

Design and analysis of pseudo hadamard transformation and non-chaotic substitution based image encryption scheme

Prajwalasimha S N, Kavya S R, Tanaaz Zeba Ahmed

Department of Electronics and Communication, ATME College of Engineering, India

Article Info

Article history:

Received Jan 28, 2019

Revised Mar 30, 2019

Accepted Apr 13, 2019

Keywords:

Correlation

Redundancy

Security

Substitution

Transformation

ABSTRACT

In this paper, Pseudo Hadamard Transformation (PHT) and non-chaotic substitution based image encryption scheme has been proposed. Images are characterized by intrinsic properties such as, strong redundancy and correlation between the adjacent pixels, hence more vulnerable to cyber-attacks. In the proposed technique, the redundancy and correlation have been effectively reduced by pixel position transformation using PHT and pixel value variation using non chaotic substitution, providing two stage security in encryption for images. Fifteen standard test images are considered for experimental analysis. Better average Number of Pixel Changing Rate (NPCR) and Unified Average pixel Changing Intensity (UACI) are obtained for a set of standard test images compared to more popular existing algorithms.

*Copyright © 2019 Institute of Advanced Engineering and Science.
All rights reserved.*

Corresponding Author:

Prajwalasimha S N,
Department of Electronics and Communication Engineering,
ATME College of Engineering,
Mysuru, Karnataka, India.
Email: prajwalasimha.sn1@gmail.com

1. INTRODUCTION

Information security plays a vital role in the field of multimedia technology. Vulnerability is one of the challenging issues in security aspects, nowadays. Due to swift maturation in multimedia technology, cyber-attacks are more common on communication channels. Images being pictorial representation of information carries bulk data are more vulnerable to cyber-attacks, due to their intrinsic properties: strong redundancy and correlation between adjacent pixels. These cyber-attacks cause data corruption or variations into miss- elucidation of data in a cloud [1-2]. Due to grid nature of images, encryption is done in different stages.

Multimedia fortification is done through several cryptographic algorithms since 1970s [3]. Security attacks are majorly categorized as: Analytical, Differential and Brute force attacks [4]. Communication channels are more vulnerable to analytical attacks. These channels are continuously monitored by security service providers. Any disruptions in the channels can be quickly drawn and information is sent to source and destination regarding the attack. Cryptanalysis is a differential attack in which the cryptographic algorithm is susceptible. This comprises cracking of cryptographic algorithm and decrypting the cipher data. Last resort tactics are also known as brute force attacks [4]. The secrete key is subjected for all possible amalgamations and analyzed in the cryptographic algorithm. With the help of all these tactics, the unauthorized third party users try to drudge the information. If an efficient cryptographic algorithm endure differential attacks, indirectly it deters analytical and brute force attacks [4].

In context of image encryption, the four classes of attacks in cryptanalysis [5] are: Ciphertext only attack, Chosen plaintext attack, Known plain text attack and Chosen ciphertext attack. In the ciphertext only attack, the attacker has access over ciphertext image and cryptanalyze the same to recover plaintext image. The attacker has access over some plaintext images and corresponding ciphertext images to reveal the

plaintext image by cryptanalyzing the algorithm, in the case of known plaintext attack. In chosen plaintext attack, the attacker has temporary access over the encryption algorithm and choose few known plaintext images to generate corresponding ciphertext images. In chosen ciphertext attack, the attacker has temporary access over the decryption algorithm and choose few known ciphertext images to generate corresponding plaintext images.

Conventional encryption algorithms such as Advanced Encryption Standards (AES), Rivest-Shamir Adleman (RSA), Data Encryption Standards (DES) and Blow-Fish algorithms are not apposite for image encryption [6] due to their intrinsic properties such as strong correlation between the adjacent pixels, strong redundancy and bulk data capacity [7-11]. Pixel value, position permutation and variation based image encryption algorithms are more proficient, nowadays. These algorithms uses chaotic theory of randomness to shuffle the pixel values and positions. With these algorithm, strong correlation and redundancy between the adjacent pixels can be effectively reduced. These chaotic maps are dynamic and very subtle to initial conditions. Due to these characteristics chaotic generators produces random values with great discrepancies. These arbitrary values are used to alter pixel values and positions in an image. The degree of arbitrariness resolves the chaotic behavior of a transformation.

Due to the intrinsic properties of chaotic maps: sensitivity to initial conditions, degree of randomness and dynamic behaviour, and these maps are more commonly used in encryption techniques. Based on the above characteristics of chaotic maps, a new image encryption scheme has been described by Hua et. al. [4]. The technique is based on 2D Logistic Sine Coupling map (2D-LSCM). Secret key elements are first subjected for initial permutation and then subjected for 2D-LSCM. In the substitution process these chaotic sequences generated by 2D-LSCM are used for pixel value variations. Very less entropy, correlation between the adjacent pixels in the cipher image, Number of Pixel Changing Rate (NPCR) and Unified Averaging pixel Changing Intensity (UACI) values are observed, indicating the algorithm is less resistive against differential attacks.

Lan et. al. [5] proposed an image encryption scheme which utilizes integrated chaotic system. The integrated chaotic system is used to increase the randomicity behavior of existing chaotic maps. 1D-Sine chaotic maps are cascaded with each other, subjected for nonlinear combination and then introduced to encryption system. The algorithm results with better resistivity against differential attacks by providing prime NPCR and very small difference in UACI compared to their respective ideal values. Very less redundancy in the cipher image has been observed by very minimum correlation between the adjacent pixels in the cipher image and high entropy values.

Li et. al. [6] proposed a combined 2D Arnold Cat chaotic map and Discrete Wavelet Transformation (DWT) based image encryption technique. The original image is first subjected for DWT. The DWT coefficients are then subjected for 2D Arnold Cat map for further reduction in redundancy. The algorithm results with less UACI values and high NPCR, indicating moderate resistivity against differential attacks. Very less correlation between the adjacent pixels values in the cipher image is also noticed, indicating optimal reduction in the redundancy. A combined chaotic map with Logistic, Sine and Tent chaotic maps based image encryption scheme has been described by Zhongyn et. al. [7]. Pixel scrambling is performed in two stages. At first stage, a combined Logistic-Sine- Cosine chaotic map is used and in the next stage Sine-Tent-Cosine chaotic map is used to reduce inter-pixel redundancy in the host image. The algorithm results with optimal reduction in the redundancy in the cipher image by providing very less correlation between the adjacent pixels in the cipher image. The algorithm results with better NPCR but comparatively less UACI values, indicating moderate stability against differential security attacks.

A new non chaotic substitution based image encryption with multi stage security is proposed by Kandar et. al. [8], in which encryption is performed in two stages: confusion and diffusion using cyclic group of sequences. Due to pixel permutation, the algorithm results with less UACI and high NPCR values, indicating moderate resistivity against differential attacks. The algorithm results with optimal reduction of redundancy in the cipher due to high entropy and very minimum correlation between the adjacent pixels.

Based on the above assessment, it can be noticed that an efficient encryption algorithm should be developed which takes very less execution time and gives better results against statistical security analysis. The paper is organized as follows. Section 2 overviews proposed methodology: transformation and substitution with different levels in the cryptographic algorithms. Experimental results are tabulated in Section 3 along with different kind of tests in encrypted domain. Final section concludes the paper.

2. METHODOLOGY

The encryption is carried out in two stages: Transformation and Substitution. The strong redundancy and correlation between adjacent pixels in an image is reduced by subjecting it to pixel position alteration with the help of Pseudo Hadamard transformation (PHT) and pixel value variation using substitution

technique. The original (Host) image is first subjected for transformation using PHT. A substitution image is considered and it is also subjected for transformation (PHT). The resultant transformed images of both original and substitution are subjected for logical pixel wise XOR operation to get cipher image from first stage. The obtained cipher image is then subjected for pixel value variation using substitution box (S-box). A predefined S-box is used for substitution in which elements are randomly arranged. Each pixel in the cipher image obtained from the first stage and elements of S-box are subjected for logical pixel wise XOR operation to get final cipher image after substitution. Flow diagram of proposed encryption algorithm as shown in Figure 1.

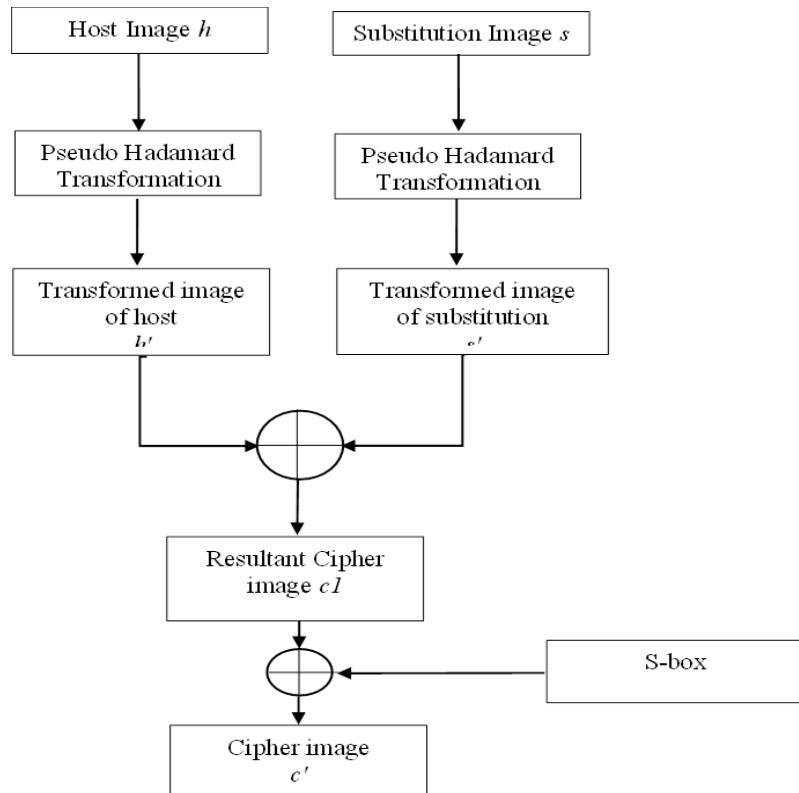


Figure 1. Flow diagram of proposed encryption algorithm

2.1. Encryption

Step1: The host image is subjected for Pseudo Hadamard transformation.

$$h'(p', q') = h \left\{ \begin{array}{l} (\alpha + \beta) \bmod 2^n, \\ (\alpha + 2\beta) \bmod 2^n \end{array} \right\} \quad (1)$$

where,

$$p' = (\alpha + \beta) \bmod 2^n$$

$$q' = (\alpha + 2\beta) \bmod 2^n$$

The initial values consider here with,

$$h'(p', q') = h \left\{ \begin{array}{l} (\alpha + \beta) \bmod 256, \\ (\alpha + 2\beta) \bmod 256 \end{array} \right\} \quad (2)$$

where,

h is the host image

h' is the Pseudo Hadamard transformed image of host

Step2: The substitution image is also subjected for Pseudo Hadamard transformation.

$$s'(p', q') = s \left\{ \begin{array}{l} (\alpha + \beta) \bmod 2^n, \\ (\alpha + 2\beta) \bmod 2^n \end{array} \right\} \quad (3)$$

The initial values consider here are same as that of the host image,

$$s'(p', q') = s \left\{ \begin{array}{l} (\alpha + \beta) \bmod 256, \\ (\alpha + 2\beta) \bmod 256 \end{array} \right\} \quad (4)$$

where,

s is the substitution image

s| is the Pseudo Hadamard transformed image of secret

Step3: The resultant transformed images of both host and substitution are subjected for logical XOR operation pixel wise.

$$c1(p', q') = h'(p', q') \oplus s'(p', q') \quad (5)$$

where,

c1 is the cipher image of second stage

Step4: The number of execution rounds (d) is placed in the four extreme corners of the cipher image along with the respective pixel values.

$$d = \sum_{n=1}^N \sum_{m=1}^M i(\alpha, \beta) \quad (6)$$

Step5: Substitution box (S-box) of size 2n x 1, which includes 128 bits of secret key. The values in the S-box are randomly selected and placed. These values are constant for both encryption and decryption processes. The obtained cipher image from the transformation stage is subject for pixel wise logical XOR operation along with S-box in the row wise manner.

$$c'(p', q') = c1(p', q') \oplus S - box \quad (7)$$

2.2. Decryption

The number of rounds for decryption stage (d) is taken from the pixel values in the four extreme corners of the cipher image.

Step1: The obtained cipher image from encryption stage is first subjected for logically XOR operation with the elements of S-box. The resultant image is the decrypted image from the second stage.

$$c1(p', q') = c'(p', q') \oplus S - box \quad (8)$$

Step2: The Substitution image is subjected for Pseudo Hadamard transformation for the same set of initial values as implemented in the encryption stage.

$$s'(p', q') = s \left\{ \begin{array}{l} (\alpha + \beta) \bmod 2^n, \\ (\alpha + 2\beta) \bmod 2^n \end{array} \right\} \quad (9)$$

The initial values consider here are same as that of the host image,

$$s'(p', q') = s \left\{ \begin{array}{l} (\alpha + \beta) \bmod 256, \\ (\alpha + 2\beta) \bmod 256 \end{array} \right\} \quad (10)$$

where,

s is the secret image

s| is the Pseudo Hadamard transformed image of secret

Step 3: The decrypted image from the first step is logically XORed with the transformed image from the second step to get the resultant image of the host in the transformed form.

$$h'(p', q') = c1(p', q') \oplus s'(p', q') \quad (11)$$

Step 4: The resultant image from the above step is subjected for inverse Pseudo Hadamard transformation to get the desired original image.

$$h(\alpha, \beta) = h' \begin{cases} (2p' - q') \bmod 256, \\ (q' - p') \bmod 256 \end{cases} \quad (12)$$

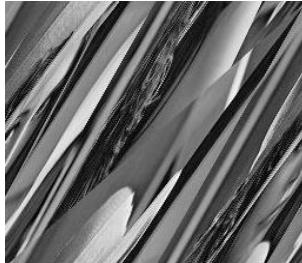
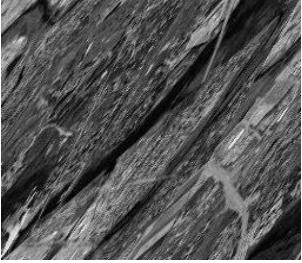
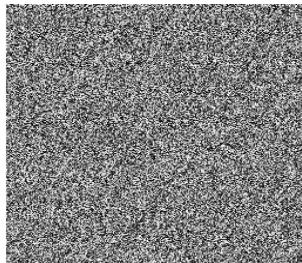
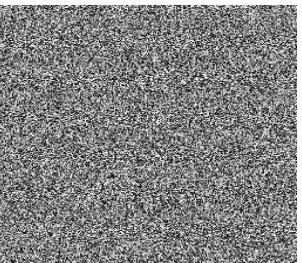
where,

h is the host (Original) image

h' is the Pseudo Hadamard transformed image of host

Illustration of Host, Substitution, Cipher Images after Transformation, Diffusion and Substitution Stages as shown in Table 1.

Table 1. Illustration of Host, Substitution, Cipher Images after Transformation, Diffusion and Substitution Stages

	
Host image (Lena)	Substitution image (Concordaerial)
	
Transformed image of host	Transformed image of Substitution
	
Diffused Cipher image of stage 1	Cipher image of final stage

3. PERFORMANCE ANALYSIS

Standard test images are considered from Computer Vision Group (CVG), Dept. of Computer Science and Artificial Intelligence, University of Granada, Spain. Resultant cipher images are subjected for statistical and differential security tests. Matlab software is used for the implementation with Intel i3 processor @ 1.7 GHz, 4GB DDR RAM and Windows 8 OS. Fifteen standard images are considered from grayscale image dataset of miscellaneous (256X256) category. The algorithm takes an average of 0.19 second for encryption process and is less than 0.29 second mentioned in modified Camellia algorithm [17],

1.27 seconds as mentioned in the hybrid chaotic map [18], 1.243 seconds mentioned in mixed chaotic map [19] and 0.48 second mentioned in hyper-chaotic system [20]. Comparison of entropy, correlation, nPCR and UACI for encrypted images with the existing algorithms as shown in Table 2.

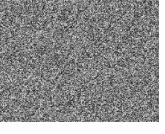
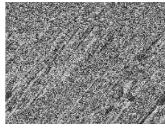
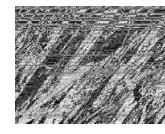
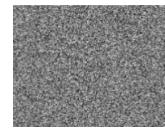
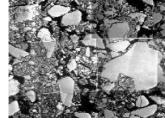
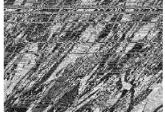
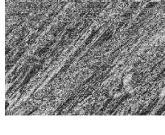
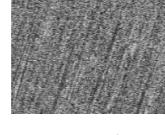
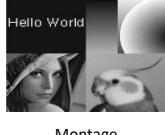
Table 2. Comparison of Entropy, Correlation, NPCR and UACI for Encrypted Images with the Existing Algorithms

Sl. No.	Images	Entropy=8 [19]	Correlation	Number of Pixel Changing Rate (NPCR) ≥ 99.609% [19]	Unified Average pixel Changing Intensity (UACI) ≥ 33.46% [19]
1	Lena	5.5407 (Blow Fish) [20] 5.5438 (Two Fish) [20] 5.5439(AES 256) [20] 5.5439 (RC 4) [20] 7.5220 [21] 7.6427 [27] 7.9950 [22] 7.9958 [23] 7.9970 [20][26] 7.9971 [24-25]	-0.0043	90.21 [21]	31.00 [21]
		7.9976		99.60 [24]	32.01 [24]
		7.9947 [24]		99.5859 [23]	33.4201 [23]
		7.9950 [25]		99.5895	33.4060
		7.9967 [2]		99.59 [2]	30.87 [24]
		7.9974		99.60 [25]	33.43 [25]
		7.9971 [24-25]		97.2387 [2]	22.2154 [2]
		7.9954 [24]		99.6094	33.2096
		7.9960 [25]		99.61 [24]	30.71 [24]
		7.9968 [25]		99.6185	33.5280
4	Airplane	7.9974	6.6523e-05	99.6338	33.4564
5	Cameraman	7.9972	0.0030	99.5743	33.4677
6	Elaine	7.9969	-0.0021	98.2354 [2]	28.1145 [2]
7	Clock	7.9973	2.6511e-05	99.6155	33.5944
8	Donna	7.9936	-0.0163	99.5636	32.9461
9	Foto	7.9973	-0.0021	99.5865	33.4483
10	Soil	7.9974	0.0053	99.6140	33.4716
11	Barche	7.9974	-0.0016	99.5789	33.4999
12	Montage	7.9972	0.0019	99.6277	33.5905
13	Pallon	7.9976	-0.0032	99.6033	33.7040
14	Vacas	7.9971	0.0036	99.6323	33.2626
15	Tulips	7.9975	0.0063	99.5682	33.5362
				99.6246	33.4510

4. CONCLUSION

On the basis of Pseudo Hadamard Transformation (PHT) and non-chaotic substitution, a new image encryption algorithm has been proposed. The algorithm encrypts an image in two stages: transformation and substitution, per each round. Pixel positions are effectively altered using PHT and pixel values are effectively modified using non-chaotic substitution (S-box). The size of the S-box is 2Kb, with 128 bits of secret key elements in between. About 2128 combinations takes huge time to execute brute force attack. Along with the S-box, a separate substitution image is considered in the transformation stage of the algorithm. The substitution image used is unique for a set of encryption. The elements of substitution image are randomly shuffled in each round of encryption using PHT. Based on these considerations, it is very difficult for unauthorized third party user to cryptanalyze the algorithm through analytical, differential and brute force attacks. The cipher image after encryption is subjected various security analysis. In Number of Pixel Changing Rate (NPCR) test, an average of 99.6023% is obtained for fifteen standard images and about 99.9932% close to the ideal value is achieved. In Unified Average pixel Changing Intensity (UACI) test, an average of 33.4382% is obtained for fifteen standard images and about 99.9348% close to the ideal value is achieved. In entropy test, 99.96% close to the ideal value is achieved and very minimum correlation between original and cipher images is observed. Further, chaotic generators can be used in the substitution stage of the algorithm to increase the level of security. Collection of original and corresponding cipher images by proposed algorithm as shown in Table 3.

Table 3. Collection of Original and Corresponding Cipher Images by Proposed Algorithm

				
Lena	Baboon	Pepper	Airplane	Cameraman
				
Cipher Image (Lena)	Cipher Image (Baboon)	Cipher Image (Pepper)	Cipher Image (Airplane)	Cipher Image of Cameraman
				
Elaine	Carnev	Donna	Foto	Soil
				
Cipher Image (Elaine)	Cipher Image (Carnev)	Cipher Image (Donna)	Cipher Image (Foto)	Cipher Image (Soil)
				
Barche	Montage	Pallon	Vacas	Tulips
				
Cipher Image (Barche)	Cipher Image (Montage)	Cipher Image (Pallon)	Cipher Image (Vacas)	Cipher Image (Tulips)

REFERENCES

- [1] H. Junhui, *et al.*, “JPEG Image Encryption with Improved Format Compatibility and File Size Preservation,” *IEEE Transactions on Multimedia*, Vol. 20, No. 10, pp. 2645-2658, 2018.
- [2] Y. Z. Leo, *et al.*, “On the Security of a Class of Diffusion Mechanisms for Image Encryption,” *IEEE Transactions on Cybernetics*, Vol. 48, No. 4, pp. 1163-1175, 2018.
- [3] J. Alireza, *et al.*, “On the Security of Permutation-Only Image Encryption Schemes,” *IEEE Transactions on Information Forensics and Security*, Vol. 11, No. 2, pp.235-246, 2018.
- [4] Prajwalasimha S.N. “(2019) Pseudo-Hadamard Transformation-Based Image Encryption Scheme”. In: Krishna A., Srikanth K., Naveena C. (eds) *Integrated Intelligent Computing, Communication and Security. Studies in Computational Intelligence*, vol 771. Springer, Singapore.
- [5] Xingyuan Wang, *et al.*, “An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map,” *IEEE Access Lett.* Vol. 6, 2018, pp. 23733-23746.
- [6] J. Alireza, *et al.*, “On the Security of Permutation-Only Image Encryption Schemes,” *IEEE Transactions on Information Forensics and Security*, Vol. 11, No. 2, pp.235-246, 2018.
- [7] Sanjeev Sharma, *et al.*, “Improved method for image security based on chaotic-shuffle and chaotic-diffusion algorithms,” *International Journal of Electrical and Computer Engineering*, Vol. 9, No. 1, pp.273-280, 2019.

- [8] Hamsa A. Abdullah, *et al.*, “FPGA Implementation of Color Image Encryption using A New Chaotic Map,” *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 13, No. 1, pp. 129-137, 2019.
- [9] Arindam Sarkar, *et al.*, “Neural Soft Computing based Secured Transmission of Intraoral Gingivitis Image in E-Health Care,” *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 14, No. 1, pp. 178-184, 2019.
- [10] Prajwalasimha S.N., *et al.*, “(2019) Logarithmic Transform based Digital Watermarking Scheme”. In: Pandian D., Fernando X., Baig Z., Shi F. (eds) *Proceedings of the International Conference on ISMAC in Computational Vision and Bio-Engineering 2018 (ISMAC-CVB)*. ISMAC 2018. *Lecture Notes in Computational Vision and Biomechanics*, vol 30. Springer, Cham.
- [11] Prajwalasimha S.N., *et al.*, “(2019) Digital Image Watermarking Using Sine Transform Technique”. In: Pandian D., Fernando X., Baig Z., Shi F. (eds) *Proceedings of the International Conference on ISMAC in Computational Vision and Bio-Engineering 2018 (ISMAC-CVB)*. ISMAC 2018. *Lecture Notes in Computational Vision and Biomechanics*, vol 30. Springer, Cham.
- [12] Zhongyun Hua, *et al.*, “2D Logistic-Sine Coupling Map for Image Encryption,” *Signal Processing*, Elsevier, Vol. 149, 2018, pp. 148-161.
- [13] Rushi Lan, *et al.*, “Integrated Chaotic Systems for Image Encryption,” *Signal Processing*, Elsevier, Vol. 147, 2018, pp. 133-145.
- [14] Chun-Lai Lia, *et al.*, “Multiple-Image Encryption by using Robust Chaotic Map in Wavelet Transform Domain,” *International Journal for Light and Electron Optics*, Elsevier, Vol. 171, 2018, pp. 276-286.
- [15] Zhongyun Hua, *et al.*, “Cosine-Transform-based Chaotic System for Image Encryption,” *Information Science*, Elsevier, Vol. 480, 2019, pp. 403-419.
- [16] Shyamalendu Kandar, Dhaibat Chaudhuri, Apurbaa Bhattacharjee and Bibhas Chandra Dhara, “Image Encryption using Sequence Generated by Cyclic Group,” *Journal of Information Security and Applications*, Elsevier, Vol. 44, 2019, pp. 117-129.
- [17] S. E. Marwa, *et al.*, “Image Encryption Using Camellia and Chaotic Maps,” *Proc. IEEE International Symposium on Signal Processing and Information Technology*, pp. 209-214, 2015.
- [18] A. N. Hikmat and A. Hamsa, “Image Encryption Using Hybrid Chaotic Map,” *Proc. IEEE International Conference on Current Research in Computer Science and Information Technology*, pp. 121-125, 2017.
- [19] W. Xingyuan, *et al.*, “An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map,” *IEEE Access Letters*, Vol. 6, pp. 23733-23746, 2018.
- [20] C. Delong, *et al.*, “Image Encryption Using Block Based Transformation with Fractional Fourier Transform,” *Proc. IEEE International Conference on Communications and Networking*, pp. 552-556, 2014.
- [21] H. Nitumoni, *et al.*, “A Wavelet Based Partial Image Encryption using Chaotic Logistic Map,” *Proc. IEEE International Conference on Advanced Communication Control and Computing Technologies*, pp. 1-5, 2015.
- [22] G. Anish and C. Kaustubh, “ Median Based Pixel Selection for Partial Image Encryption,” *Proc. IEEE International Conference on Image Processing Theory, Tools and Applications* , pp. 1-5, 2016.
- [23] A. B. Zaheer , *et al.*, “Energy Efficient Image Encryption Algorithm,” *Proc. IEEE International Conference on Innovations in Electrical Engineering and Computational Technologies* , pp. 1-6, 2017.
- [24] B. S. Nabil , *et al.*, “Nested Chaotic Image Encryption Scheme using Two-Diffusion Process and the Secure Hash Algorithm SHA-1,” *Proc. IEEE International Conference on Control Engineering & Information Technology* , pp. 1-5, 2016.
- [25] N. Zhengchao, *et al.*, “A Novel Image Encryption Algorithm based on Bit-level Improved Arnold Transform and Hyper Chaotic Map,” *Proc. IEEE International Conference on signal and Image processing*, pp. 3229-3234, 2016.
- [26] Prajwalasimha S N and S. R. Bhagyashree, “ Image Encryption using Discrete Radon Transformation and Non chaotic Substitution,” *Proc. 2nd IEEE International Conference on Electrical, Computer and Communication Technologies*, pp. 842-846, 2017.
- [27] Prajwalasimha S N and Usha Surendra,” Multimedia Data Encryption based on Discrete Dyadic Transformation,” *Proc. IEEE International conference on Signal processing and Communication*, pp. 492-496, 2017.