International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

A New Color Image Encryption Algorithm With Three Stage Shuffling And Xor Diffusion

Subashanthini S, Pounambal M

Abstract: ***The world has developed far beyond our expectations with the essence of technology, which has a profound effect on recent ways of data transmission. Data can be transmitted in many ways, but not so efficiently and securely as digital data. Imagery data is very vital these days considered these are used everywhere around the world. This paper mainly emphasizes on the prime issue i.e. "making the system more secure". Therefore securing the image is a principal factor of this paper as the present issue that is ongoing now with data theft which is predominantly in an image. So, this paper mainly focuses on how to proliferate the sensitivity to the attacks and securing the image which is an integration of different algorithms of diffusion and shuffling based on chaotic logistic maps. A new approach for the proposed algorithm was generated. A few basic examinations like NPCR (Number of Pixel Change Rate), Histogram investigations, UACI (Unified Average Change of Intensity) and PSNR (Peak Signal to Noise Ratio) are performed against various test images of size 256 × 256×3. Results obtained from the analysis endorses that it offers a high level of security. This proves the credibility for this algorithm for the future usage in the real world.***

Keywords: Chaotic logistic map, Image Encryption, Diffusion, Shuffling, Knight's tour

I. INTRODUCTION

In this digital world, everyone tends to find a better way of communicating with each other which can be in any form of data. The data could be text, image or any graphical content. A number of ways to transmit the data have been employed since the early days. Many algorithms like DEA (Data Encryption Algorithm), DES (Data Encryption Standard), and AES (Advanced Encryption Standard) came into existence, but they are only efficient in encrypting the text but not appropriate for the image. The proliferation of Digital image processing has increased rapidly because it offers more security and it is even more efficient when compared to text-based data. Everyone who is trying to transmit the data are looking for a faster transmission system with added security where there will be low transmission loss and better yields of retrieval of their data without losing the minimal. This has been the case for so many years, so many image encryption algorithms are introduced to secure the imagery information while transmission. Well, being in a digital world every activity happens so fast as this transmission, but the question remains the same, i.e. "Is this sensitive information going to be secure?" This has been the buzzing question around the world for a while. This Image encryption technique have raised a question of security during the transmission of the imagery data for which the proposed algorithm solves the question as much as possible. These algorithms can hold the brute force attacks without loss of data provided if intensified algorithms in terms of confusion are employed. In this kind of situation, an undeviating solution to all these questions could be using a very well-known encryption algorithm like DES, but they don't stand a chance against the brute force attack. Chaotic did play well as they are quite interesting and intriguing in the aspect of their properties like aperiodicity, pseudo-random property. Chaotic sequences are very sensitive to the infinitesimal amount of change in the input, as a result, it yields high discrepancy in the output, in turn creating a high randomness in the system. This work focuses on many confusion and diffusion techniques. Several analyses were conducted on this system which yield better results than the existing one.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Subashanthini S, School Of Information Technology and Engineering, VIT University - Vellore; subashanthini@vit.ac.in
Pounambal M*, School Of Information Technology and Engineering, VIT University - Vellore; mpounambal@vit.ac.in

II. LITERATURE REVIEW

Increasing the level of security has been an issue over the years and it is often overlooked and tried by so many researchers to improve the algorithms first proposed and yield better results, but still, they haven't achieved the robustness required to hold the brute force attack. So many came with an idea of increasing the randomness by using chaotic theory upon different levels. They have excelled at showing the exponential increase in the level of security by using a chaotic logistic map which will have the greater disproportion in the output for smaller and minute changes in the input, in turn, creating more randomness in the system.

Initial values for the parameters are generated using logistic map [1]. They have used two different diffusion algorithms on an RGB image and a shuffling algorithm to increase the level of security and security analysis have done to prove the robustness. The difference between two-dimensional chaotic maps are studied much on the parameters of the chaotic map like ergodicity and random behavior. They developed their algorithms using chaotic maps [2].

Alvarez and Li [3] have studied mostly on failures of implementing chaos-based systems with an allowed degree of security. They provided a framework for key space, implementation and security analysis. In [4], a 2D chaotic map is taken and it is generalized to 3D map for shuffling the image to create a greater difference between a cipher and plain image.

A 3D standard map is taken and cascaded with 3D cat map. Diffusion is generated by XOR-ing the shuffled image with diffusion template. They have analyzed on key space, differential analysis like NPCR, UACI [5]. A new algorithm that combines RC4 (Rivest Cipher 4) stream cipher with chaotic map is proposed by Ginting and Dillak [6]. Chaotic map is employed to generate the key stream which is then XORed with the image pixels, in turn, decreasing the numerical correlation between plain and ciphered image and have shown the sensitivity to the minimal change in the key. They have even calculated the image loss in terms of hash values. In [7], the authors have implemented a cryptographic system using the chaotic logistic and baker map in particular a logistic map. They have used XOR technique for the quantization of the original image. A review is conducted on existing chaos-based cryptosystems, where the authors have studied and analyzed few state-of-the art algorithms[8 – 15].

III. RELATED WORKS

A. Logistic Map

Logistic map is employed to generate the keys, which is represented as,

$$X_{i+1} = \mu \times X_i[1 - X_i] \quad (1)$$

Here X_i belongs to the range (0, 1) and is an iterative value. μ belongs to the range [3.9, 4). This dynamical system can yield results very differently for a minute change in the input. To get better chaotic sequences, three keys are generated for three planes i.e. one key for the red plane, one for the green plane, one for the blue plane. To generate a key using the chaotic logistic map mentioned above initial conditions of X_0 and μ are required.

B. Knight's tour algorithm

Knight's tour is an algorithm that totally depends on the legal knight moves on a chessboard. Here chessboard can be replicated with a 2D matrix in, turn, making moves on every plane in an image. This algorithm works according to four legal moves which is circularly executed after every four moves to complete the whole matrix if and only if it satisfies the hidden clause i.e. knight should only visit a position only once. It is shown in Fig. 1.It can be an extended version for the encryption scheme and the key reflects in terms of moves. It will be an added security for the image.

61	46	49	34	53	38	57	42
64	35	52	39	56	43	60	47
13	62	1	50	5	54	9	58
16	51	4	55	8	59	12	63
29	14	17	2	21	6	25	10
32	3	20	7	24	11	28	15
45	30	33	18	37	22	41	26
48	19	36	23	40	27	44	31

Fig. 1. Knight's tour for 8 8 matrix

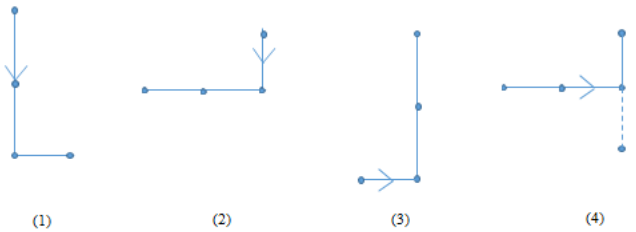

Fig. 2. Knight's tour pictorial representation

Fig. 1 and 2 explains Knight's tour algorithm for image shuffling. In Fig. 1, number 1 represents the shuffled image position for original pixel co-ordinate (1,1) and number 2 represents the shuffled image position for original pixel co-ordinate (1,2). Similarly other values in the matrix relocates the original pixel to new location. Finally the resultant 8×8 matrix will results a shuffled image matrix.

This journal uses double-blind review process, which means that both the reviewer (s) and author (s) identities concealed from the reviewers, and vice versa, throughout the review process. All submitted manuscripts are reviewed by three reviewer one from India and rest two from overseas. There should be proper comments of the reviewers for the purpose of acceptance/ rejection. There should be minimum 01 to 02 week time window for it.

C. XOR Diffusion

XOR – a bitwise operator is a widely used symmetric cipher encryption operator. When XOR is applied between two bits, either value 1 or 0 is returned. It is completely reversible and therefore it is best suited for symmetric encryption. Hence the original pixel value is retrieved by performing XOR operation twice as in Equation 2.

$$XOR\left(key, XOR\left(key, P\right)\right) = P \quad (2)$$

The detailed working of XOR operator is shown in Fig. 3, where P is the plain text and key is the symmetric key used for both encryption and decryption. Inner XOR is the encryption procedure, and the outer XOR is the decryption procedure.

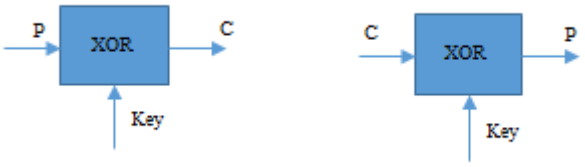

Fig. 3. (a)XOR – Encryption. (b) XOR – Decryption

IV. PROPOSED ALGORITHM

Consider a chaotic system which is highly nonlinear that can yield better robustness in the system. A chaotic sequence of X_i is generated using the initial conditions and seeds are generated using Equation 1.

Dividing an image into RGB planes is the first part of the encryption which will divide the plain image into three planes of the same size which are further divided into cells of specific size.

Secondly, a shuffling algorithm is employed to change the position of the pixels based on an approach which is described as creating a vector from a cell and shuffling their positions with other vectors. A new shuffling algorithm is incorporated in which some of the pixels are used to generate a key and in, turn, used for every plane for shuffling. The third step is performed by setting the shuffled planes through diffusion in which pixels are XORed with the key values generated using logistic map. Finally, these planes are fused back to generate an encrypted image.

Decryption plays a major role to bring back the plain image. The process decryption is the reverse process of encryption. The planes are extracted out of the encrypted image which falls under the section of dividing an image into 2D planes.

Reverse diffusion uses the same mathematical equation to retain the input by XOR-ing the cells of the output with the cells used in the input to generate the diffusion output of the encryption procedure. De-shuffling can be explained as a reverse shuffling to get back the original plane. After fusing these planes back into a whole image will yield the original image.

Differential analysis and statistical analysis were accomplished to investigate the toughness of the cryptographic system that has been created. These analysis include NPCR, UACI, Histogram and PSNR analysis.

The detailed encryption and decryption block diagram of the proposed algorithm is shown in Fig. 4 and Fig. 5.

A. Algorithm for Encryption

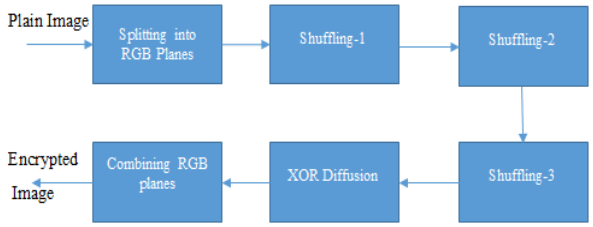

Fig. 4. Encryption block diagram of the proposed algorithm

Step-1: Splitting an image into RGB planes

Dividing the image into RGB planes is explained as a division of 3D (m×n×3) matrix into 2D (m×n×1) matrices of size m×n. m represents the length and n represent the width of an image.

Step-2: Shuffling 1 (Plane to Plane Shuffling)

There are basically two types of algorithms related to encryption which are shuffling and diffusion. Shuffling means simply altering the location of the pixels without modifying the intensity of the pixel. Diffusion means changing the pixel intensity by applying the algorithms. This shuffling algorithm is employed by changing the matrix dimensions of the original image into row vectors. Consider an image of size 4×4×3 and R_i, G_i, B_i, where 1>= i <= 16.

$$V1 = [R1G1B1R2G2B2G3 \dots R6] \quad -16\ pixels$$
$$V2 = [G6B6R7G7B7R8 \dots \dots \dots G11] \quad -16\ pixels$$
$$V3 = [B11R12G12B12R13 \dots \dots \dots B16] \quad -16\ pixels$$

This shuffling results scrambled image with pixels from one plane to another plane as per the above order (V1, V2, V3)

Step-3: Shuffling 2 (Shuffling using logistic map)

Each shuffled plane pixels are further shuffled by using the sequence generated by the initial conditions of the chaotic logistic map as discussed in section III - A. The shuffling algorithm which was generated based on explained above offers a perk of an extra bit of security.

Step-4: Shuffling 3 (Knight's tour algorithm)

Each shuffled plane is sub-divided into 8×8 matrices and all the matrices are shuffled by Knight's tour algorithm.

Step-5: XOR Diffusion

The resultant shuffled image undergoes the process of encryption by implementing XOR operation between the image pixel values and the key value generated using the logistic map, which utilizes the image size as explained in section III - C.

Step-6: Combining RGB planes

Reverse piling is a quite opposite approach to divide an image into RGB planes shown in the encryption as a part of it. Now, these three encrypted planes are fused back to form an encrypted image.

B. Algorithm for Decryption

Decryption is a total reverse process of encryption as shown in Fig. 5, which is done layer by layer to obtain the original image from the encrypted image. The decryption steps are as follows:

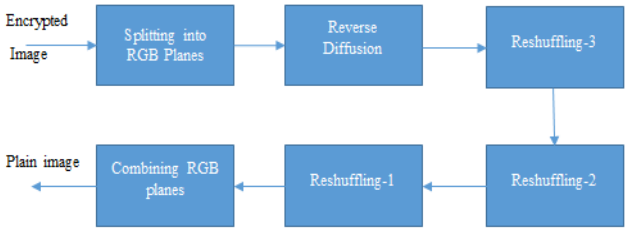

Fig. 5. Decryption block diagram of the proposed algorithm

Step-1: Splitting an image into three planes

Finally, in decryption, the encrypted image is again segmented into three planes of the same size. These are divided into three planes of the same size called piling and planes are P1, P2, and P3.

Step-2: Reverse diffusion

Reverse diffusion is performed on the split planes using XOR diffusion technique with the same key generated during the encryption process.

Step-3: Reshuffling with Knight's tour

The key used to generate shuffling with the key part is used again in the reverse process of shuffling with the key. With the help of sorting function in Matlab, the shuffling process was reversed.

Step-4: Reshuffling using logistic map

Key is generated using logistic map as mentioned in section III - A. Reverse shuffling process is carried out in three planes of image.

Step-5: Plane to Plane Re-shuffling

The shuffled image was reversed with the help of vectors. With the help of Matlab functions that can reshape the image for retaining its original form is all articulated in de-shuffling.

V1= [R1G1B1] -----3 pixels
V2= [R2G2B2] -----3 pixels
V3= [R3G3B3] -----3 pixels up to Vn.

From the above equations, it is reshaped using the function in Matlab to their original image.

Step-6: Combining RGB planes into one image

These planes of the current image are again merged to get back the original image. These planes are reverse piled in order to get the Decrypted image.

V. SECURITY ANALYSIS

If the system has to be secure enough if and only if the algorithm is robust enough and resistant enough to the attacks of statistical, cryptanalytic, cipher text in the real world. So this analysis is the most important one. This analysis covers key sensitivity analysis.

A. Key sensitivity analysis

High sensitivity key is needed by any cryptographic scheme to be more secure and more robust against different attacks. If there is even a small or marginal change in the key while decrypting the image, then it will yield the incorrect results of the image used for experimentation. So the alignment of the keys is very crucial and it is the very prime thing to use the correct key to decrypt the image.

VI. RESULTS AND DISCUSSION

Five test images (256×256×3)are taken for this implementation and results are shown in Fig. 6 and Fig. 7. Numerical results are presented in Table I and Table II.

Histograms are pictorial representations of the pixel intensities that are distributed in an image. So it clearly shows the how pixels are confined in the red plane, green plane and blue plane. Fig. 7 shows the Histogram of the plain, encrypted and decrypted Len image's Red, Green and Blue planes. Acknowledging from above image, a histogram of every plane P1, P2, P3 are constantly residing at the same level. This proves statistically that every pixel distribution is one and the same to confuse the attacker in, turn, increasing the robustness by using these algorithms.

A. PSNR and MSE analysis

The value of mean square error and peak signal to noise ratio is calculated among original image and all other images by the following Equation 3 and 4,

$$MSE = \frac{1}{w*h}\sum_{i=1}^{w}\sum_{j=1}^{h}||I(i,j) - I'(i,j)||^2 \quad (3)$$

$$PSNR = 10log_{10}\frac{255\times255}{MSE} \quad (dB) \quad (4)$$

Where I, I'→intensity function of decrypted and original image. (i, j) represents position. The MSE of the cipher image should be zero with respect to the original image because of the same intensities.

The average of fifty iterations of PSNR was employed. The resultant is 6.3780dB. If PSNR is increasing, it signifies that signal quality increases. For image encryption, it all deals with how best the factor of differentiation has been embedded between plain and encrypted image. Lower the PSNR will lower the similarities between plain and encrypted image.

B. NPCR and UACI analysis

Here NPCR and UACI were calculated to observe the sensitivity of the system towards differential attacks. As the system has been designed on a basis of chaotic system which is very sensitive to the minor changes in the input can cause a huge difference in the output. If it happens to be changed in the value of even one pixel can cause large alterations in the cipher image then these attacks become ineffective.

NPCR can be best described as the number of change in pixel rate when a change of one pixel value happened in the plain image and cipher is generated for the image. The formulation is as follows

$$NPCR = \frac{\sum_{i,j}K(i,j)}{N\times M}\times 100\% \quad (5)$$

where,

$$R(i,j) = \begin{cases} 0 & if\ C_1(i,j) = C_2(i,j) \\ 1 & if\ C_1(i,j) \neq C_2(i,j) \end{cases} \quad (6)$$

M, N represents the length and width of an image.

UACI defined as Unified Average Change Intensity is employed to calculate the difference of average intensities of two encrypted images. It is as follows

$$UACI = \frac{1}{N\times M}\left(\frac{|C_1(i,j) - C_2(i,j)|}{255}\right)\times 100\% \quad (7)$$

M represents the length and N represent the width of an image.

The values of NPCR , UACI, MSE and PSNR values for the proposed approach are tabulated as given below,

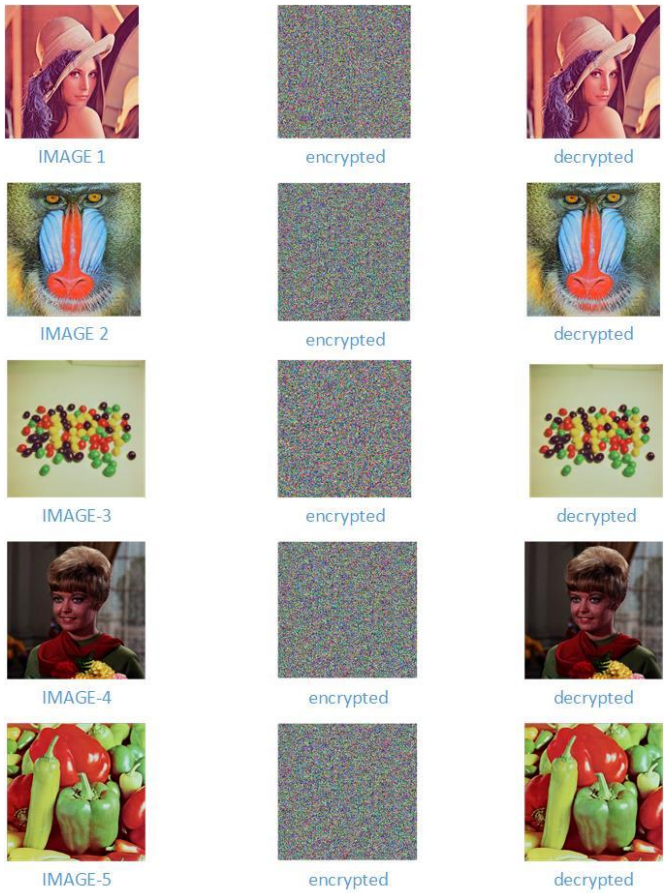

Fig. 6. Plain, Encrypted and Decrypted image results of all the test images using the proposed algorithm

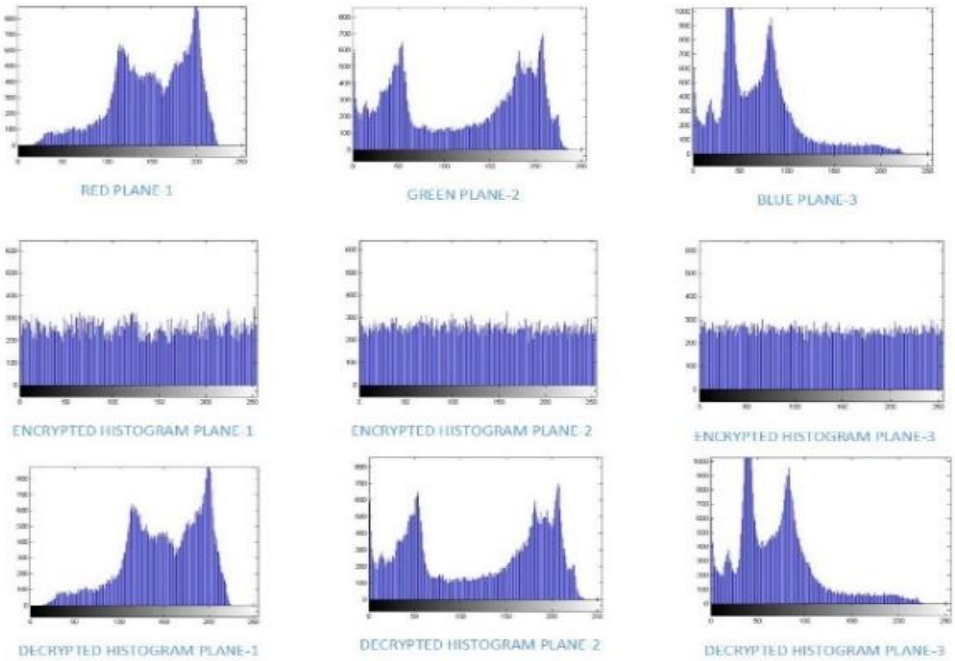

Fig. 7. Histogram of the plain, encrypted and decrypted Len image's Red, Green and Blue planes

Table I. NPCR and UACI values of encrypted Lena image using the proposed approach

Components of a plain RGB image	NPCR (%)	UACI (%)	MSE	PSNR (dB)
Red component	99.5728	33.567	1.4983 ×10^-4	9.4312
Green component	99.6109	33.568	1.4982 ×10^-4	9.3013
Blue component	99.6262	33.714	1.4984 × 10^-4	8.9989

C. Correlation analysis

Correlations of the adjacent pixels in the plain and cipher image, we randomly choose 2000 pairs of adjacent pixels in horizontal, vertical and diagonal directions from the plain image and its encrypted image. The correlation values as shown in Table II, shows that the original plain image has more correlation and the cipher image has less correlation. Moreover, standard formulae from existing literature is used to calculate the correlation coefficient of each pair.

Table II. Plain and Encrypted image Horizontal (H), Vertical (V) and Diagonal (D) correlation values for the proposed algorithm

mage	Horizontal direction	Vertical direction	Diagonal direction
Plain Lena	0.9396	0.9975	0.9263
Cipher Lena	-0.0033	0.0446	0.0394
Plain baboon	0.9506	0.9099	0.9172
Cipher baboon	0.0108	-0.0082	-0.0291
Plain house	0.9879	0.9803	0.9830
Cipher house	0.0432	0.0298	-0.0443
Plain red girl	0.9425	0.8500	0.8588
Cipher red girl	-0.0230	0.0238	-0.0170
Plain green	0.9723	0.9491	0.9421
Cipher green	-0.0339	0.0.219	0.0128

VII. CONCLUSION

A proper chaotic logistic map is utilized efficiently to generate the keys which possess an important property of dynamical system or chaos after the discretization. This Encryption process of image encryption provides a better and secured network. A new algorithm called Knight's tour as an extension can be added to the top of this algorithm which is employed in encryption in order to complicate the confusion process, in turn, reducing the threat of data thefts. NPCR is pretty well. The key space analysis yielded better results than many techniques out in the world, in turn, increasing the key aspect of the cryptographic system that is security. Having low MSE justifies that data loss would be on a negligible scale. Hence, this proposed method offers better security than the existing one. This can be used for many color images to transmit them securely.

REFERENCES

1. Kumar, M., Powduri, P., & Reddy, A. (2015) 'An RGB image encryption using diffusion process associated with the chaotic map', *Journal of Information Security and Applications*, *21*, pp.20-30.
2. Akhshani, A., Behnia, S., Akhavan, A., Hassan, H. A., & Hassan, Z. (2010) 'A novel scheme for image encryption based on 2D piecewise chaotic maps', *Optics Communications*, *283*(17), pp.3259-3266.
3. Alvarez, G., & Li, S. (2006) 'Some basic cryptographic requirements for chaos-based cryptosystems', *International Journal of Bifurcation and Chaos*, *16*(08),pp. 2129-2151.
4. Chen, G., Mao, Y., & Chui, C. K. (2004) 'A symmetric image encryption scheme based on 3D chaotic cat maps', *Chaos, Solitons & Fractals*, *21*(3), pp.749-761.
5. Gupta, K., & Silakari, S. (2011) 'A new approach for fast colour image encryption using chaotic map', *Journal of Information Security*, *2*(04), pp.139.
6. Ginting, R. U., & Dillak, R. Y. (2013, October) 'Digital colour image encryption using RC4 stream cipher and chaotic logistic map', In *Information Technology and Electrical Engineering (ICITEE), 2013*, pp. 101-105.
7. Rathore, D., & Suryavanshi, A. (2016) 'A proficient Image Encryption using Chaotic Map Approach', *International Journal of Computer Applications*, *134*(10), pp.20-24.
8. Tomer, D., & Vijayalakshmi S. (2014) 'Review on Different Chaotic Based Image Encryption Techniques'.
9. [9] Elabady, N. F., Abdalkader, H. M., Moussa, M. I., & Sabbeh, S. F. (2014, April) ' Image encryption based on the new one-dimensional chaotic map', *2014 International Conference on Engineering and Technology (ICET)*, pp. 1-6.
10. Yun-Peng, Z., Wei, L., Shui-ping, C., Zheng-jun, Z., Xuan, N., & Wei-di, D. (2009, October) 'Digital image encryption algorithm based on chaos and improved DES. *IEEE International Conference on Systems, Man, and Cybernetics', 2009. SMC 2009.* pp. 474-479.
11.]Kumar, M., Mishra, D. C., & Sharma, R. K. (2014) 'A first approach to an RGB image encryption',*Optics and Lasers in Engineering*, *52*, pp.27-34.
12. Pareek, N. K., Patidar, V., & Sud, K. K. (2011) ' A symmetric encryption scheme for color BMP images' , *International Journal of Computer Applications in Special Issue on Network Security and Cryptography*, *2*, pp.42-46.
13. Singh, N., & Sinha, A. (2009), 'Optical image encryption using Hartley transform and logistic map' , *Optics Communications*, *282*(6),pp. 1104-1109.
14. Sun, F., Lü, Z., & Liu, S. (2010), 'A new cryptosystem based on spatial chaotic system', *Optics Communications*, *283*(10), pp.2066-2073.
15. Huang, C. K., & Nien, H. H. (2009) ' Multi chaotic systems based pixel shuffle for image encryption', *Optics Communications*, *282*(11), pp. 2123-2127.

AUTHORS PROFILE

SUBASHANTHINI S is with the School of information Technology and Engineering, VIT University. She received her B.E . in Computer Science and engineering from Bharathidasan University, TamilNadu, India, and her M.Tech. in Information Technology from VIT University. Currently, She is doing research on Image Encryption in VIT University. Her research interests is Image processing, Information security and Wireless Network design.

POUNAMBAL M is with the School of information Technology and Engineering, VIT University. She received her B.E .in Computer Science and engineering from Bharathiyar University, TamilNadu, India, and her M.Tech. in computer science and engineering from VIT University. She has received her Ph.D from VIT University in Computer science. Her research interests is Wireless Network design and databases.