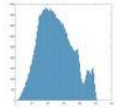
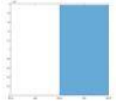
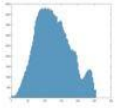
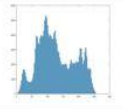
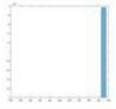
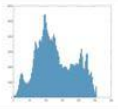
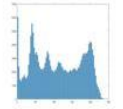
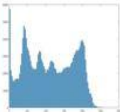
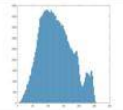
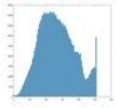
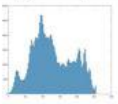
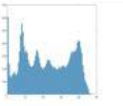
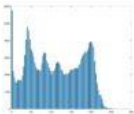
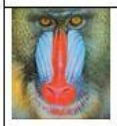
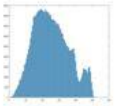
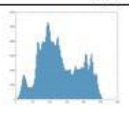
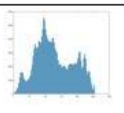
Process 1 Spiral Wave Scan			
Image	Original Histogram	Encrypted Histogram	Decrypted Histogram
			
			
			
Process 1 Raster Spiral Scan			
			
			
			

Table- IV: Process 2 histogram analysis

Process 2 Spiral wave scan			
Image	Original Histogram	Encrypted Histogram	Decrypted Histogram
			
			
			
Process 2 Raster Spiral Scan			
			

Security Analysis

Now, we discuss the security strengths of the suggested method to verify its impact against various security attacks. In a case of visual attacks, encrypted images are generated after performing various operations of the suggested method, and thus, it is hard to retrieve visual information from an encrypted picture. The correlation coefficient and histograms are generated for both (encrypted and original) images. Further, an intruder cannot extract any values from encrypted images, and thus, the proposed scheme can resist a statistical attack. The estimation of a number of pixel change rate (NPCR) and unified average change intensity (UACI) are required to perform differential attacks. However, an adversary cannot retrieve any information from encrypted images because the encrypted image is not the same as the original image. To know the pixel change rate of an encrypted image, we have measured the number of pixels based on the number of pixel change rate and the unified average changing intensity. Generally, NPCR and UACI values should be large enough to protect against differential attacks, and this property is satisfied in the proposed system. Moreover, NPCR and UACI are 99.60 and 33.46 respectively for the suggested method, and it is discussed in Table VIII and Table XI. Results of the proposed method show better performance compared to relevant methods, and therefore, it achieves security requirements to preserve confidentiality and integrity.

Correlation Analyses of Two Adjacent Pixels

We have analyzed the correlation for two vertically/horizontally/diagonally nearby pixels on an image. Further, a pair of two adjacent pixels (i.e., vertically/horizontally/diagonally) is randomly chosen from both types of images (i.e., original and encrypted). Moreover, these correlation coefficients indicate the performance results of the suggested method on Lena, Peppers, and Baboon images. The correlation coefficients have the range from ’1’ highly correlated to ’-1’ highly uncorrelated. Furthermore, they ensure that both images (original and encrypted) are statistically .Table VII, IX and X describes the correlation distribution of adjacent pixels in the encrypted image. Fig 9, 10, 11, 12, and 13 display different comparisons, i.e., entropy, mean square error (MSE), peak signal to noise ratio (PSNR), signal-to- noise ratio (SNR), NPCR and UACI respectively based on spiral wave and raster spiral scan patterns. In these results, process 1 is comparatively better rather than process 2. Besides, the resultant image is highly complex, and therefore, it is difficult to extract any information from an encrypted picture.

Table-V: Entropy, MSE, PSNR, SNR, NPCR, UACI values of process-1 and process-2 of spiral wave scan

Spiral wave scan	Image	Entropy	MSE	PSNR	SNR	NPCR	UACI
Process 1	Lena	0.031745	19497.07	5.23111	0.085538	99.60	33.46
	Peppers	0	19255.76	5.285196	-0.11824	99.60	33.46
	Baboon	2.732783	24107.21	4.309333	-1.63408	99.60	33.46
Process 2	Lena	0.029469	19496.77	5.231176	0.085604	99.60	33.46
	Peppers	0.003282	19255.67	5.285217	-0.11822	99.60	33.46
	Baboon	0.726677	25010.38	4.1496	-1.79382	99.60	33.46

Table-VI: Entropy, MSE, PSNR, SNR, and NPCR, UACI Values of process-1 and process-2 of raster spiral scan

Raster spiral scan	Image	Entropy	MSE	PSNR	SNR	NPCR	UACI
Process 1	Lena	0.052741	19496.42	5.231254	0.085682	99.6	33.46
	Peppers	0.004755	19255.69	5.285212	-0.11823	99.6	33.46
	Baboon	2.302299	24102.29	4.31022	-1.6332	99.6	33.46
Process 2	Lena	0.012978	19500.77	5.230286	0.084714	99.6	33.46
	Peppers	0	19255.76	5.285196	-0.11824	99.6	33.46
	Baboon	1.857878	24293.84	4.275842	-1.66757	99.6	33.46

Table-VII: Adjacent Pixel Correlation (Existing Image Encryption Methods)

REFERENCE	Horizontal	Vertical	Diagonal
Adrian et al [22]	0.0002	0.0006	0.0043
Khaled Loukhaoukha et al [13]	0.0068	0.0091	0.0063
Vidhya and Venkatesulu [14]	0.0177	0.0491	0.0034
Panduranga et al [8]	0.0263	0.0163	0.0114
Bani Younes et al. [2]	0.034	0.038	0.0245
G.A.Sathishkumar et al [10]	- 0.0332	0.0608	0.0567
G.A.Sathishkumar et al [12]	- 0.002818	0.006232	0.005763
C.K.Huang and H.H.Nien [3]	0.01776	0.04912	0.00348

Table-VIII: NPCR value of existing methods

REFERENCE	NPCR value (%)
Khaled Loukhaoukha et al [13]	99.5850
G.A.Sathishkumar et al [10]	98.4754
C. K. Huang et al [23]	99.5400
M Bin Younas et al [11]	80.7482
This paper	**99.60**

Table-IX: Adjacent pixel correlation - Proposed method

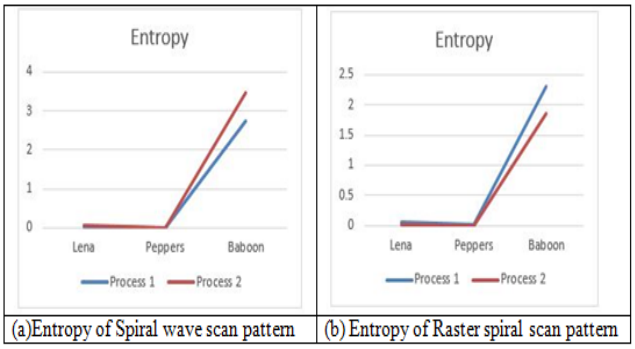
Spiral wave scan	Image	Horizontal	Vertical	Diagonal
Process 1	Lena	0.006009	0.006475	0.005941
	Peppers	NA	NA	NA
	Baboon	0.030644	0.029631	0.03075
Process 2	Lena	NA	NA	NA
	Peppers	0.021469	0.019017	0.021414
	Baboon	0.008982	0.00681	0.00558

Table-X: Adjacent pixel correlation - Proposed method

Raster spiral scan	Image	Horizontal	Vertical	Diagonal
Process 1	Lena	0.002023	0.00214	0.001981
	Peppers	-0.01454	-0.01704	-0.01501
	Baboon	0.022227	0.024575	0.02263
Process 2	Lena	-0.00484	-0.00518	-0.00502
	Peppers	NA	NA	NA
	Baboon	0.032995	0.034233	0.032302

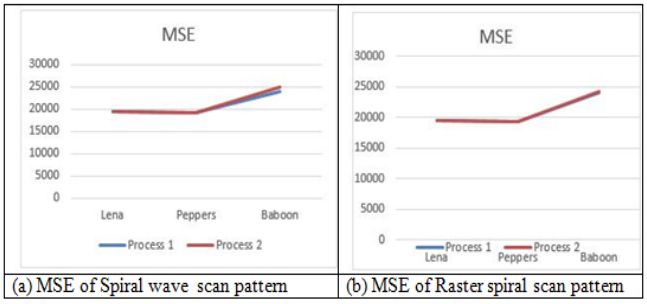
Table-XI: UACI value of existing methods

REFERENCE	UACI Value (%)
Khaled Loukhaoukha et al [13]	28.6210
G.A.Sathishkumar et al [10]	32.2128
C. K. Huang et al [23]	28.2700
Panduranga et al [8]	32.069
M Bin Younas et al [11]	28.9903
This paper	**33.46**



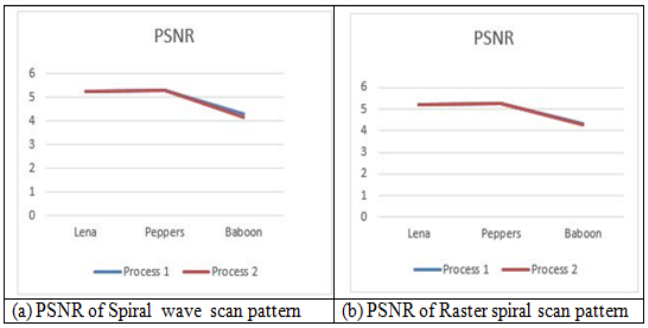
(a)Entropy of Spiral wave scan pattern (b) Entropy of Raster spiral scan pattern

Figure 9: Entropy comparison for process-1 and Process-2



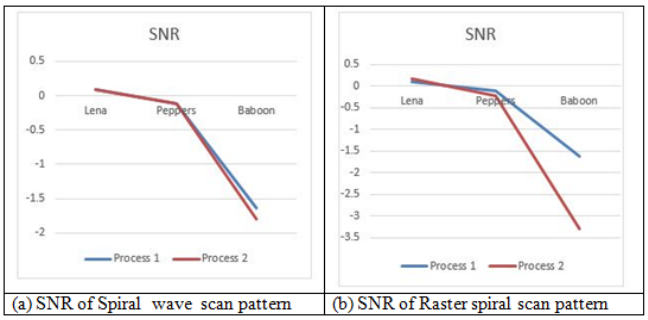
(a) MSE of Spiral wave scan pattern (b) MSE of Raster spiral scan pattern

Figure 10: MSE comparison for process-1 and Process-2



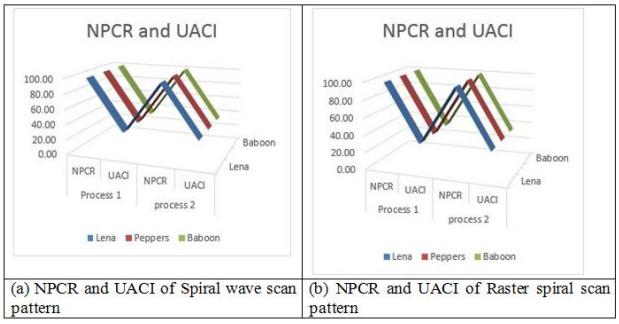
(a) PSNR of Spiral wave scan pattern (b) PSNR of Raster spiral scan pattern

Figure 11: PSNR comparison for process-1 and Process-2



(a) SNR of Spiral wave scan pattern (b) SNR of Raster spiral scan pattern

Figure 12: SNR comparison for process-1 and Process-2



(a) NPCR and UACI of Spiral wave scan pattern (b) NPCR and UACI of Raster spiral scan pattern

Figure 13: NPCR and UACI comparison for process-1 and Process-2

V. CONCLUSION

We have suggested a new substitution image encryption method by using a spiral wave and raster wave scan patterns. Further, we have implemented the suggested scheme on three color images (i.e., Lena, Pepper, and Baboon) to check its performance results. The test-bed results show that our proposed method performs better in terms of security and implementation. Furthermore, the correlation (of horizontal, vertical, and diagonal) is approximately close to zero for the adjacent pixels of the encrypted image using the proposed scheme. Moreover, the suggested method achieves confusion and diffusion properties significantly. Further, the proposed method resists to different security types of attacks, and thus, it meets the confidentiality and integrity of an image. Therefore, the proposed system is helpful to transfer vital information publicly.

REFERENCES

1. M. Zeghid, M. Machhout, L. Khriji, A. Baganne, R. Tourki,"*A Modified AES Based Algorithm for Image Encryption*", World Academy of Science, Engineering and Technology 2007.
2. Mohammad Ali, BaniYounes and Aman Jantan "*Image Encryption Using Block-Based Transformation Algorithm",(*IAENG), International Journal of Computer Science,2008.
3. Saroj Kumar, Panigrahy, Bibhudendra Acharya and Debasish Jen "*Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm*",1st t International Conference on Advances in Computing, Chikhli, India, 21-22, February, 2008.
4. Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda "*Image Encryption Using Advanced Hill Cipher Algorithm",* International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.
5. C. K. Huang and H. H. Nien, "Multi chaotic systems based pixel shuffle for image encryption," *Optics Communications*, Vol. 282, 2009, pp. 2123-2127.
6. Seyed Mohammad, Seyedzade, Reza Ebrahimi, Atani and SattarMirzakuchaki, *"A Novel Image Encryption Algorithm Based on Hash Function",* 6th Iranian Conference on Machine Vision and Image Processing, 2010.
7. William Stallings, *Cryptography and Network Security: Principles & Practices*, second edition,2010.
8. H. T. Panduranga and S. K. N. Kumar, "Hybrid approach for image encryption using SCAN patterns and carrier images," *International Journal on Computer Science and Engineering*, Vol. 2, 2010, pp. 297-300.
9. X. Liao, S. Lai, and Q. Zhou, "A Novel Image Encryption Algorithm based on Self-adaptive Wave Transmission", *Signal Processing*, vol. 90, no. 9, pp. 2714-2722, 2010.
10. G. A. Sathish kumar and K.Bhoopathy Bagan, "A novel image encryption algorithm using pixel shuffling and Base-64 encoding based chaotic block cipher", WSEAS Transactions on Computers, vol. 10, no. 6, 2011, pp. 169-178.
11. M Bin Younas, Jawad Ahmad "*Comparative Analysis of Chaotic and Non-chaotic Image Encryption Schemes*",978-1-4799-6089-7,IEEE 2014,
12. G. A. Sathish kumar, K. Bhoopathy, and R. Sriraam,"Image encryption based on diffusion and multiple chaotic maps," *International Journal of Network Security and its Applications*, Vol. 3, 2011, pp. 181-194.
13. Khaled Loukhaoukha, Jean-Yves Chouinard and Abdellah Berdai, "A secure image encryption algorithm based on Rubik's cube principle", Journal of Electrical and Computer Engineering, Article ID 173931, vol. 2012, 2012, pp. 1-13.
14. P. Vidhya Saraswathi and M. Venkatesulu, "A block cipher algorithm for multimedia content protection with random substitution using binary tree traversal", Journal of Computer Science, vol.8, no. 9, 2012, pp. 1541-1546.
15. Monisha Sharma, Chandrashekhar Kamargaonkar, Amit Gupta, "*A Novel Approach of Image Encryption and Decryption by Using Partition and Scanning Pattern"* International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 7, September – 2012 ISSN: 2278-0181
16. Rasul Enayatifar and Abdul Hanan Abdullah" *Image Security via Genetic Algorithm",* International Conference on Computer and Software Modeling IPCSIT vol.14 (2011) 2011
17. Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh Sushanta Biswas, D. Sarkar, Partha Pratim Sarka "*Image Encryption Using Affine Transform and XOR* Operation", International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011) 2011
18. M. A. B. Younes and A. Jantan, "Image encryption using block based transformation algorithm," *IAENG International Journal of Computer Science*, Vol. 35, 2008, pp. 15-23.
19. Rajinder Kaur, Er.Kanwalprit Singh, *"Image Encryption Techniques: A Selected Review"* IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 6 (Mar. - Apr. 2013), PP 80-83,2013.
20. Reza Moradi Rad, Abdolrahman Attar, and Reza Ebrahimi Atani "A New Fast and Simple Image Encryption Algorithm Using Scan Patterns and XOR" International Journal of Signal Processing, Image Processing and Pattern RecognitionVol.6, No.5 (2013), pp.275-290
21. T. Sivakumar, R. Venkatesan "A Novel Image Encryption Approach using Matrix Reordering"Wseas Transactions on COMPUTERS E-ISSN: 2224-2872 Issue 11, Volume 12, November 2013
22. Adrian Viorel Diaconu and Khaled Loukhaoukha, "An Improved Secure Image Encryption Algorithm Based On Rubik's Cube Principle And Digital Chaotic Cipher", Mathematical Problems in Engineering, Article ID 848392, vol. 2013, 2013, pp. 1-10.
23. C. K. Huang, C.W. Liao, S.L. Hsu and Y.C. Jeng, "Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system", Telecommunication Systems – Springer, vol. 52, no. 2, 2013, pp 563-
24. T. Sivakumar, R. Venkatesan "A Novel Image Encryption Method with Z-Order Curve and Random Number" International Journal of Computer Applications (0975 – 8887) Volume 103 – No.12, October 2014
25. T.Sivakumar and R.Venkatesan "A Novel Approach for Image Encryption using Dynamic SCAN Pattern" IAENG International Journal of Computer Science, 41:2, IJCS_41_2_0227 May 2014
26. T. Sivakumar And R. Venkatesan "A New Image Encryption Method Based on Knight's Travel Path and True Random Number". Journal of Information Science and Engineering 32, 133-152 (2016)
27. Chandra Prakash Singar, Jyoti Bharti, R.K. Pateriya "Image Encryption based on Cell Shuffling and Scanning Techniques" Proceeding International conference on Recent Innovations is Signal Processing and Embedded Systems (RISE-2017) 27-29 October,2017

AUTHORS PROFILE

Mr.Chandra Prakash Singar presently working as an Assistant Professor in Information Technology Department, at Shri G.S. Institute of Technology & Science Indore. He completed his bachelor of engineering at University Institute of Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya Bhopal in 2007 and continued his Masters of Technology in Software Engineering at Motilal Nehru National Institute of Technology Allahabad (MNNIT) in 2009. Presently doing Ph.D from Maulana Azad National Institute of Technology Bhopal. Since 2009 he began his career in the field of education at the RKDF Group of engineering as an assistant professor & Head, he also worked as an assistant professor in various engineering institute and More than 8 year of teaching experience with reputed engineering institutes.

Dr. Jyoti Bharti presently working as an Assistant Professor in Department of Computer Science and Engineering at Maulana Azad National Institute of Technology Bhopal. Educational Qualification is Ph.D, Master of Technology (I.T), and Bachelor of Engineering (CSE). More than 10 year of teaching experience in the field of Computer Graphics, Image Processing and Biometric. Her research fields include wireless network, Computer Graphics, E-commerce security system, Image Processing, Biometric Recognition and Computer Network. Her teaching experience in various engineering institute and from 2007 to till dated she is assistant professor at MANIT Bhopal. Her research published in various journals, national and international conference. More than 15 expert lectures delivered in various engineering institute.

Dr. R.K. Pateriya, Associate Professor in Department of Computer Science and Engineering at Maulana Azad National Institute of Technology Bhopal. Educational qualifications is PhD (CSE), M.Tech (CSE), BE (Computer Technology), his research work has been published in different reputed journals and national and international conference which are indexed in IEEE, SCIE, web of science and Scopus. He published 32 papers in International Journals, 05 Papers in the National Level Conference, and 10 papers in International Level Conference, total 47 papers published. Presently he is member of various professional bodies like LMCSI, MIEEE, MIAENG, and MIACSIT. He visited various countries for educational perspective. He is Chief Investigator of Information Security Education and Awareness (ISEA), MHRD Government of India Project. His research domain includes Data Mining, Cloud Computing, Information Security, and Information Retrieval. More than 24 year of teaching experience. He delivered more than 20 expert lectures at various organizations like Bank of India Training Center, IIITM Gwalior, and other reputed Institutes.