IMAGE SECURITY USING SCAN PATTERN AND CHAOTIC MAP

Dr. Raghu M.E[1], Mr. Vishwas C G M[2], Niyam L Gingade[3], Prathiksha H P[4] , Sahana G R[5], Vilas N[*]
[1]Professor, Dept. of CS&E, Government Engineering College, Hassan, India.

[2]Assistant Prof., Dept. of IS&E, JNN College of Engineering, Shivamogga, India.

[345*]UG students Dept. of IS&E, JNN College of Engineering, Shivamogga, India.

ABSTRACT

Encryption can be accomplished in various ways for the transportation of images, data, video, and audio over wireless networks. Encryption can safeguard information from hackers, thereby ensuring the security of confidential data through a cryptosystem. Due to the escalating number of cyber-attacks, encryption has emerged as a crucial component of modern-day communication. This paper introduces a technique for image encryption. The method employs a combination of Scan pattern, confusion utilizing Arnold cat map, and xor operation using diffusion technique, thereby ensuring enhanced security for the image. Scan is a language-based spatial accessing methodology that generates a wide range of scanning paths. Arnold cat map is a system that stretches and folds image trajectories in phase space. The diffusion operation involves spreading out or shuffling the bits of an image in such a way that the relationship between the original pixels and the encrypted pixels becomes highly complex and difficult to discern. Furthermore, our scheme achieves better values of Entropy, PSNR and MSE compared to its counterparts from the literature. Additionally, correlation coefficients for images serve as magnificent indicators for a reliable chaotic scheme.

Keywords: Encryption, Cryptosystem, SCAN, Arnold Cat Map, Diffusion, Chaotic System.

I. INTRODUCTION

Multimedia encompasses the integration of various types of information like images, audio, video, and text to create cohesive and engaging experiences. Nowadays, digital images are used for communication. Any information shared over the internet needs a high level of protection from intruders. Cryptography is the art of protecting information by transforming readable information (plain data) into an unreadable format (cipher) with the help of well-structured encryption algorithms and secret keys. Cryptography refers to the process of encoding data in such a way that only authorized users can access and interpret it during storage or transmission. Cryptography schemes are of two types. One is known as symmetric key cryptography, in which a single secret key is used for both encryption at the sender’s end and decryption at the receiver’s end. Chaotic systems are sensitive, nonlinear, deterministic, and easy to reconstruct after filling in the image. This image encryption method is based on the rearrangement of the image pixels. The rearrangement is done by scan patterns that are generated by the scan methodology. With the aim to increase the key space of the algorithm, the concepts of Scan pattern and Chaotic map are combined in this work. In traditional encryption algorithm such as DES, AES, and RSA are appropriate for text encryption but not appropriate for image encryption. Here are some reasons why one might choose scan pattern and chaotic map-based approaches over AES and DES for image security, Scan pattern and chaotic map can be designed to influence the visual appearance of the encrypted image and high security. This is particularly beneficial when the encrypted data is an image, as maintaining visual confidentiality is often crucial. In our proposed work the image is shuffled using zeta z scan pattern and confusion operation is performed using ACM and diffusion operation is performed by xoring the confused image pixel and random key sequence using logistic map.

II. RELATED WORK

V Praveen et,al., [1] A novel encryption method for images combines SCAN patterns, a carrier image from ASCII strings, and Hill cipher, ensuring robust security through intricate spatial accessing and encryption techniques. Sara Farrag et.al.,[2] Introduces triple-layer security: AES-128 and chaotic map encryption, followed by LSB steganography with zigzag pattern in RGB planes, achieving superior performance in various metrics. Krishna Raj A et.al.,[3] In today’s cybersecurity landscape, cryptography safeguards data against hackers, viruses, and fraud, employing various algorithms for encryption and decryption. This project integrates SCAN patterns and extended tiny encryption for image security, rearranging pixels and applying encryption techniques to ensure robust protection. Shana K U et.al.,[4] This paper introduces a novel grayscale image encryption method employing Logistic map and Z-order curve, enhancing security by incorporating the original image in key generation. Experimental validation demonstrates its resilience against diverse attacks, affirming its high security level. Pranjali Sankhe et.al.,[5] This paper presents a novel symmetric image encryption method utilizing Henon’s chaotic system and pixel shuffling, ensuring effective and efficient encryption. Chaotic encryption and decryption applied to images provide robust security in real-time transmission systems, thwarting unauthorized access and ensuring confidentiality. Pranjali Sankhe et.al., [6] This article introduces a novel image encryption algorithm using chaos theory and dynamic substitution, based on Henon and Ikeda chaotic maps with S-box transformation. Security analysis reveals high entropy values, a large key space, and superior performance in NPCR and UACI compared to state-of-the-art algorithms, affirming its efficiency and security. Diya Achu Pradeep et.al.,[7] Utilizing the Henon chaotic maps for image encryption to the enhances security in critical fields like banking and medicine, proving its robustness through comparative analysis and simulation results, fostering confidence in its application for secure data transmission. Anak

Agung Putri Ratna et.al.,[8] Amidst the rapid digital advancements, safeguarding sensitive data via image encryption is imperative. Analysing 1D, combined, and enhanced chaotic maps highlight Logistic, Tent, and Sine maps as top performers in security assessments across various domains. Rashmi P and Supriya M C et.al.,[9] This study develops a tele dermatology image encryption system using chaos-based encryption with Arnold's cat map for confusion and Henon map for diffusion, ensuring security with a 30-digit secret key from Diffie-Hellman exchange. Tests demonstrate flat histograms and distributed gray values in encrypted images, with key sensitivity showing significant differences with just one number change, yet unable to restore the original image. Veena G et.al.,[10] A novel hybrid image encryption technique integrating continuous orthogonal scan, Arnold cat map, and Tent map for pixel scrambling and key generation, surpassing limitations of existing methods. Through simulation experiments and security analysis, the efficacy of the proposed method in mitigating plaintext attacks and enhancing encryption strength is demonstrated.

III. BACKGROUND THEORY

In this background theory, pixel shuffling using scan pattern, confusion operation using ACM is described and key is generated using logistic map is discussed.

1. Scan Pattern

The SCAN method is a formal language-based, two-dimensional spatial accessing methodology capable of representing and generating a wide variety of scanning paths. The SCAN language utilizes four fundamental scan patterns: continuous raster (C), continuous diagonal (D), continuous orthogonal (O), spiral (S), Right orthogonal (A), diagonal parallel (E), vertical symmetry (S), continuous orthogonal (L), zeta (Z), block band raster (R) [1].

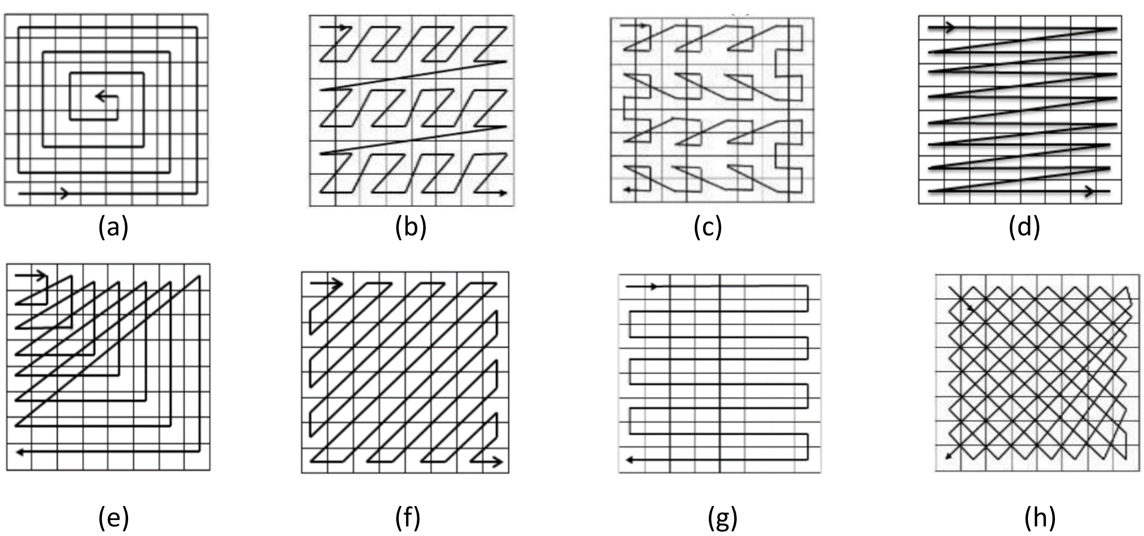


Figure 1: Different Scan Pattern (a) Spiral-In (b) Zeta-Z (c) Block-B (d) Raster-R
(e) Right Orthogonal-A (f) Diagonal-D (g) Continuous Raster-C (h) Diagonal parallel-E

2. Arnold Cat Map

According to Arnold's transformation

$$\begin{bmatrix} Xn' \\ Yn' \end{bmatrix} = R \begin{bmatrix} Xn \\ Yn \end{bmatrix} \text{mod } N \tag{1}$$

$$\text{Where } R=\begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \tag{2}$$

$$\begin{bmatrix} Xn' \\ Yn' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} Xn \\ Yn \end{bmatrix} \text{mod } N \tag{3}$$

where N is the size of the image, p and q are positive integer and det(A) = 1. (Xn, yn)is the position of sample in the N x N data such as image, so that

$$(Xn, Yn) \in N \times N, \quad n \in \{0, 1, 2, . . N-1\}$$

and (Xn+1 , Yn+1) is the position transformed after the cat map. There are two typical factors that lead to chaotic movements in cat maps: tension (X, Y) and fold (using mods to put X, Y in the identity matrix)[1]. Equation (1) is used to transform each pixel coordinate of the image. When all the coordinates have been transformed, the resulting image is a confusing image.

3. Logistic map

The logistic map is a mathematical function used to model dynamic systems or other population growth. It is often used to describe the behaviour of chaotic systems, particularly in the context of population dynamics. The formula for the logistics map is shown in equation (4).

$$X_{n+1} = r * (1 - X_{n)} \tag{4}$$

When Xn represents the state at time n, and r represents the control parameter, also known as the growth rate (where r ∈ [0,4]), if the value of r falls between 3.57 and 4, the map exhibits chaotic behaviour.

IV. SYSTEM DESIGN AND ARCHITECTURE

In this proposed methodology, the image of size 512 x 512 is taken as input then zeta z scan operation is performed on image, then obtained scan image is confused using Arnold cat map in which pixels are confused, then obtained confused image is taken as input for the diffusion operation in diffusion operation the obtained pixel values of confused image is xored with random key sequence generated using logistic map then we get cipher image as shown in the Figure 2(a). The cipher is taken as input for the decryption process then process continues in reverse order of encryption process to obtain original image as shown in the Figure 2(b).

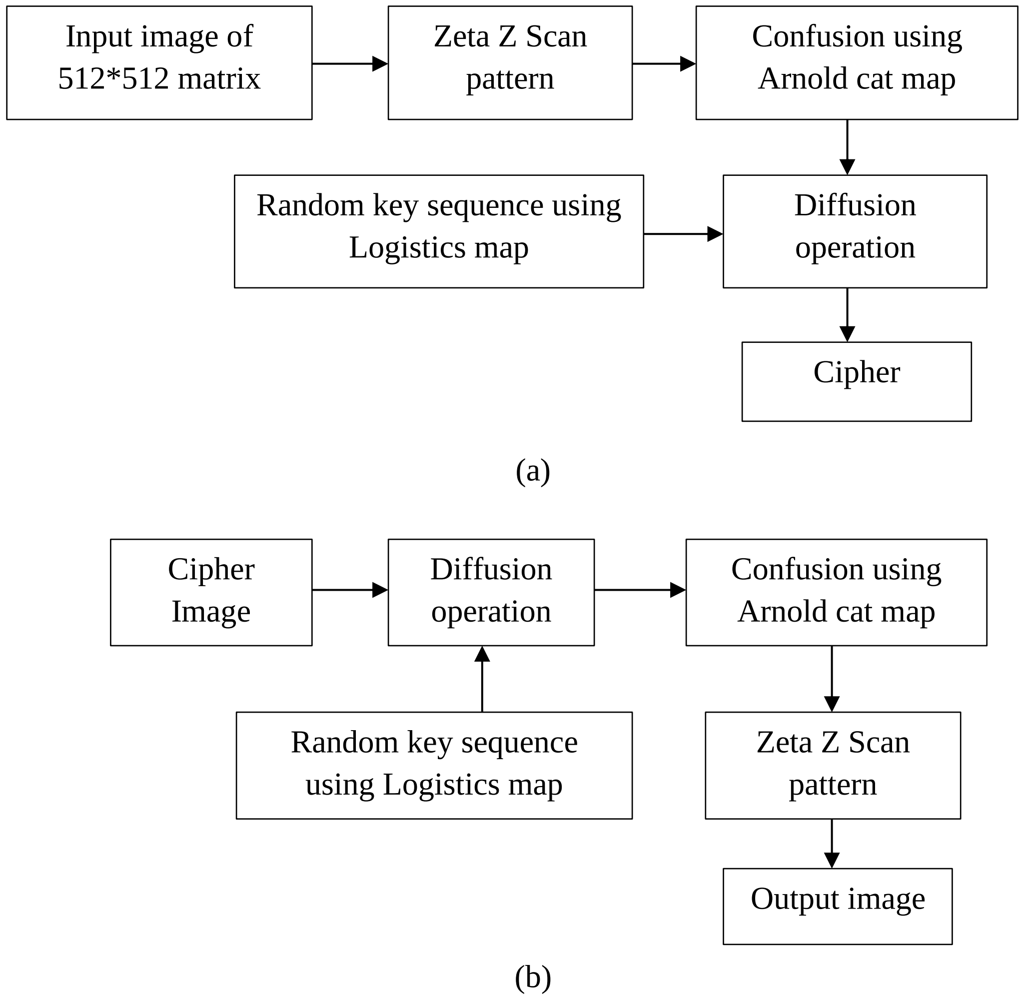


Figure 2: a) Proposed encryption method b) Proposed decryption method

V. PROPOSED METHODOLOGY

This section provides detailed instructions for the proposed image encryption and decryption process using scan pattern and chaotic map.

1. Encryption process

Step 1: Read input image of dimension m*n.

Step 2: Perform scan operation on the input image using Zeta-Z scan pattern .

Step 3: Perform confusion operation on the scanned image using Arnold cat map.

Step 4: Random key sequences are generated using the Logistics map.

Step 5: Perform diffusion operation between the pixel values of the confused image and random key selected from the logistic map .

Step 6: The Cipher image or Encrypted image is successfully created, marking the completion of the encryption process

2. Decryption process

Step 1: The cipher image obtained from the encryption process is selected for decryption.

Step 2: Diffusion operation is performed by doing XOR operation between the pixel values of cipher image and the random key sequence generated by the Logistic map, reconstructing the image from these pixel values.

Step 3: The Confusion operation is carried out on the diffused image using Arnold cat map.

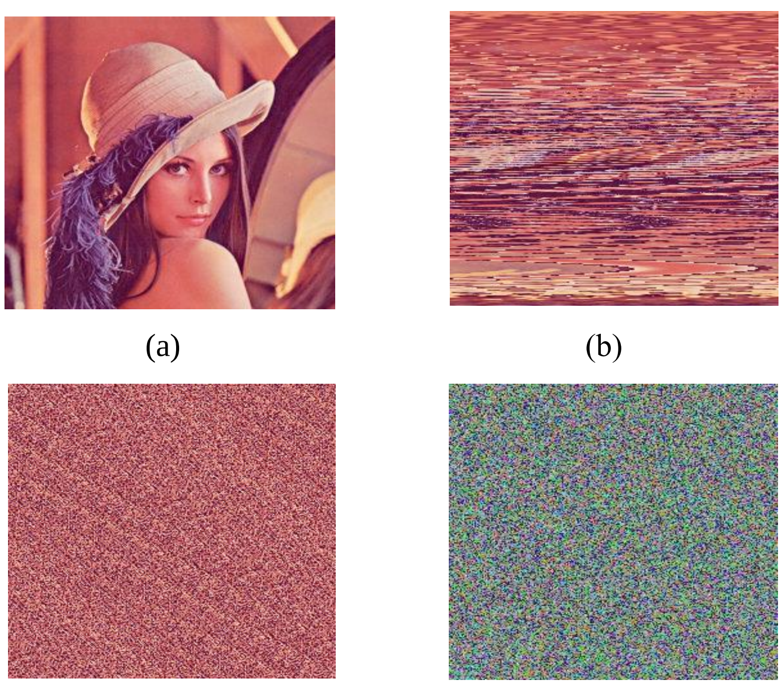
Step 4: The Zeta Z scan pattern operation is employed on the image to retrieve the original image.

Step 5:The original image is successfully recovered from the cipher image, marking the completion of the decryption process.

VI. RESULT AND ANALYSIS

1. Input and Output of proposed system:

Lena image of size 512x512 is considered as input image as shown in Figure 6 (a). The input image is considered as input for the scan operation. The image is shuffled Using the zeta z scan pattern. The obtained scan image is as shown in Figure 6 (b). The scan image is considered as input for the confusion process. The image is confused Using the x sequence generated by Arnold's Cat map as shown in equation (3). The obtained confused image is as shown in Figure 6 (c). Obtaining pixel values from confused image and xored with random key sequence then cipher image is obtained as shown in the Figure 6 (d).



(a) (b) (c) (d)

Figure 6: a) Lena image, b) Scan image, c) Confused image, d) Cipher image

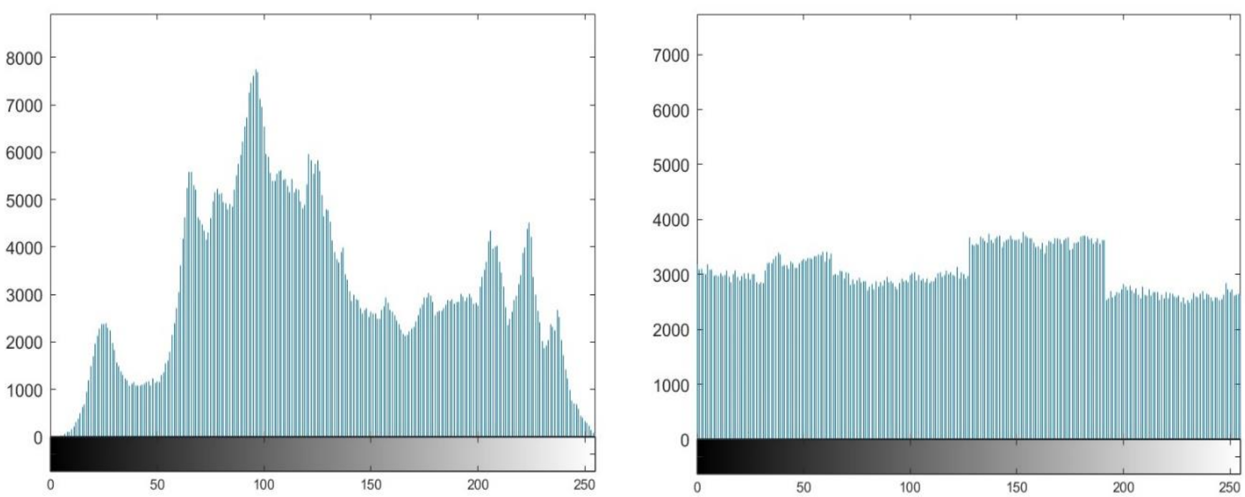
An image decryption algorithm should be able to decrypt the cipher image into original image. Only with the correct key, the cipher images can be correctly decrypted. The cipher image is considered as input image as shown in Figure 7(a) and decrypted image is shown in Figure 7(b).

(a) (b)

Figure 7: a) Input cipher image, b) Decrypted Lena image.

2. Histogram Analysis:

Figure 8(a). illustrates a histogram of the input (Lena) to the cryptosystem in which pixels of the input image are not uniformly distributed. Whereas in Figure 8(b), it can be observed from the cipher that the pixels are uniformly distributed and do not provide any clue to perform the statistical attack on the cryptosystem. Similar histograms are also derived for cameraman and baboon cipher images.



(a) (b)

Figure 8: a) The histogram of Lena image, b) The histogram of cipher image

3. Correlation Coefficient:

The correlation coefficients for the input and cipher of Lena image are shown in Figure 9. Where Lena image is converted into gray scale. Results for the correlation coefficients in horizontal, vertical, and diagonal are obtained and are listed in Table 1. It is seen that the correlation of the adjacent pixels in the plane image is nearer to 1 and the values of the cipher are nearer to 0.

Table 1: Correlation coefficient of original image and cipher image

Image	**Horizontal**		**Vertical**		**Diagonal**	
	Original image	Cipher	Original image	Cipher	Original image	Cipher
Lena	0.9952	-0.02743	0.9976	0.01822	0.9919	0.00923
Cameraman	0.9952	0.03173	0.9976	-0.00059	0.9921	-0.01297
Baboon	0.9950	-0.00134	0.9948	-0.00821	0.9898	0.00532
Dog	0.9983	0.03967	0.9985	-0.02104	0.9968	0.03960

4. Information Entropy:

The information entropy is one of the standard measures that used to measure the intensity of a symmetric cryptosystem. The information entropy H (m) of source message m is defined by (5). The perfect value of information entropy for an 8-bit message is 8, which means that the message source m can be counted as random.

$$E = \sum_{i=0}^{2^n-1} \left[P(i) * \log_2 \frac{1}{P(i)} \right] \quad (5)$$

where P(i) represents the probability of occurrence of the symbol. The entropies of plain and encrypted images are shown in Table 2. The results in this table show that the entropies of the cipher image generated by the proposed algorithm are near to the ideal value of 8.

Table 2: Information Entropy

Image	**Original image Entropy**	**Cipher image Entropy**
Lena	7.4329357	7.3566823
Cameraman	7.0487328	7.2826304
Baboon	7.1449323	7.3466725
Dog	7.4643126	7.3070145

5. Mean Square Error and Peak Signal-To-Noise Ratio (MSE & PSNR)

The mean-square error (MSE) and the peak signal-to-noise ratio (PSNR) are used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image.

Whereas, PSNR represents a measure of the peak error. The lower the value of MSE, the lower the error. The equation to calculate MSE is as given below

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M * N} \quad (8)$$

Where, M and N are the number of rows and columns in the input images. The equation to calculate MSE is as given below

$$PSNR = 10 \log_{10}\left(\frac{R^2}{MSE}\right) \quad (9)$$

Where, R is the maximum fluctuation in the input image data type. Table 4.6 lists the values for MSE and Table 3 lists the value for PSNR.

Table 3: MSE and PSNR Analysis

Image	MSE	PSNR
Lena	21749.289	4.7563
Cameraman	28791.253	3.5382
Baboon	18349.041	5.4946
Dog	28679.908	3.5550

VII. CONCLUSION

In this paper, the security of the encryption technique relies on both a secret key and the sensitivity of the Scan pattern and Chaotic system to initial values and parameters. By leveraging the randomness property of chaotic schemes such as the Arnold cat map and Logistic map, a highly secure encryption process is achieved. The generation of a random key sequence using the Logistics map, combined with pixel shuffling using the Arnold cat map and scan patterns, ensures robust encryption. Results demonstrate that the cipher image exhibits high entropy close to the ideal value of 8, minimal pixel correlation coefficients and high MSE and low PSNR thereby enhancing data security against unauthorized access.

REFERENCES

[1] V Praveen, P Hari Manohara Varma, BVSSN Raju, “Image Encryption using Scan Patterns and Hill Cipher”, IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT-2018), pp.1-6,2018.

[2] Sara Farrag, Wassim Alexan, Hisham H. Hussein, “Triple-Layer Image Security Usinga Zigzag Embedding Pattern”, pp-1-8,2019.

[3] Krishna Raj A ,Sharath Chandra N R, “ Image encryption and decryption using Scan -pattern XTEA encryption algorithm.” IOSR Journal of Electronics and Communication Engineering (IOSR-JECE),vol. 13, pp. 65-71,2018.

[4] Shana K U, Anuj Mohamed ,"An Image Encryption Technique using Logistic map andZ-order curve", IEEE Access, pp. 978-1-5386-5744-7,2018.

[5] Pranjali Sankhe, Anitha Lahan, “An Image cryptography using Henon map and Arnoldcat map**”,** IRJET Access , vol. 5, pp. 1900-1904,2018.

[6] Abdhulla Qayyum , Jawad Ahamud , Wadii Boulila and Saeed Rubaiee ,"Chaos-Based Confusion and Diffusion of Image Pixels Using Dynamic Substitution", IEEE Access, vol. 8 pp. 140876-140895, 2020.

[7] Diya Achu Pradeep, Harsha A , Aison Jacob, "Image Encryption Using Chaotic Map And Related Analysis", IEEE Access. DOI: 10.1109/ICACC- 202152719.2021.9708189,2021.

[8] Anak Agung Putri Ratna, Frenzel Timothy Surya, Ketut Eddy Purnama, “Chaos-Based Image Encryption using Arnold’s Cat Map Confusion and Henon Map Diffusion”, ASTES, pp-1-11,2021.

[9] Rashmi P and Supriya M C, “Self Adaptive Image Encryption Based on Orthogonal Scan Patterns Using Arnold Cat Map and Tent Map”, SSAHE Journal of Interdisciplinary Research,Vol.1(2), pp. 36-42, 2020.

[10] Veena G and Dr. Ramakrishna M,“A Survey on Image Encryption using Chaos- based Techniques”, IJACSA, Vol.12, pp.379-384, 2021.

[11] N.Bourbakis, “Image data compression encryption using G-SCAN patterns,” IEEE conference on SMC, October 1997, pp.1117-1120.

[12] Shalin J Patel, “Image Encryption and Compression using Scan Pattern,” IJSRD - International Journal for Scientific Research & Development Vol. 3, Issue 03, 2015 | ISSN (online): 2321-0613

[13] Chao Shen Chen and Rong Jian Chen, “Image encryption and decryption using SCAN methodology,” Proc. PDCAT, 2006.

[14] S.S. Maniccam and N.G. Bourbakis, “Image and video encryption using SCAN patterns,” Pattern Recognition, vol. 37, pp. 725-737, 2004.