Performance analysis of transformation and bogdonov chaotic substitution based image cryptosystem

Prajwalasimha S. N., Basavaraj L.
Department of Electronics and Communication Engineering, ATME Research Centre, India

Article Info

Article history:

Received Oct 2, 2018
Revised Aug 23, 2019
Accepted Aug 30, 2019

Keywords:

Chaotic generator
Confidentiality
Correlation
Encryption
Substitution

ABSTRACT

In this article, a combined Pseudo Hadamard transformation and modified Bogdonav chaotic generator based image encryption technique is proposed. Pixel position transformation is performed using Pseudo Hadamard transformation and pixel value variation is made using Bogdonav chaotic substitution. Bogdonav chaotic generator produces random sequences and it is observed that very less correlation between the adjacent elements in the sequence. The cipher image obtained from the transformation stage is subjected for substitution using Bogdonav chaotic sequence to break correlation between adjacent pixels. The cipher image is subjected for various security tests under noisy conditions and very high degree of similarity is observed after deciphering process between original and decrypted images.

Corresponding Author:

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

1. INTRODUCTION

Images are pictorial depiction of information. Due to swift maturation in internet technology, digital images being major class of multimedia, plays a vital role in communication systems. These images are characterized inimitably by high inter pixel redundancy, strong correlation between adjacent pixels and bulk data capacity [1-7].

Confidentiality is one of the dominant facets of communication system. Fortification of information can be accomplished by adopting an efficient cryptosystem, which should encrypt and decrypt the information without flaws. More prevalently and habitually used encryption algorithms such as Rivest, Shamir and Adleman (RSA), Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Advance Encryption Standards (AES) are inapposite for images due to their inimitable characteristics [2]. Chaotic systems found proliferate implementation in the fields of cryptography, due to their intrinsic properties such as volatility, subtlety to the initial conditions, similar casualness and aperiodicity [3, 8]. With the help of chaotic theory, the inter pixel redundancy and strong correlation between adjacent pixels can be effectively reduced.

In many low dimensional chaos based cryptographic algorithms, the cipher data directly depends on chaotic orbit of a single chaotic system. Due to this, many low dimensional chaotic systems are more prone to phase space reconstruction attacks [9]. Such kind of attacks can be reduced by using S-box (Substitution box) in the algorithm. Complexity of cryptanalysis and brute force attacks can be further reduced by increasing the size of S-box in the algorithm. One such technique is developed by Silva-García and et al [10]. They introduced S-boxes in Advanced Encryption Standard (AES) algorithm to increase the level of security. Nonlinear chaotic differential equations are used to generate random numbers inside the S-box. But immunity against noise has not been noticed in the algorithm.

A double humped logistic map has been developed by Lingfeng & et al. [11] by introducing general parameters to the existing chaotic map to generate pseudo random key sequence for the substitution stage. Robustness of the algorithm against Gaussian noise has been noticed but not against other kind of noises. Better UACI values are observed for various images but considerable differences in the NPCR values are noticed compared to ideal values. Rasul Enayatifar & et al. [12] developed combined permutation and diffusion technique using 3-D logistic chaotic map. Better entropy is observed in the absence of noise for many standard images but considerable difference in the values of NPCR and UACI is observed compared to ideal values. A combined 1-D logistic map and 2-D Baker chaotic map based block wise permutation algorithm has been developed by Lingfeng Liu & et al. [13]. Even though low dimensional chaotic maps are considered, phase space is made large by multiple chaotic maps. Very minimum correlation between the adjacent pixels in the cipher image has been noticed along with slightly high entropy but considerable difference in the values of NPCR and UACI is observed compared to ideal values for few standard images.

Based on the above considerations a combined 2-D Pseudo Hadamard chaotic transformation (MPHT) and 2-D Bogdonav chaotic random diffusion based algorithm has been proposed in which a large phase space is considered along with a substitution image. The paper is organized as follows: Section 2 describes the proposed scheme. Section 3 with statistical and differential analysis followed by conclusion in Section 4.

2. RESEARCH METHOD

Three stages per round are involved in the encryption process: Transformation, Diffusion and Substitution. Modified Pseudo Hadamard transformation is used in the first stage and random sequence generated by Bagdonov chaotic generator is used in the substitution stage. Figure 1 illustartes the flow diagram of the system.

2.1. Encryption algorithm

Step1: Original image of size 2^n X 2^n is transformed using modified Pseudo Hadamard transformation.

$$H1'(x,y) = H((a+b+c)\ mod\ 2^n, (a+2b+c)\ mod\ 2^n) \quad 1 < a,b < 2^n \tag{1}$$

Where,

$H(a,b)$ is the host image of size 2^n X 2^n
$H1'(x,y)$ is the transformed image of size 2^n X 2^n
c is the constant ($c = 37$)

Step2: Block truncated substitution image of size 2^n X 2^n is transformed using modified Pseudo Hadamard transformation.

$$S1'(x,y) = S^t((a'+b'+c)\ mod\ 2^n, (a'+2b'+c)\ mod\ 2^n) \quad 1 < a',b' < 2^n \tag{2}$$

Where,

$S1'(a',b')$ is the block truncated substitution image of size 2^n X 2^n
$S^t(x,y)$ is the transformed truncated image of size 2^n X 2^n
c is the constant ($c = 37$)

Step3: Both transformed images are subjected for bitwise XOR operation

$$C1(x,y) = H'(x,y) \oplus S'(x,y) \tag{3}$$

Step4: The cipher image from first stage is subjected for substitution with pre-defined S-box.

$$C2(x,y) = C1(x,y) \oplus S\text{-}box \tag{4}$$

Step4: The cipher image from substitution stage is subjected for diffusion with random sequence generated Bogdonov chaotic equation.

$$x' = (x + y')mod\ 2^n \tag{5}$$

$$y' = (y + \varepsilon y' + Kx'(x'-1) + \mu x'y')\ mod\ 2^n \tag{6}$$

Where,

ε = 7(d)^2
K = 9(d)^2
μ = 3(d)
d = $\sum_{1}^{256}\sum_{1}^{256} H(a,b)$

$$C3(x,y) = C2(x,y) \oplus x' \quad (7)$$

Where,

$C3(x,y)$ is the cipher image after diffusion of size 2^n X 2^n

Step5: The number of execution rounds (d) is placed in the four extreme corners of the cipher image along with the respective pixel values.

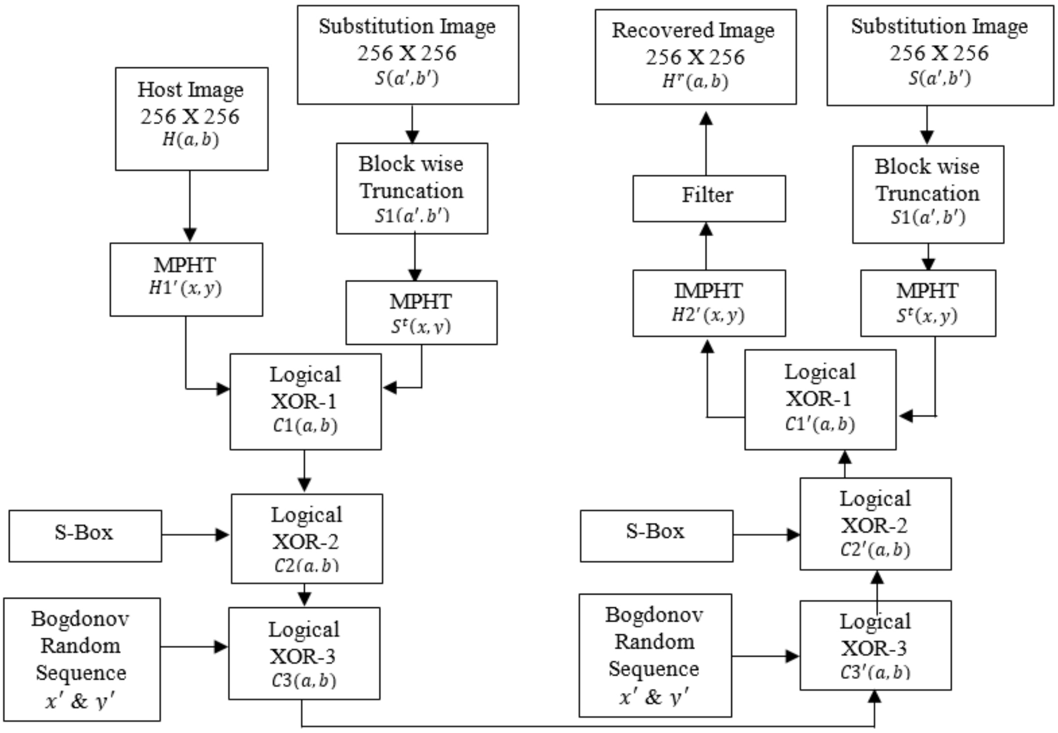


Figure 1. Flow diagram of proposed cryptosystem

2.2. Decryption algorithm

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 cipher image is then subjected for XOR operation with random sequence generated Bogdonav chaotic equation with the same constant co-efficient.

$$x' = (x + y')mod\ 2^n \quad (8)$$

$$y' = (y + \varepsilon y' + Kx'(x' - 1) + \mu x'y')\ mod\ 2^n \quad (9)$$

Where,

ε = 7(d)^2
K = 9(d)^2
μ = 3(d)

$$C2'(x,y) = C3'(x,y) \oplus x' \quad (10)$$

Step2: The obtained cipher image XORed with the elements of S-box used for encryption.

$$C1'(x,y) = C3'(x,y) \oplus S\text{-}box \quad (11)$$

Step3: The block truncated substitution image is subjected for MPHT with same constant and then XORed with cipher image from previous stage.

$$S1'(x,y) = S^t(a'+b'+c) \ mod\ 2^n, (a'+2b'+c) \ mod\ 2^n \quad (12)$$

$$H1'(x,y) = C1'(x,y) \oplus S'(x,y) \quad (13)$$

Step4: the obtained image from previous step is subjected for inverse MPHT to get original image.

$$H^r(a,b) = H1'(5x-4y-c) \ mod\ 2^n, (y-x) \ mod\ 2^n) \quad (14)$$

3. EXPERIMENTAL RESULTS

Standard test images are considered from Computer Vision Group (CVG), Dept. of Computer Science and Artificial Intelligence, University of Granada, Spain. Matlab software is used for performance analysis and implementation. Performance analysis is made based on various security tests. Table 1 compares resultant Entropy, Correlation, UACI and NPCR of different encryption schemes with the proposed system. The results indicates very less correlation between the adjacent pixels after substitution phase along with high entropy value indicating that the pixel values are altered effectively in the cipher image.

Table 1. Comparision of entropy and correlation between standard and encrypted images

Images	Entropy = 8 [14]	Correlation	UACI ≥ 33.4635% [14]	NPCR ≥ 99.6093% [14]
Lena	5.5407 (Blow Fish) [15]			
	5.5438 (Two Fish) [15]		31.00 [16]	90.21 [16]
	5.5439(AES 256) [15]			
	5.5439 (RC 4) [15]	0.1500 [16]		
	7.5220 [16]		33.4201 [19]	99.5859 [19]
	7.9972 [17]			
	7.9950 [18]			
	7.9958 [19]			
	7.6427 [20]		32.01 [22]	99.60 [22]
	7.9971 [21]	0.0020		
	7.9970 [22]		33.4303	99.6063
	7.9973			
Baboon	7.9950 [18]		30.87 [21]	99.59 [21]
	7.9947 [21]	-4.6636e-04		
	7.9968		33.2305	99.5544
Peppers	7.9960 [18]		30.71 [21]	99.61 [21]
	7.9954 [21]	-0.0040	33.3761	99.6490
	7.9973			
Airplane	7.9972	0.0040	33.2971	99.6231
Cameraman	7.9972 [23]	-0.0041	33.3763	99.6201
	7.9975			
Barche	7.9973	0.0048	33.3745	99.6017
Carnev	7.9971	-9.7275e-04	33.3590	99.5651
Donna	7.9973	1.6005e-04	33.4637	99.6460
Foto	7.9968	-0.0028	33.4974	99.5667
Galaxia	7.9972	0.0024	33.4866	99.5773
Leopard	7.9972	0.0013	33.3751	99.5911
Montage	7.9966	-0.0050	33.3403	99.6384
Clock	7.9969	0.0038	33.3330	99.6094
Vacas	7.9974	-4.2689e-04	33.3868	99.6140
Fiore	7.9972	0.0058	33.4856	99.6262
Mapasp	7.9972	0.0040	33.2827	99.6201
Soil	7.9970	0.0026	33.3852	99.6017
Mesa	7.9976	0.0077	33.3114	99.6155
Papav	7.9969	4.2616e-04	33.4553	99.6216
Tulips	7.9974	0.0058	33.4337	99.5987

3.1. Noise interference

The correlation coefficient decides the similarity between retrieved (decrypted) and original images [24]. The performance analysis of decrypted image under noisy condition is decided by comparing the correlation coefficient between decrypted and original images. Figure 2 illustartes retrieved and original image under different noisy conditions and Table 2 discribes the similarity in the order of correlation between the de-crypted and original images under noise interference. If the correlation coefficient is equal to unity, the retrieved image is same as that of the original watermark. The cipher image is considered under various noisy conditions and the performance analysis of the algorithm is made after decrypting the noisy cipher image.

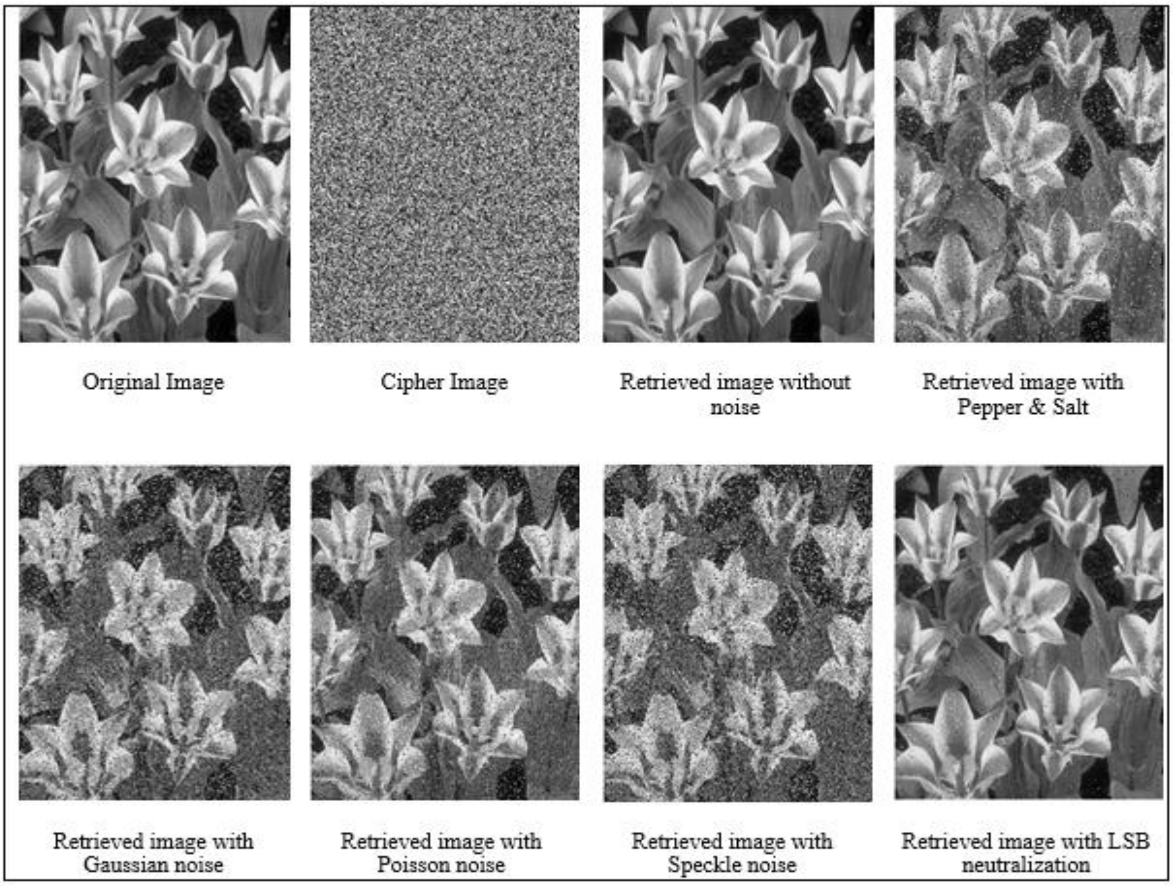

Original Image
Cipher Image
Retrieved image without noise
Retrieved image with Pepper & Salt
Retrieved image with Gaussian noise
Retrieved image with Poisson noise
Retrieved image with Speckle noise
Retrieved image with LSB neutralization

Figure 2. Performance analysis of retrieved and original image under noisy conditions

Table 2. Performance analysis of retrieved and original image under noisy attacks

Noise Interference	Correlation
Pepper & Salt	0.8617
Gaussian	0.7062
Poisson	0.8449
Speckle	0.6527
LSB neutralization attack	0.9790

3.2. Inference

The correlation co-efficient value drops to a minimum 0.6527 with speckle (multiplicative) noise in cipher image indicating 65% similarity between the corresponding pixels in original and retrieved images. Due to LSB neutralization attack, the correlation co-efficient of 0.9790 is observed indicating 98% similarity between original and retrieved images. It has been observed that, an average of 81% similarity between original and retrieved images is observed under noisy conditions. And hence the proposed algorithm gives better results under noise attacks. Figure 3 illustrates similarity in the order of correlation between the de-crypted and original images under different noise densities. Figure 4 Illustration of resultant images under different stage of the crypto-process. Also very close to the ideal values of Unified Average Changing Intensity (UACI=33.39%) but slight less and Number of Pixel Changing Rate (NPCR=99.61%) equal to the ideal value, slightly greater than that as observed in non-Chaotic substitution [25] are noticed from the outcome of the standard images.

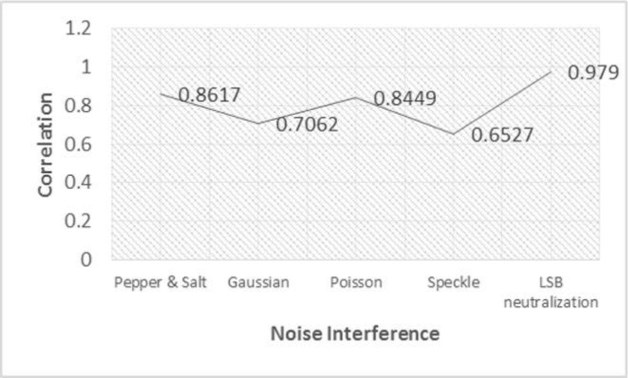
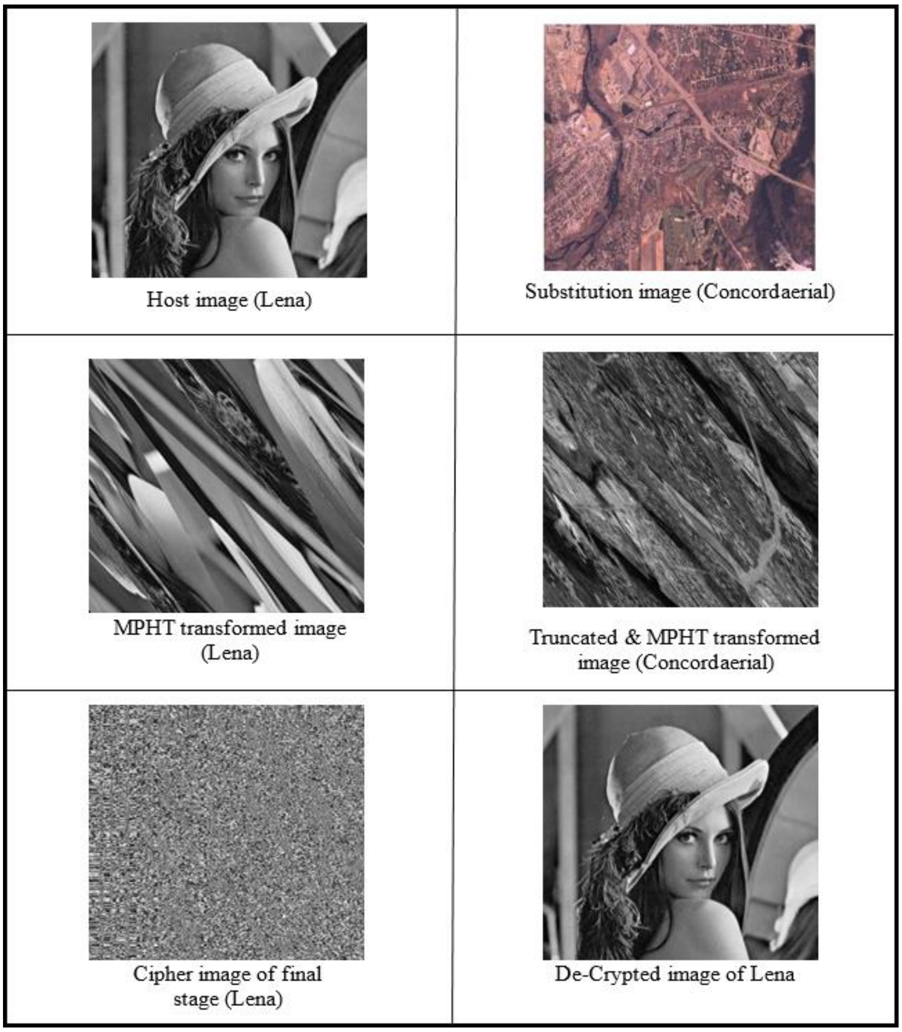


Figure 3. Correlation between the retrieved and original watermarks under noise interference


Host image (Lena)

Substitution image (Concordaerial)

MPHT transformed image (Lena)

Truncated & MPHT transformed image (Concordaerial)

Cipher image of final stage (Lena)

De-Crypted image of Lena

Figure 4. Illustration of Host image, Substitution image and Cipher image after transformation, diffusion and substitution stages

4. CONCLUSION

In the proposed encryption scheme, Pseudo Hadamard transformation is used in the transformation stage to vary pixel positions and Bogdonov chaotic random sequence generator is used in the substitution stage to vary the pixel values in an image. High redundancy and strong correlation between the adjacent pixels are effectively reduced by the proposed technique. High degree of randomness obtained from Bogdonav chaotic generator in the substitution stage leads to achieve better entropy in the cipher image. Correlation between host and cipher images is very less indicating poor similarities between them. Average values of 99.61% number of pixel changing rate (NPCR) is observed which is almost equal to the ideal value and an average value of 33.39% unified average changing intensity (UACI) is obtained which is very close to the ideal values, for a set of twenty standard images. Further, more number of chaotic generators can be used to get random sequences for substitution stage of encryption to increase the level of security.

REFERENCES

[1] Leo Yu Zhang, *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.

[2] Alireza Jolfaei, *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, 2016.

[3] Yue Wu, *et al.*, "Discrete Wheel-Switching Chaotic System and Applications," *IEEE Transactions on Circuits and Systems*, vol. 61, no. 12, pp. 3469-3476, 2014.

[4] Prajwalasimha S N, *et al.*, "Performance analysis of DCT and successive division based digital image watermarking scheme," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 15, no. 2, pp. 750-757, 2019

[5] Prajwalasimha S N, *et al.*, "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,* Springer, Cham, vol 30, 2019.

[6] Prajwalasimha S N, *et al.*, "Performance Analysis of Combined Discrete Fourier Transformation (DFT) and Successive Division based Image Watermarking Scheme," *International Journal of Recent Technology and Engineering*, vol. 8, no. 3, Sep. 2019

[7] Prajwalasimha S N, *et al.*, "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*, Springer, Cham, vol. 30, 2019.

[8] Sanjeev Sharma, *et al.*, "Improved method for image security based on chaotic-shuffle and chaotic diffusion algorithms," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 1, pp. 273-280, 2019.

[9] Samar M. Ismail, *et al.*, "Generalized double-humped logistic map-based medical image encrytpion," *Journal of Advanced Research, Elsevier*, vol. 10, pp. 85-98, 2018.

[10] V.M. Silva-García, *et al.*, "Substitution box generation using Chaos: An Image Encryption Application," *Applied Mathematics and Computation, Elsevier*, vol. 332, pp. 123-135, 2018.

[11] Lingfeng Liu and Suoxia Miao, "A new image encryption algorithm based on logistic chaotic map with varying parameter," *SpringerPlus*, vol. 286, no. 5, pp. 1-12, 2016.

[12] Rasul Enayatifar, *et al.*, "Image encryption using a synchronous permutation-diffusion technique," *Optics and Lasers in Engineering, Elsevier*, vol. 90, pp. 146-154, 2017.

[13] Lingfeng Liu, *et al.*, "Image block Encryption method based on chaotic maps," *IET Journal on Signal Processing*, vol. 12, no. 1, pp. 22-30, 2018.

[14] Xingyuan Wang, *et al.*, "An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map," *IEEE Access Lett*, vol. 6, pp. 23733-23746, 2018.

[15] Delong Cui, *et al.*, "Image Encryption Using Block Based Transformation With Fractional Fourier Transform," *Proc. of 8th International Conference on Communications and Networking in China*, pp. 552-556, 2013.

[16] Nitumoni Hazarika, *et al.*, "A Wavelet Based Partial Image Encryption using Chaotic Logistic Map," *Proceedings of IEEE International Conference on Advanced Communication Control and Computing Technologies*, pp. 1-5, 2014.

[17] Prajwalasimha S.N., "Pseudo-Hadamard Transformation-Based Image Encryption Scheme." In: Krishna A., Srikantaiah K., Naveena C. (eds) *Integrated Intelligent Computing, Communication and Security, Studies in Computational Intelligence*, Springer, Singapore, vol. 771, 2019.

[18] Anish Goel and Kaustubh Chaudhari, "Median Based Pixel Selection for Partial Image Encryption," *Proc. of Sixth International Conference on Image Processing Theory, Tools and Applications*, 2016.

[19] Zaheer Abbas Balouch, *et al.*, "Energy efficient image encryption algorithm," *Proc. of International Conference on Innovations in Electrical Engineering and Computational Technologies*, 2017.

[20] S N Prajwalasimha, Usha Surendra, "Multimedia Data Encryption based on Discrete Dyadic Transformation," *Proc. of IEEE International conference on Signal processing and Communication*, pp. 492-495, 2017.

[21] Nabil Ben Slimane, *et al.*, "Nested chaotic image encryption scheme using two-diffusion process and the Secure Hash Algorithm SHA-1," *Proc.of 4th International Conference on Control Engineering & Information Technology,* 2016.

[22] Prajwalasimha S N and S. R. Bhagyashree, "Image Encryption using Discrete Radon Transformationand Non chaotic Substitution," *Proc. 2nd IEEE International Conference on Electrical, Computer and Communication Technologies*, pp. 842-846, 2017.

[23] Prajwalasimha S N, Kavya S R and Tanaaz Zeba Ahmed, "Design and Analysis of Pseudo Hadamard Transformation and non-Chaotic Substitution based Image Encryption Scheme," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 15, no. 3, 2019.

[24] Shetter A., *et al.*, "Image de-noising algorithm based on filtering and histogram equalization," *Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC*, pp 325-328, 2018.

[25] Prajwalasimha S N and Basavaraj L, "Design and Implementation of Transformation and non-Chaotic Substitution based Image Cryptosystem," *International Journal of Engineering and Advanced Technology,* vol. 8, no. 6, pp. 1079-1083, 2019.

BIOGRAPHIES OF AUTHORS

Prajwalasimha S N received Bachelor of Engineering (B.E) Degree in Electronics & Communication from Visvesvaraya Technological University, India in 2012, Master of Technology (M.Tech) Degree in Digital Electronics & Communication Systems from Visvesvaraya Technological University, India in 2014 and pursuing Doctoral Degree (Ph.D) in the field of Cryptography under Visvesvaraya Technological University, India. He has published more than 20 research papers in International Journals, Conferences & Book Chapters and serving as Reviewer for many International Journals and Conferences. He has been conferred with best research contribution award from *IEEE ICECCT 2017.* His research interest includes Cryptography, Steganography, Digital Image Watermarking and Image Processing.

Dr. L Basavaraj received Bachelor of Engineering (B.E) Degree in Electrical & Electronics Engineering from University of Mysore, India, Master of Technology (M.Tech) Degree in Digital Electronics from Darwad University, India and Doctoral Degree (Ph.D) in the field of Image & Signal Processing under University of Mysore, India. He has published more than 40 research papers in International Journals, Conferences & Book Chapters and currenty guiding 7 Ph.D scholars. Being senior member of *IEEE,* his research interest includes Image & Signal Processing.