LIGHT WEIGHT HYBRID CHAOTIC BASED ENCRYPTION SCHEME FOR IMAGE TRANSMISSION IN WIRELESS MULTIMEDIA SENSOR NETWORK

Basavaraj Patil

Assistant Professor, Sri Dharmasthala Manjunatheshwara Institute of Technology,
Ujire – 574240, Dakshina Kannada
Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India
bbpatilcs@gmail.com

Sangappa Ramachandra Biradar

Professor, SDM College of Engineering and Technology,
Dharwad, Karnataka 580001, India
srbiradar@gmail.com

Abstract

In the present technology growth, the need of multimedia data transmission. The key challenge to provide the secured data transmission in WMSNs owing to their tough situations. In this paper, a novel light-weight hybrid 3D chaotic based encryption algorithm is developed to address the issue of transmission of information securely. The proposed technique consists of two the combination of chaotic encryption scheme and cryptographic methods to build a secured technique. Initially, the input image of the size M*N is considered in which the first 128-bit of the data is processed with Chaotic encryption scheme and remaining 128-bit with 3D Logistic Map based encryption to generate the pseudo random key values, the input is encrypted. In the OMNET++ simulated environment, the encrypted cipher image is transmitted and decrypted at the receiver end. By the experimental analysis results, the proposed algorithm exhibits as efficient and secure compared to existing algorithms.

***Keywords*: Attacks, Chaotic System, Logistic map, Multimedia, WMSN.**

1. Introduction

In this technological era, the rapid evolution of the communication and internet usage has enhanced the huge quantity of multimedia data like text images, audio, video, etc. are generated with the wireless sensors network. In which, the research on the image data transmission is one of the most trending area of interest. In the wireless sensor network, the process of dealing with the multimedia data is hectic and challenging due the security vulnerabilities. In this regard, the various authors have proposed different conventional cryptographic algorithms like DES, IDEA, AES, 3DES etc., [1-2]. But, according to [4], the traditional crypto-algorithms are not fully serving the present needs for multimedia sensor data. As these algorithms have larger key size, requires more storage capacity, more iterations and inefficient in encrypting large-sized images. The intrinsic features of image like higher pixel correlation between adjacent pixels, strong redundancy, etc. are the most challenging to address in the broad area of sensor networks.

The new modern techniques are required to perform the faster encryption and authentic transmission of the data along with the good efficiency. If the time taken to encrypt is more, then the processing speed decreases for the larger data.

Chaos-based cryptosystem [5] proposed to meet the necessity of image encryption with faster encryption and higher efficiency. Currently, the research is being carried out on the chaos-based cryptosystems for efficient key generation, key-exchange, and secured data transmission techniques. Edward Lorenz used the concepts of chaos theory in 1963 for the first time in the computer system.

Presently, the cryptography algorithms based on chaotic system capture the interest for the addressing the major concerned issue like ergodicity, noise-like signals for intruders, and sensitivity to initial conditions by providing the better solution to generate ciphers using such as confusion and diffusion [6-7].

According to literature review, the researchers [4-12] proposed and developed efficient chaotic algorithms to provide secure data transmission from cryptanalytic attacks. The chao based algorithms are based on two types viz., position permutations (pixels are permuted without modifying the actual values of input) and value transformations (pixel value is substituted by other pixel value not changing the location).

The XOR operation is used to exhibit the linear independency of two or more elements. The use of XOR operation in encryption makes it unbearable to inverse the operation without the initial conditions of arguments. The shuffling of the bits position in a plain image and shifting the values of the shuffled bits can have more secured image encryption process. The lightweight hybrid 3D chaotic based encryption scheme is proposed by considering XOR based encryption technique using 3D logistic maps [41-44] to provide the secured encryption to generate the cipher image and secured image transmission in an OMNET++ simulation environment. The rest of the work is as follows.

The study of existing mechanisms presented in section 2. The background study of Chaotic Map & 3D Multiscroll is discussed in section 3. The developed hybrid image encryption techniques detailed in section. Statistical performance analysis is compared with some existing algorithm and discussion in section 5 and followed by the conclusion.

2. Literature Review

The proposed encryption algorithm [3] is designed based on chaotic variable-parameters and dynamics. The authors claim the results show that the proposed technique is better and competitive with existing. The dynamical algorithm built with shuffling of pixels subjected to the mathematical objects and code transformation to generate driven sequence.

The S-box algorithm is proposed [11] for the image encryption process. The original input image is XORed with the chaos based RGN mechanism and sub-byte operation is performed with proposed S-Box algorithm to encrypt the image. The NIST tests are carried out to test the proposed algorithm. The experimental results say that the proposed algorithm produces better results when compared to Chaos and AES algorithm. They also performed the security analysis and key space analysis to prove the stability of the proposed algorithm.

The chaotic behavior with non-equilibrium system [12] is implemented with the real electronic circuit for the image encryption application. The design includes the generation of three s-boxes with cryptographic properties. According to the authors, implementing the system with real-time circuits provide feasibility to verify the theoretical methods. The measurements are evaluated by using oscilloscope. The method show that the results are non-linear with the performance analysis. The sub byte operations exhibit the better encryption results with the chosen s-box and also presented the time taken for encryption process verified by phase portraits, Lyapunov exponents, and entropy.

In the rapid growth of wireless communication, the need for secure data transmission with efficient encryption and decryption mechanism are much needed. The chaotic s-box based image encryption technique is presented [13] and tested for the effective image transmission. The authors considered the Sine & tent maps to improve the 1D chaotic maps, then proposed s-box generating techniques is applied to create the s-box to encrypt the given image. The Lyapunov Exponent and bifurcation diagram of the Sine map justifies the dynamic behaviour of the system. The proposed dual s-box based encryption algorithm is tested for the known and chosen simple plain-text attacks and cipher-text attacks along with statistical analysis.

The evolution of data processing in the medial field is much needed area of research to prevent the chronic diseases like hypertension, BP and sugar. The design of wearable secured application can help in resolving the collection of the real-time data for the study and treatment of such diseases in the wireless body area network (WBAN). Wei Wang and et.al [14], presents the chaotic based secure data transmission in WBAN by the collection of physiological information with the help of sensor nodes to process efficiently. The Logistics and Kent based chaotic maps are used to construct the sub-chaotic matrices to obtain the encrypted chaotic matrix, XORed with original matrix elements to get the encrypted output image. The visual result, quantitative results and key-space analysis tests ate performed.

The cryptosystem is proposed [15] for the encryption process with Tangent Delay Ellipse Reflecting Cavity Map System (TD-ERCS) maps and Piecewise Linear Chaotic Map (PWLCM). The encryption process includes the generation of keys with hashing and set with initial conditions for each round of confusion & diffusion, then applied with affine transformation on every pixel to generate the cipher pixels. The experimental analysis is carried out with statistical analysis, PSNR, key-space & sensitivity analysis to prove the sensitivity for small pixel distribution and attacks.

The implemented algorithms [16] help to encrypt the binary images and their databases of the same size. The binary image is split vertically or horizontally into blocks, reconstruct the new image of the same size with transformation of pixels. The experiment is conducted on few binary images and a data-set with numerical and visual tests to prove the efficiency of algorithm.

Ahmed G. Radwan. et.al [17] reviewed 27 different encryptions using by experimental analysis and the comparison of various discrete chaotic maps, non-chaotic key generators are discussed. They also presented the list of various available statistical analysis methods to validate the efficiency of algorithm in terms of key sensitivity, histogram-analysis, entropy, etc. The permutation techniques based on logistic maps, based on indices, Arnold's cat, Lorenz system, Chess algorithm and mixed permutation-substitution are investigated at different phases. Also, concluded with NIST standard tests to be performed.

3. Background Study

3.1. Logistic Map

Logistic Map is a non-linear polynomial & dynamical equation of degree 2 with complex chaotic behaviours [17]. The Eq. (1) is used to generate random number sequence by appropriate selection of seed value (X_n) and growth rate (r).

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

Where, r $\in$ (0, 4) growth rate/control parameter, a positive value
$X_n \in$ (0, 1) the seed value

In this method, two-random number sequences are generated based on 3D logistic map, in which one random sequence is used for row shuffling and another random sequence for column shuffling. The logistic sequence exhibits different characteristics for the values of r and the logistic sequence presents diverse characteristics [18]. The equation (1) has a positive Lyapunov exponent and behaves chaotic for the values $3.43 \leq$ r ≤ 4 . Hence, the values generated (x_0, r) can be used as secret keys, where $x_0 \in$ (0, 1) and $3.58 \leq$ r ≤ 4. For the values of r > 4 behaves more chaotic, make the system very complex and unable to predict keys.

3.2. 3D Multi Scroll Chaotic Systems

The non-linear systems with multiscroll attractors behave complex as compared to the basic mono-scroll chaotic attractors. The state space equation for automatic chaotic system is given by Eq. (2),

$$\begin{aligned} \dot{x}_1 &= -ax_1 + bx_2x_3 \\ \dot{x}_2 &= -cx_2^3 + dx_1x_3 \\ \dot{x}_3 &= ex_3 - fx_1x_2 \end{aligned} \tag{2}$$

The 3D chaotic Eq. (2) is modified by the hyperbolic function $p_1\, tanh(\, x_2 + g)$ as given in Eq. (3).

$$\begin{aligned} x_1 &= -ax_1 + bx_2x_3 \\ x_2 &= -cx_2^3 + dx_1x_3 \\ x_3 &= ex_3 - fx_1x_2 + p_1\, tanh(\, x_2 + g) \end{aligned} \tag{3}$$

The initial condition values are $[x_1(0), x_2(0), x_3(0)] = [0.1, 0.1, 0.6]$ chosen by the iterative method. Later, chaotic attractor calculated for values of $a = 2$, $b = 6$, $c = 6$, $d = 3$, $e = 3$, $f = 1$, $p_1 = 1$, $g = 2$.

Table 1: Initial values for multi scroll property

State	p_1	g	Initial Values $[x_1, x_2, x_3]$	Attractor	Remarks
First	-	-3	[0.1, -0.1, -0.6]	Double-scroll	Based on the values of p_1 and g, system holds multiscroll property
Second	-1	-3	[0.1, -0.1, -0.6]	Four-scroll	
Third	1	3	[0.1, 0.1, 0.6]	Single scroll	

It is observed that the system holds multi scroll property by changing the values of 'p1' and 'g' in third state with hyperbolic function as in the Table 1. Hence, the behavior of the system depends much on parameter 'g'. The Eq. (3) are revised by applying derivative properties [19] to exhibit the multi scroll chaotic systems as in Eq. (4).

$$\begin{aligned} \frac{d^q x_1}{dt^q} &= -ax_1 + bx_2x_3 \\ \frac{d^q x_2}{dt^q} &= -cx_2^3 + dx_1x_3 \\ \frac{d^q x_3}{dt^q} &= ex_3 - fx_1x_2 + p_1\, tanh(\, x_2 + g) \end{aligned} \tag{4}$$

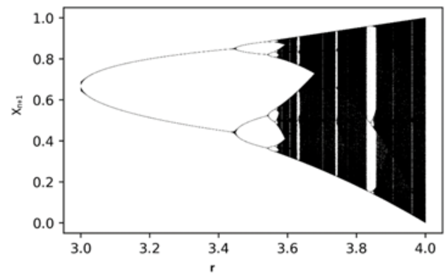

Fig 1: The Bifurcation Diagram for the Multi Scroll Chaotic Systems.

The defects can be witnessed in the bifurcation diagram of the chaotic systems in Fig. 1. It bifurcates less for the value initial values of r and the chaotic ambit/bifurcation is more within 3.57 and 4. The variation on the behaviour of chaotic sequence generated with the change of r [1,4] does not have the uniform distribution, hence it can't be assumed to have similar behaviour.

4. Proposed Technique

The design of the developed chaotic based encryption process is shown in Fig. 2. The input image of the size 256 x 256 is given as an input, then converted to grayscale. The method is designed based on the network centric, consists of two phases.

In first phase, the initial conditions are chosen to form the chaotic equations and pseudo random key (k1) is generated and in second phase the inter-byte operations are performed on the input image, then XORed with permutations and diffusion techniques to generate another key is generated (k2). The key k1 and k2 are XORed to get final key (key = k1$\oplus$k2). Finally, the full stream input image is encrypted using the combination of generate key to generate the encrypted cipher image [28-29].

The following process is incorporated for a Hybrid Chaotic Encryption Mechanism:
Step 1: Consider an image X of size M*N
Step 2: Calculate S1 using network centric chaotic encryption and S2 using 3D logistic map.
Step 3: Encrypt input image X with S1 to get cipher

$$G = \{g1, g2, g3, \ldots\ldots gL\} \text{ by}$$
$$\mathrm{I} = mod\,(1+m, L) + 1 \qquad \text{for I = 1, 2 …. L} \qquad (5)$$
$$g(L) = mod(Inter\_byte\{S1, X(i) + r, 256\}) \qquad \text{for i = 0, 1, 2 . . . L}$$

Where, interbyte (S1, X(i)) → substitution bytes by S1 for X.

The encryption between the 3D Network Centric and Plain image bytes X is based on cross permutation and diffusion process which yields high secured intermediate sequences.

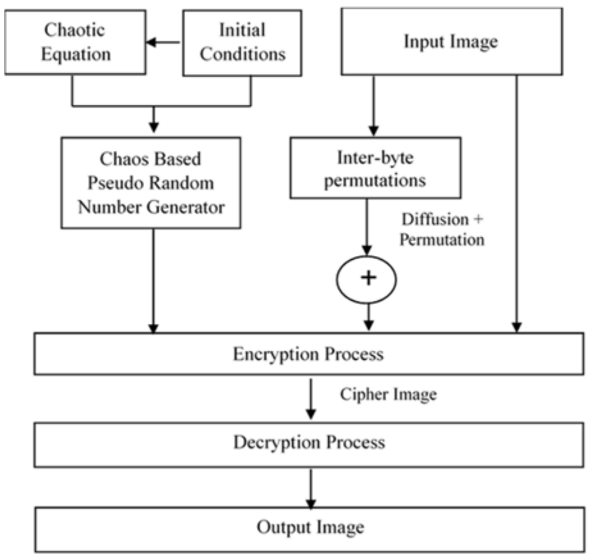

Fig 2: The proposed encryption scheme

Step 4: Again, encrypt the intermediate cipher image G with S2 to get final cipher

$F = \{f1, f2, f3, \ldots..gL\}$ by

J= $mod\ (1 + m, L) + 1$ for J=1,2 ………L

$g(L) = mod(Inter\_byte\{S2, G(i) + r, 256\})$ for i= 0,1,2 …. L (6)

where, interbyte (S2, G(i)) →substitution bytes by S2 for G. Now, the cross permutation and diffusion process performed as in previous cases to get the more chaotic encrypted data.

5. Statistical Performance Analysis

The experimental results carried out on the proposed hybrid chaotic system. The proposed system is tested with distinct standard image like lena image, pepper image, and mammogram image of size 256x256 shown in Fig. 3. The analysis results prove that the encrypted images are really unrecognizable.

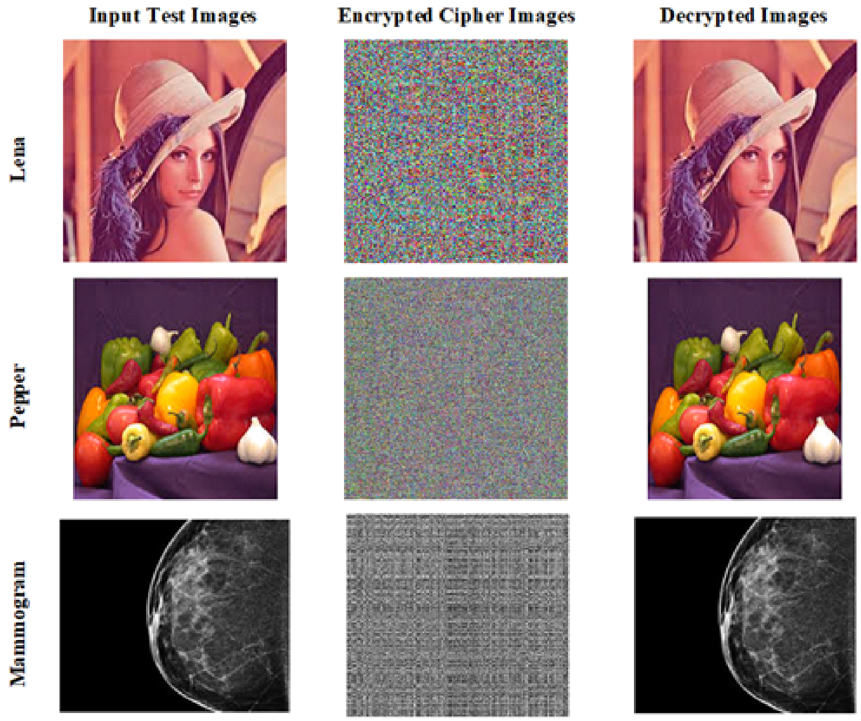

Fig 3: Encrypted and decrypted images

5.1. Histogram analysis

The modified distribution features are the main concern in image processing and encryption process. The image histogram shows in what way pixels in an image are scattered at each intensity level of pixels. The histograms of the input test image, and encrypted cipher images as shown in Fig. 4. The histogram variance measures the pixel distribution of encrypted images, lesser the variance higher the uniformity of pixel distribution in image [31]. The histogram variance is calculated using Eq. (7).

$$var(Y) = \frac{1}{n^2} \sum_{i=0}^{n} \sum_{k=1}^{n} \frac{1}{2} \left(y_i - y_j\right)^2 \quad (7)$$

where, Y → the vector of histogram value

y_i, y_j →the no. of grey pixels i and j

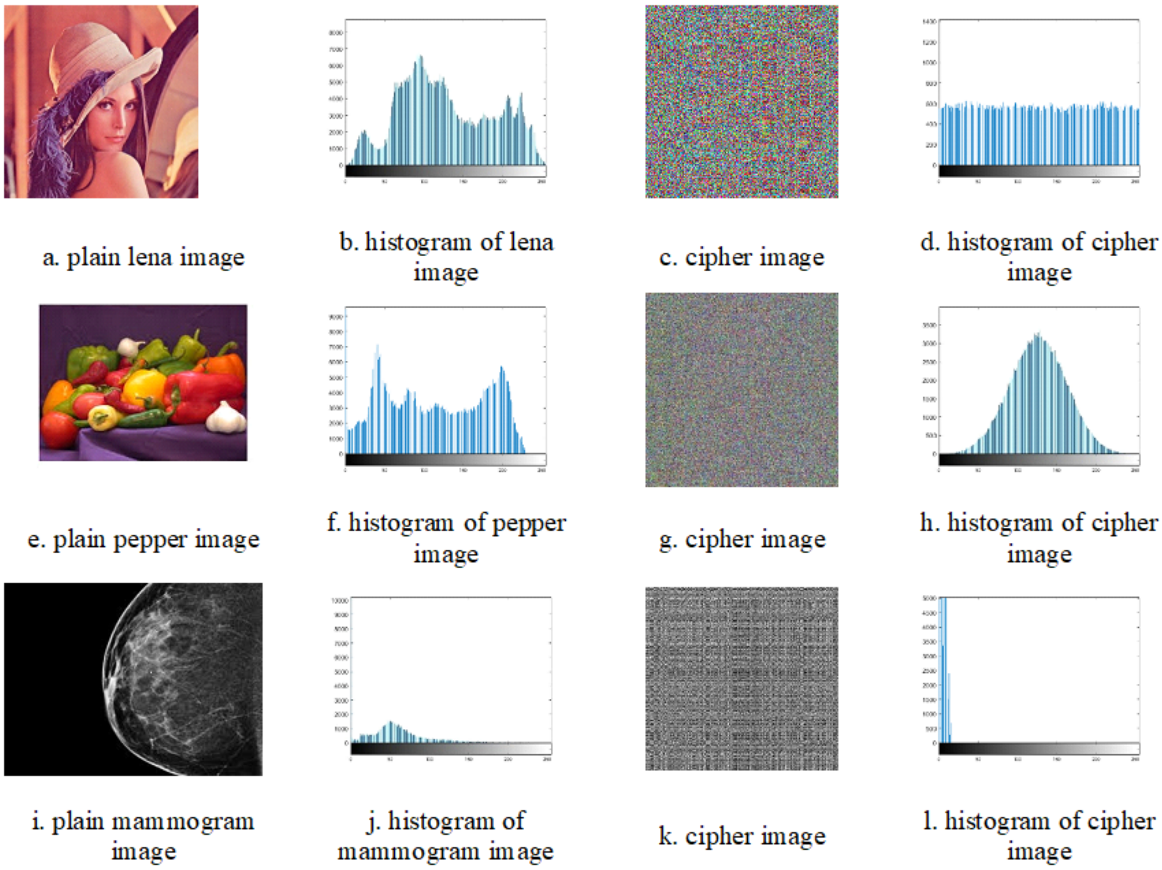

Fig 4: Histograms of the plain input images and cipher images

Table 2: Analysis of histogram variances

	Histogram Variance		
Input Image→	**Lena**	**Peppers**	**Mammogram**
Cipher image (Proposed)	185.459	213.902	223.78
Aruna S et al. [21]	190.455	214.560	234.90
Zhu et al. [13]	221.84	224.35	-
X. P. Zhang et al. [22]	284.44	269.34	-
X. Wang et al. [12]	283.156	227.56	-
Çavuşoğlu et al. [11]	381.67	332.89	-

The histogram variance values of test input and its respective cipher images presented in Table 2. The variance values are evident that, the proposed method has higher uniformity and uniform distribution of pixels as compared to the existing methods. Hence, the proposed scheme is robust and withstands statistical attacks.

5.2 Differential attack analysis

It is utmost important to validate the sensitivity of key generated for its resistance towards mild to strong attacks. The initial values of the chaotic sequence for the generation of key are real numbers, the slight variation gets more changes in the encrypted cipher image. Thus, it's necessary to resist against differential attacks. The important parameters to test the performance of encryption key includes Number of Pixels Shift Rate (NPCR) and Unified Average Changing Intensity (UACI) are the preferred security analyses technique [32-33]. NCPR find the pixels changes in original image, and UACI estimates the mean values of intensity between original and encrypted image.

The NPCR and UACI are calculated using the Eq. (8) and Eq. (9)

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W*H} * 100 \quad (8)$$

$$UACI = \frac{1}{W*H} \sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{256} * 100 \quad (9)$$

where, C1 and C2 → Cipher images
W and H → width and height of C1 and C2 of size (i, j)
D → Bipolar image of size (i, j)

$$D(i,j) = \begin{cases} 1, & C1(i,j) \neq C2(i,j) \\ 0, & C1(i,j) = C2(i,j) \end{cases}$$

The result shown in Table 3 proves that the proposed algorithm is sensitive to the key for various input test images and it guarantees the security against attacks[22].

Table 3: Cryptoanalysis values for the encrypted images

	Input→	Lena	Pepper	Mammogram
Proposed Method	**NPCR**	99.82	99.68	99.73
	UACI	33.87	33.83	33.83
Zhu et al. [13]	**NPCR**	99.64	-	-
	UACI	33.55	-	-
X. P. Zhang et al. [22]	**NPCR**	99.6125	99.6102	-
	UACI	33.4823	33.6128	-
Çavuşoğlu et al. [11]	**NPCR**	99.75	99.45	99.7
	UACI	33.94	33.34	33.9
M. B. Hossain et al. [24]	**NPCR**	99.6048	99.5972	-
	UACI	33.5044	33.5189	-

5.3 Adjacent Pixel Point Correlation Analysis

It is quite interesting to estimate the correlation factor of encrypted images. Unlike normal images, the correlation factor is relatively low for any efficient encryption scheme [31]. To present the correlation intuitively, the selected pairs of pixels along diagonal, horizontal or vertical to represent the correlation graph. The pixel correlation is calculated using following Eq (10-13).

$$R_{xy} = \frac{cov(a,b)}{\sqrt{E(x)E(y)}} \quad (10)$$

$$cov(a,b) = E\{[a - E(a)][b - E(b)]\} \quad (11)$$

$$e(a) = \frac{1}{n} \sum_{i=1}^{n} a_i \quad (12)$$

$$L(x) = \frac{1}{n} \sum_{i=1}^{n} [a_i - a(x)]^2 \quad (13)$$

where, e(a) and L(x) indicates the expectancy and variance of input & cipher images. The correlations of original image and cipher are presented in Table 4.

Table 4: Coefficient Analysis and Correlations

Image→	Input			Cipher		
	Horizontal	**Vertical**	**Diagonal**	**Horizontal**	**Vertical**	**Diagonal**
Lena Image	99.466	99.890	99.883	0.0000345	0.003123	0.000201
Peppers Image	235.890	228.900	228.08	0.000785	0.002456	0.002829
Mammogram Image	432.900	444.890	442.900	0.00444590	0.0000732	0.027890

5.4. Information Entropy Analysis

Entropy estimation deals with the amount of haphazardness exist in encrypted image which mirrors the features of the original image. The higher entropy value relates to higher irregularity in the image. The entropy g(m) is calculated using Eq. (14).

$$g(m) = \sum_{l}^{l-1} q(m) \log_2 \frac{1}{q(m_i)} \quad (14)$$

where, l→ is the no. of symbols
$m_i \in m$
$q(m_i)$ → probability of m_i

Table 4: Entropy Analysis for the different encrypted image

	Entropy Values		
Encrypted Image→	**Lena**	**Peppers**	**Mammogram**
Proposed Method	7.999991	7.999990	7.99992
Zhu et al. [13]	7.9976	7.9975	-
X. P. Zhang et al. [22]	7.9992	7.9993	-
M. B. Hossain et al. [24]	7.9890	7.9896	-
Aruna S et al. [21]	7.999989	7.999989	7.999991

The values of entropy vary from 1 to 8 and the value 1 is equated to a dim level and the value 8 is equated to most brightness level. The different entropy values observed for various data sets are tabulated. Table 4 illustrates that the entropies of encrypted image found to be very close to 8.

6. Conclusion

The secured transmission of the multimedia data is one of the vital processes in wireless sensor network. The conventional encryption algorithms have more key size, requires more space, number of iterations are more and less efficient for encrypting of images. The proposed technique is designed based on the 3D chaotic scheme and 3D logistic maps. The combination of 3D chaotic and 3D logistic techniques provide efficient encryption process. The input grayscale image is used to generate pseudo random key values, processed using Chaotic encryption scheme first and then with 3D Logistic Map to get stronger cipher image. The encrypted cipher image is transmitted and decrypted at the receiver end in the OMNET++ simulated environment. The experimental analysis exhibits that the proposed encryption scheme withstands to differential attack and secured compared to existing schemes. In addition, statistical performance analysis is conducted for different elements such as sensitivity to initial conditions, variance of histograms, NPCR, UACI, Adjacent Pixel Point Correlation and information entropy analysis.

Acknowledgement
Authors would like to thank SDM College of Engineering and Technology, Dharwad, SDM Institute of Technology, Ujire and Visvesvaraya Technological University (VTU), Belagavi, Karnataka.

References

[1] M. Kaur et al., "New security approach in real-time wireless multimedia sensor networks," Comput. Electr. Eng., vol. 3, no. 1, pp. 1–12, Dec. 2016. (39-40)
[2] N. A. Wahid, A. Ali, B. Esparham, and M. Marwan, " A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention," J. Comput. Sci. Appl. Inf. Technol., vol. 3, no. 2, pp. 1–7, 2018.
[3] L. Liu and S. Miao, "A ne w image encryption algorithm based on logistic chaotic map with varying parameter," Springerplus, vol. 5, no. 1, pp. 1–12, 2016.
[4] A. Msolli, A. Helali, and H. Maaref, "New security approach in real-time wireless multimedia sensor networks," Comput. Electr. Eng., vol. 72, pp. 910–925, Nov. 2018.
[5] Y. Luo, L. Yao, J. Liu, D. Zhang, and L. Cao, "A block cryptographic algorithm for wireless sensor networks based on hybrid chaotic map," Proc. - 21st IEEE Int. Conf. High Perform. Comput. Commun. 17th IEEE Int. Conf. Smart City 5th IEEE Int. Conf. Data Sci. Syst. HPCC/SmartCity/DSS 2019, no. 3, pp. 2790–2797, 2019.
[6] W. Wang et al., "An encryption algorithm based on combined chaos in body area networks," Comput. Electr. Eng., vol. 65, pp. 282–291, 2018.
[7] J. Ahmad and S. O. Hwang, "A secure image encryption scheme based on chaotic maps and affine transformation," Multimed. Tools Appl., vol. 75, no. 21, pp. 13951–13976, Nov. 2016.

[8] D. Yang, X. Liao, Y. Wang, H. Yang, and P. Wei, “A novel chaotic block cryptosystem based on iterating map with output-feedback,” Chaos, Solitons and Fractals, vol. 41, no. 1, pp. 505–510, Jul. 2009.
[9] I. Mishkovski and L. Kocarev, “Chaos-based public-key cryptography,” Stud. Comput. Intell., vol. 354, pp. 27–65, 2011.
[10] Z. Zhou, H. Yang, Y. Zhu, W. Pan, and Y. Zhang, “A block encryption scheme based on 3D chaotic Arnold maps,” in International Asia Symposium on Intelligent Interaction and Affective Computing, ASIA 2009, 2009, pp. 15–20.
[11] Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, “Secure image encryption algorithm design using a novel chaos based S-Box,” Chaos, Solitons and Fractals, vol. 95, pp. 92–101, Feb. 2017.
[12] X. Wang et al., “S-box based image encryption application using a chaotic system without equilibrium,” Appl. Sci., vol. 9, no. 4, Feb. 2019.
[13] Zhu, Wang, and Zhu, “A Secure and Fast Image Encryption Scheme based on Double Chaotic S-Boxes,” Entropy, vol. 21, no. 8, p. 790, Aug. 2019.
[14] J. Ahmad and S. O. Hwang, “A secure image encryption scheme based on chaotic maps and affine transformation,” Multimed. Tools Appl., vol. 75, no. 21, pp. 13951–13976, Nov. 2016.
[15] A. Houas, Z. Mokhtari, K. E. Melkemi, and A. Boussaad, “A novel binary image encryption algorithm based on diffuse representation,” Eng. Sci. Technol. an Int. J., vol. 19, no. 4, pp. 1887–1894, Dec. 2016.
[16] A. G. Radwan, S. H. AbdElHaleem, and S. K. Abd-El-Hafiz, “Symmetric encryption algorithms using chaotic and non-chaotic generators: A review,” Journal of Advanced Research, vol. 7, no. 2. Elsevier, pp. 193–208, 01-Mar-2016.
[17] F. Özkaynak, “A novel method to improve the performance of chaos based evolutionary algorithms,” Optik (Stuttg)., vol. 126, no. 24, pp. 5434–5438, Dec. 2015.
[18] G. Alvarez and S. Li, “Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems *.”
[19] G. Gugapriya, P. Duraisamy, A. Karthikeyan, and B. Lakshmi, “Fractional-order chaotic system with hyperbolic function,” Adv. Mech. Eng., vol. 11, no. 8, Aug. 2019.
[20] A. S and D. U. G, “HPAC-sbox- a novel implementation of predictive learning classifier and adaptive chaotic s-box for counterfeiting side channel attacks in an IOT networks,” Microprocess. Microsyst., vol. 81, Mar. 2021.
[21] X. P. Zhang, R. Guo, H. W. Chen, Z. M. Zhao, and J. Y. Wang, “Efficient image encryption scheme with synchronous substitution and diffusion based on double S-boxes,” Chinese Phys. B, vol. 27, no. 8, Aug. 2018.
[22] M. K. Mandal, M. Kar, S. K. Singh, and V. K. Barnwal, “Symmetric key image encryption using chaotic Rossler system,” Secure Communication Networks, vol. 7, no. 11, pp. 2145–2152, Nov. 2014.
[23] M. B. Hossain, M. T. Rahman, A. B. M. S. Rahman, and S. Islam, “A new approach of image encryption using 3D chaotic map to enhance security of multimedia component,” in 2014 International Conference on Informatics, Electronics and Vision, ICIEV 2014, 2014.
[24] H. El Zouka, “A Secured Wireless Multimedia Sensor Network,” IJCSIS, J. Comput. Sci., vol. 14, no. 1, pp. 11–17, 2016.
[25] Z. Deng and S. Zhong, “A digital image encryption algorithm based on chaotic mapping,” J. Algorithms Comput. Technol., vol. 13, pp. 1–11, 2019.
[26] X. J. Tong, Z. Wang, and K. Zuo, “A novel block encryption scheme based on chaos and an S-box for wireless sensor networks,” Chinese Phys. B, vol. 21, no. 2, pp. 1–12, 2012.
[27] A. Houas, Z. Mokhtari, K. E. Melkemi, and A. Boussaad, “A novel binary image encryption algorithm based on diffuse representation,” Eng. Sci. Technol. an Int. J., vol. 19, no. 4, pp. 1887–1894, 2016.
[28] M. A. Khan, J. Ahmad, Q. Javaid, and N. A. Saqib, “An efficient and secure partial image encryption for wireless multimedia sensor networks using discrete wavelet transform, chaotic maps and substitution box,” J. Mod. Opt., vol. 64, no. 5, pp. 531–540, 2017.
[29] H. Liu, B. Zhao, J. Zou, L. Huang, and Y. Liu, “A Lightweight Image Encryption Algorithm Based on Message Passing and Chaotic Map,” Secure Communication Networks, 2020.
[30] A. Karthikeyan, V. Srividhya, P. Gupta, and N. Rai, “A hybrid approach for simultaneous compression and encryption of an image in wireless media sensor networks,” Adv. Intell. Syst. Comput., vol. 452, pp. 475–484, 2016.
[31] K. Shankar and M. Elhoseny, “An optimal lightweight cryptographic hash function for secure image transmission in wireless sensor networks,” Lect. Notes Electr. Eng., vol. 564, pp. 49–64, 2019.
[32] Y. Wu, J. P. Noonan, and S. Agaian, “NPCR and UACI Randomness Tests for Image Encryption,” Cyberjournals.Com, 2011.
[33] L. Xu, Z. Li, J. Li, and W. Hua, “A novel bit-level image encryption algorithm based on chaotic maps,” Opt. Lasers Eng., vol. 78, pp. 17–25, 2016.
[34] T. Xiang, C. Yu, and F. Chen, “Secure MQ coder: An efficient way to protect JPEG 2000 images in wireless multimedia sensor networks,” Signal Process. Image Commun., vol. 29, no. 9, pp. 1015–1027, 2014.
[35] M. Ghadi, L. Laouamer, and T. Moulahi, “Securing data exchange in wireless multimedia sensor networks: perspectives and challenges,” Multimed. Tools Appl., vol. 75, no. 6, pp. 3425–3451, 2016.
[36] H. Shen and G. Bai, “Routing in wireless multimedia sensor networks: A survey and challenges ahead,” J. Netw. Comput. Appl., vol. 71, pp. 30–49, 2016.
[37] M. A. Khan, A. Ali, V. Jeoti, and S. Manzoor, “A Chaos-Based Substitution Box (S-Box) Design with Improved Differential Approximation Probability (DP),” Iran. J. Sci. Technol. - Trans. Electr. Eng., vol. 42, no. 2, pp. 219–238, 2018.
[38] J. S. Khan, A. Ur Rehman, J. Ahmad, and Z. Habib, “A new chaos-based secure image encryption scheme using multiple substitution boxes,” Proc. - 2015 Conf. Inf. Assur. Cyber Secur. CIACS 2015, pp. 16–21, 2016.
[39] N. K. Pareek, V. Patidar, and K. K. Sud, “Image encryption using chaotic logistic map,” Image Vis. Comput., vol. 24, no. 9, pp. 926–934, 2006.
[40] M. Guerrero-Zapata, R. Zilan, J. M. Barceló-Ordinas, K. Bicakci, and B. Tavli, “The future of security in Wireless Multimedia Sensor Networks: A position paper,” Telecommun. Syst., vol. 45, no. 1, pp. 77–91, 2010.
[41] Y. Luo, J. Yu, W. Lai, and L. Liu, “A novel chaotic image encryption algorithm based on improved baker map and logistic map,” Multimed. Tools Appl., vol. 78, no. 15, pp. 22023–22043, 2019.
[42] A. U. Rehman, J. S. Khan, J. Ahmad, and S. O. Hwang, “A New Image Encryption Scheme Based on Dynamic S-Boxes and Chaotic Maps,” 3D Res., vol. 7, no. 1, pp. 1–8, 2016.
[43] H. E. D. H. Ahmed, H. M. Kalash, and O. S. Farag Allah, “An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for image encryption and decryption,” Inform., vol. 31, no. 1, pp. 121–129, 2007.
[44] J. Gayathri and S. Subashini, “A survey on security and efficiency issues in chaotic image encryption,” Int. J. Inf. Comput. Secur., vol. 8, no. 4, pp. 347–381, 2016.
[45] C. Li, G. Luo, and C. Li, “A parallel image encryption algorithm based on chaotic Duffing oscillators,” Multimed. Tools Appl., vol. 77, no. 15, pp. 19193–19208, Aug. 2018.

Authors Profile

Basavaraj Patil is presently working as Assistant Professor in the Department of CSE/ISE, SDM Institute of Technology, Ujire, Karnataka, INDIA. He is pursuing Ph.D. in Computer Science and Engineering at Visvesvaraya Technological University, Belagavi. He obtained his M. Tech in Computer Science and Engineering from SDM College of Engineering and Technology, Dharwad and B.E. degrees in Computer Science and Engineering from Rural Engineering College, Hulkoti. His research interest includes Computer Networks, Wireless Sensor Networks, Cryptography.

Dr. Sangappa Ramachandra Biradar is Professor in the Department of Information Science and Engineering, at S.D.M. College of Engineering and Technology, Dharwad, Karnataka, INDIA. He obtained his Bachelor of Engineering from BLDEA's College of Engineering & Technology, Bijapur. He obtained his Master of Technology from M.I.T., MAHE, MANIPAL. He received his Ph.D. from Jadavpur University, Kolkata, INDIA. He is guiding 06 Ph.D. students at Visvesvaraya Technological University, Belagavi, Karnataka. He has published 20 papers at International Journal and 32 at International and National Conferences. He is a life member of ISTE, ACM and IAENG.