A novel Dynamic Key based chaotic image encryption

R.Vidhya* and M.Brindha
Department of Computer science and Engineering,
National Institute of Technology ,Trichy, India
vidhu.cs111@gmail.com, brindham@nitt.edu

Abstract

Many encryption algorithms are proposed based on chaos and many of them have been shown to be successful because of the adapting nature of the traditional confusion-diffusion architecture. Still few problems have been identified. The plain image is not related with the cipher image which induces the chosen /known plain text attack. Further the keys used for the encryption is always fixed and is not chosen dynamically. In order to reduce these flaws, a novel chaotic encryption is proposed with dynamic keys selected from plain image itself. For the key generation, hyper chaos system is used along with the sum of the intensity values to encrypt the image with high security. The pixel change rate and changed intensity values are as high as 99.7123 and 33.4432 respectively which exhibit the resistance against chosen/known plain text attack. Simulations are performed for histogram analysis, correlation between adjacent pixels, entropy analysis and sensitivity analysis which reveals that the proposed scheme have good security which in turn can be adopted for secure communication applications.

Keywords: Hyper chaos, Dynamic keys, Image encryption, Security

1 Introduction

Military, electronic commerce and government related applications use cryptography from 1970's. Because of the evolution of computer and network technologies, multimedia data like images, videos, audio etc are exchanged in various applications like medical sector, bank, mobile transformations etc. Hence there is a need to protect the multimedia information from the attackers before transmission. The secrecy of information is established by enciphering the information using secret key to transform into an unreadable form as cipher. For the encryption of images, the conventional encryption algorithms like Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES), Data Encryption standard (DES), International Data Encryption Algorithm (IDEA), Blowfish etc. are not suitable in view of the implicit properties of image such as enormous data size, high correlation between adjacent pixels and redundancy [12, 14, 13, 17, 19]. Since 1970's a well known mathematical concept is chaos and is used in variety of applications. Chaos is a non-linear dynamical system used for encrypting the images with high randomness. The intrinsic properties of chaos like mixing property, ergodicity, high sensitive to the initial seed/parameters and randomness has been noticed by many researchers for encryption.The mixing property and sensitive to initial conditions of the chaos are used to achieve the confusion and diffusion property of cryptography. A simple algorithm using chaos produces complex and random outputs related to the algorithmic complexity of cryptography. The principal difference between the chaos and cryptography is that,cryptography system deals with the integers [18] while the chaos systems rely on the real numbers [9].Using that features, a series of image encryption algorithms is proposed in [14, 13, 19, 2, 24]. The classical architecture of the chaos based image encryption is given in the Figure 1.
The rest of the paper is described as follows. The review of image encryption techniques is explained in

Journal of Internet Services and Information Security (JISIS), volume: 8, number: 1 (February 2018), pp. 46-55
*Corresponding author

section 2 and the proposed encryption and decryption algorithm are described in section 3. The security analysis iscarried out for the proposed work and discussed in section 4 and finally the paper is concluded in section 5.

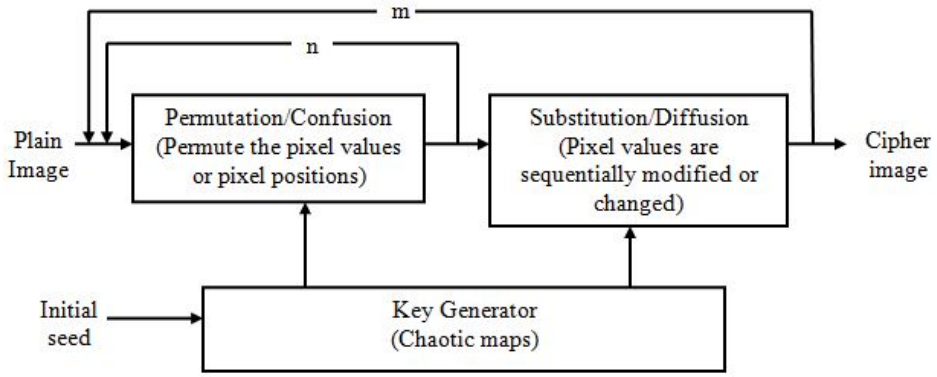


Figure 1: Classical architecture for image encryption

2 Related works

The procedures for designing a chaotic based image encryption system are given in [11] which include the steps involved in choosing a chaotic map, parameters selection, discretize the results to obtain one-to-one mapping and evaluation of security and performance. Jakimoski and Kocarev [10] proposed a block encryption cipher for text encryption and the work is proved against differential and linear cryptanalysis. The first chaos based architecture is proposed by Fridrich [7]. The architecture is defined as two steps i) confusion ii) diffusion. During the confusion phase, the location of pixels is changed and at the diffusion phase intensity values are changed. Many image encryption algorithms, such as bit level permutation methods [3, 8, 20], enchaned substitution method [17], and improved key generation methods [25] reach the best results with these two stages. Moreover, some chaotic algorithms are found to be insecure [12, 1, 6, 22]. The common flaw found from these algorithms is its insecurity against differential attacks. In [22] a new encryption algorithm is implemented using shuffling and tent chaotic map. Further this method is improved by Eslami et al. [6], but this image encryption algorithm is cryptanalyzed by Akhavan et al.[1], in which it is found that this algorithm is resistant to differential attack and vulnerable to known/chosen plain text attack. A few encryption algorithms for images have been suggested based on the correlation with plain text in [4, 21, 23]. Ye et al [21] proposed self-adaptive type block chaotic image encryption based on initial conditions which are combined with plain image in each round. Chen et al. [4], presented a non-linear confusion-diffusion dynamic state variable selection method, in which for the permutation and substitution stage, secret keys are selected dynamically from the plain text. Zhang et al. [23], implemented a new image encryption with temporary value feedback and the secret keys used in the logistic map are computed by the plain image. Chen et al. [5], proposed good diffusion procedures for image encryption. In this, two levels of diffusion are performed and the first level diffusion output is given as the control parameter of the supplementary diffusion. Luo et al. [15], developed a input image related and chaotic map- control- based cryptosystem. In this method, the pixel values of the plain image are first quantified to a decimal value. It can be used as a seed for the tent map and the generated random sequences are modified into two ergodic sequences. Zhu et al.[26], proposed a number theory

based theorem for encryption and compression of the encrypted image but this method is resistant to chosen/known plain text attacks. Norouzi et al.[16], proposed a simple and high sensitive secure image encryption algorithm using hyper chaotic sequences with one round of diffusion.In fact, these methods improve the relationship between plain image and encryption algorithms but still some flaws are not resolved: i) The chosen secret keys for the encryption are not mixed with the plain pixels and this makes the encrypted image vulnerable to differential attacks ii) If one pixel value is modified in the input image, then the effect is not applied to the whole plain image and also the range of changed pixels is limited. To overcome these flaws from the prior analyzes, an efficient dynamic key based encryption based encryption is implemented for image.

2.1 Hyper chaotic system

A hyper chaos system is employed for the key generation of the proposed algorithm and is defined as:

$$\begin{cases} \dot{z} = p(w-z)+wx \\ \dot{w} = rz-w-zx+x \\ \dot{y} = zw-sx \\ \dot{x} = tx-zy \end{cases} \tag{1}$$

where p=35, r=8/3, s=55, and t= 1.3 are the system variables of the hyper chaos system. For solving the equations, 4^{th} order Runge-Kutta method is used and the hyper chaotic sequences$\{(z_k, w_k, y_k, x_k)|k = 1,2,3...\}$ are generated with the initial conditions (z_0, w_0, y_0, x_0)which ranges between 0 to 1.

3 Proposed Algorithm

3.1 Encryption algorithm

Step1: The input image P with size $k = m \times n$ is arranged into a one dimensional vector $v_k = v_1, v_2, \ldots v_{mn}$.The hyper-chaotic system of length k is iterated to get the sequences $z_k = z_1, z_2, ..., z_{mn}, w_k = w_1, w_2, ..., w_{mn}, y_k = y_1, y_2, ..., y_{mn}, x_k = x_1, x_2, ..., x_{mn}$.
Step 2: The key sequence is defined by the following equation (2)

$$Key(k) = mod(v_k, 4); k = 1,2,3...m \times n \tag{2}$$

The key sequence is formed for z_k, w_k, y_k, x_k when $Key(k) = 0,1,2,3$ respectively.
Step 3: The sum of the plain image is computed from the equations (3), (4), (5)

$$Sum = \sum_{j=1}^{k} p_j, \;\; 1 \leq j \leq k \tag{3}$$

The plain image is iterated using

$$sum(j) = Sum - p(j), \;\; 1 \leq j \leq k \tag{4}$$

$$q = floor(mod(\frac{sum(j)}{256^5} \times Key(k) \times 10^{10}, 256)) \tag{5}$$

Step 4: The first pixel is encrypted by (6) using q and the first chaotic key,

$$c_1 = p_1 \oplus mod(q, 256) \oplus Key(1) \tag{6}$$

Step 5: The second pixel value to k^{th} pixel value is encrypted by the previous cipher pixel value using the following equation:

$$c_k = p_k \oplus mod(Key(k) + c_{k-1}, 256) \oplus q \quad 2 \leq k \leq m \times n \tag{7}$$

The encrypted values are stored in an array $C = c_1, c_2, \ldots, c_k$ and converted into a matrix to obtain the encrypted image of size $m \times n$.

3.2 Decryption algorithm

In the decryption side, the key sequences are sent along with the enciphered image for deciphering the image. For the security purpose, the key sequence is XORed with the another random sequence L_s created from the one dimensional chaotic map and the sequence named as U_s. The initial seed is sent via the Diffie-Hellman exchange protocol. In the decryption side, the initial seed of logistic map is set and the random sequence L_s is generated for retrieving the key sequence Key(k). After getting the key sequence, the steps in decryption algorithm are defined as:
Step 1: The cipher image C with size $m \times n$ is reshaped into a one dimensional array $C = c_1, c_2, \ldots c_{mn}$ and the reverse diffusion process is performed from the final pixel to initial pixel. The following equations (8)-(10) are used to decrypt the image.

$$p_k = c_k \oplus mod(Key(k) + c_{k-1}, 256) \oplus q \tag{8}$$

$$Sum = Sum + p(k) \tag{9}$$

$$q = floor(mod(\frac{sum(j)}{256^5} \times Key(k-1) \times 10^{10}, 256)) \tag{10}$$

Step 2: The above steps are performed till k=2 and for the first pixel, the decipher value is computed by the following equation

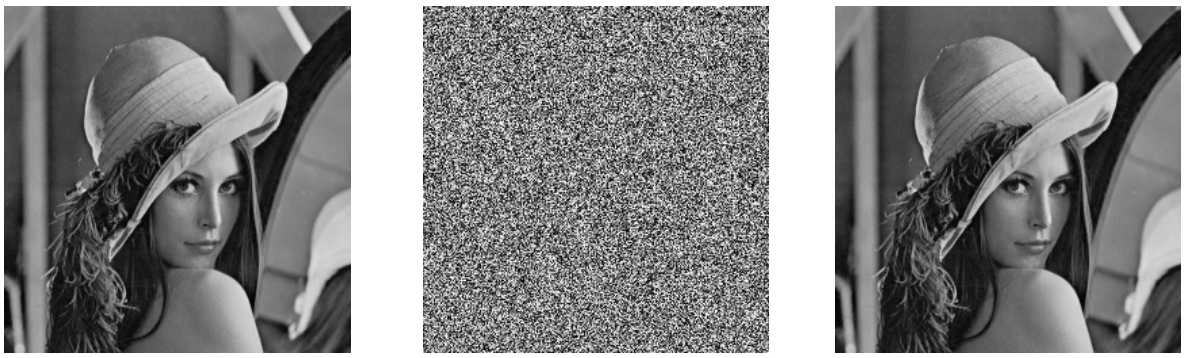
$$p_1 = c_1 \oplus mod(q, 256) \oplus Key(1) \tag{11}$$

Step 3: The plain image is recovered by reshaping the 1-D vector P into a 2-D image of size $m \times n$. Figure 2 illustrates the simulation results of the proposed encryption technique. The unique feature of this algorithm is the dynamic keys that are generated from the plain image that exhibits a high security compared to other existing algorithms. The next section performs the security analyzes of the proposed work.

4 Security analysis

4.1 Key space analysis

The brute force attack is impossible if the space of key is high. The proposed algorithm uses secret keys z_0, w_0, y_0, x_0 from the hyper chaotic system and for the decryption it uses one secret key x_0 for logistic map. IEEE floating point standard indicates that, computer precision is 10^{-14}. According to this precision the key space is as high as 10^{70} which indicates brute force attack is impractical for the proposed method.

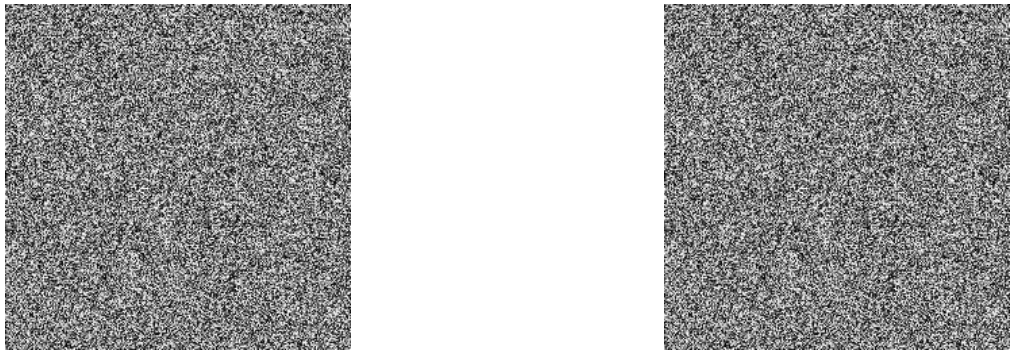


(a) (b) (c)

Figure 2: (a) Input image (b) Enciphered image (c) Deciphered image

4.2 Key sensitivity analysis

This analysis deals with the sensitivity of the two keys applied in this algorithm i) Encryption key: For a slight modification in the encryption key, if the two enciphered images are totally different, then the secret key is highly sensitive to the proposed algorithm. ii) Decryption key: For a small modification in the deciphering key, the deciphered image should be entirely dissimilar from the plain image. The simulations are performed to analyze the algorithm that is proposed. The value of encryption key x_0 is modified into $x_0 + 10^{-14}$and the enciphered image is shown in figure 3a. Also in the decryption side the key y_0 is modified into $y_0 + 10^{-14}$, and the deciphered image is shown in figure 3b. From this analysis it is proved that the secret keys are highly sensitive to the implemented method.

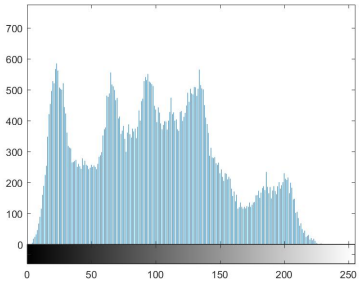


(a) Encrypted image using $x_0 + 10^{-14}$ (b) Decrypted image using key $y_0 + 10^{-14}$

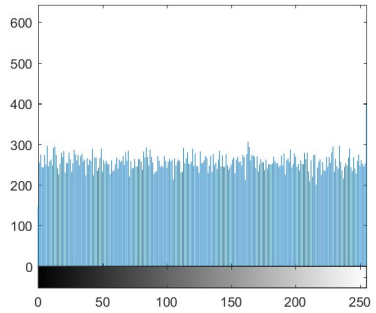
Figure 3: Key Sensitivity test

4.3 Histogram analysis

Histogram reveals the concept of distribution of pixel levels and for an enciphered image the histogram must be uniform and flat. The attackers use the statistical feature to obtain the original image. So, there is a need to hide the statistical details of the plain image. Figure 4a and 4b illustrates the gray level distributions of plain and enciphered image of Lena. It shows clearly that the proposed scheme pixel levels are uniformly distributed which in turn insists that the statistical attack is ineffective.



(a) plain image



(b) cipher image

Figure 4: Histogram analysis

4.4 Correlation analysis

In the plain image, adjacent pixels have strong connection between diagonal, vertical and horizontal directions. If the adjacent pixel correlation is high, some amount of visual information of the encrypted image can be obtained. If the ciphered image correlation is nearer to zero, then the encryption algorithm is effective. The correlation co-efficient r_{st} of pixels is calculated using (12).

$$r_{st} = \frac{E((s-E(s))(t-E(t)))}{\sqrt{V(s)V(t)}} \tag{12}$$

where $E(s)$ is the expectation and $V(s)$ is the variance of the gray-level x respectively.The results obtained from simulation are shown in the Table [1]. Table [3] shows the comparisons of various methods with the proposed work and the proposed scheme has very less correlation for the ciphered image and shows that the proposed method gives high security. Figure 5 illustrates the distribution of neighboring pixels of plain and enciphered image in three directions.

Table 1: correlation coefficient values of Lena

Image	Input image			Encrypted image		
-	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.9436	0.9732	0.9245	3.9721×10^{-004}	-0.0015	0.0011

4.5 Entropy analysis

The entropy of the encryption algorithm is the salient feature of randomness. The formula in (13) is applied to calculate the information entropy.

$$H(x) = \sum_{r=0}^{255} p(x_r) \log \frac{1}{p(x_r)} \tag{13}$$

Where $p(x_r)$ indicates the probability of each pixel x_r and the information entropy value is represented as bits. For the gray scale images, the expected entropy value is 8, and Table [2] gives the entropy value of different images. The average entropy value of proposed scheme is 7.9995 (nearer to 8) and this value is high compared to other schemes as shown in Table [3].

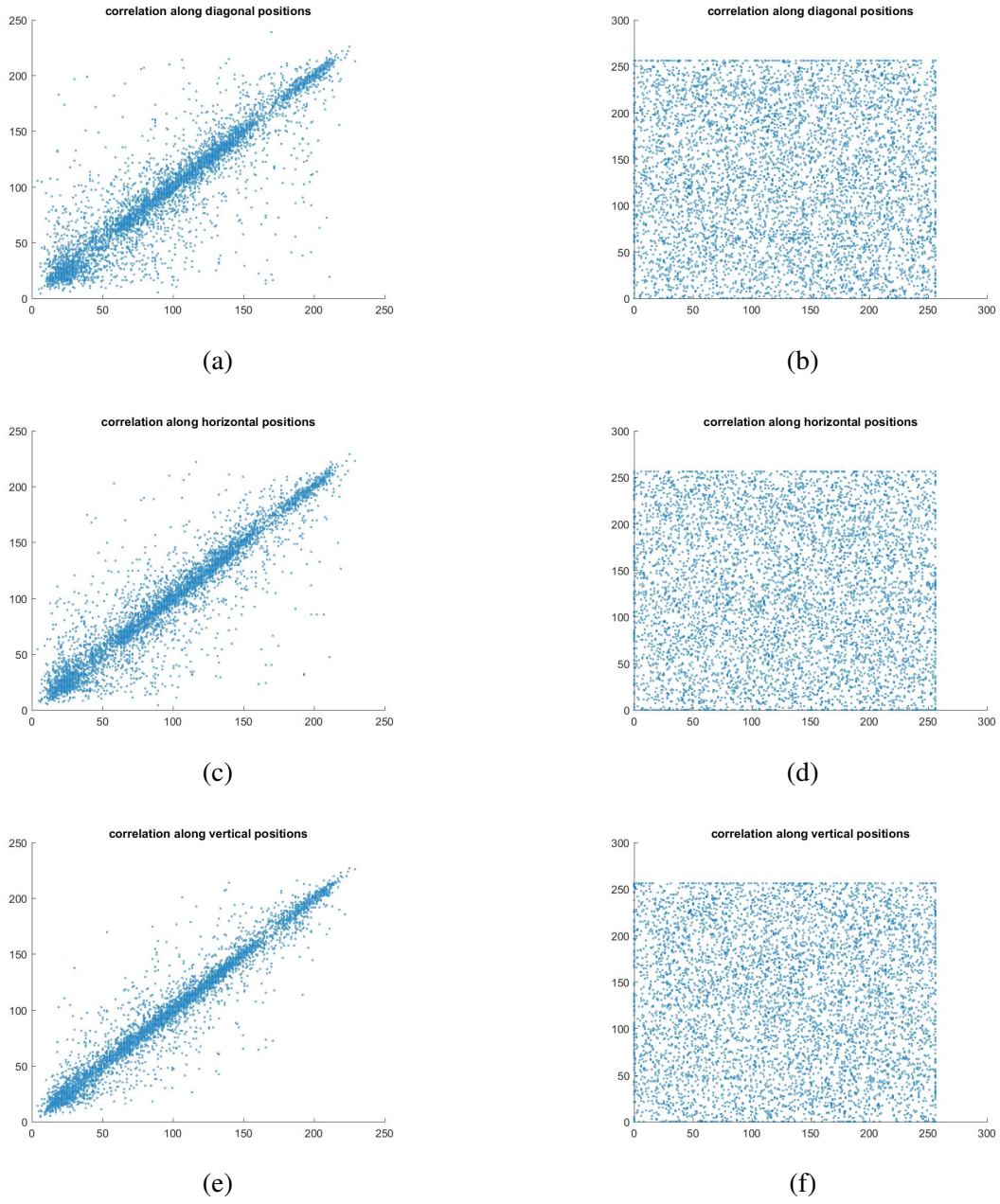


Figure 5: The adjacent pixels are distributed along diagonal, horizontal and vertical positions

Table 2: Entropy analysis

Image	Lena	Baboon	Girl face	pepper	Boat
Entropy	7.9995	7.9972	7.9973	7.9972	7.9973

4.6 Differential analysis

Two common measures are used to analyze the differential attack and they are NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changed Intensity). In this analysis, slight changes are made

Table 3: Comparisons of various image encryption schemes

S.No	Encryption scheme	Entropy	NPCR %	UACI %	Horizontal correlation	Vertical correlation	Diagonal correlation	Algorithm used
1	Ref[2]	7.9931	99.2	33.24	0.001	0.002	0.006	Dynamic S-box
2	Ref[16]	7.9932	99.61	33.42	$7.7491 \times e^{-004}$	0.0045	0.0061	DSVSM
3	Ref[15]	7.9971	99.60	33.41	0.0008	0.0037	0.0001	P-box and skew tent chaotic map
4	Ref[11]	7.9994	99.60	33.36	0.0007	0.0021	0.0148	spatio-temporal and NCML
5	proposed	7.9995	99.71	33.44	3.9721×10^{-004}	-0.0015	0.0011	Hyper chaotic sequence

at the original image and the variations in the corresponding enciphered images are analyzed. The NPCR and UACI are measured by the subsequent formulas (14), (15) and (16).

$$NPCR = \frac{\sum_{x,y} D(x,y)}{m \times n} \times 100\% \tag{14}$$

where D(x,y) is computed by (15)

$$D(x,y) = 1, if c_1(x,y) \neq c_2(x,y) otherwise 0 \tag{15}$$

$$UACI = \frac{1}{m \times n} \sum_{x,y} \frac{c_1(x,y) - c_2(x,y)}{255} \times 100\% \tag{16}$$

where $c_1(x,y), c_2(x,y)$ are the two ciphered images with one pixel change. In the proposed algorithm, NPCR and UACI values are 99.7123% and 33.4432% respectively. Table[3] shows the comparison of UACI & NPCR values with other encryption schemes.

4.7 Speed analysis

Speed of the encryption algorithm is also considered as the crucial factor. So, for the proposed method encryption and decryption time is analyzed. Table [4], shows time for encryption and decryption for different sized images.

Table 4: Speed analysis

S.No	Image	Size	Encryption time in secs	Decryption time in secs
1	Lena	1024×1024	0.1	0.097
2	Girl face	512×512	0.095	0.090
3	Pepper	512×512	0.089	0.088
4	Baboon	256×256	0.053	0.045
5	Barbara	720×576	0.082	0.073

5 Conclusion

A novel image encryption based on chaos has been proposed with dynamically selected key sequences in this paper. The keys are generated dynamically by the hyper-chaotic system along with the input pixels. Since, a minor modification in the input image yields totally different keys, one time encryption is achieved. In addition, sum of the plain pixels is used to encrypting the image. The proposed scheme

has high key space and satisfies statistical test. The pixel change rate and changed intensity values are high to overcome the differential attack and it also has high sensitivity to the key. The entropy value is nearer to theoretical value which shows that the encryption algorithm have good randomness.

References

[1] A. Akhavan, A. Samsudin, and A. Akhshani. Cryptanalysis of an improvement over an image encryption method based on total shuffling. *Optics Communications*, 350:77–82, September 2015.

[2] A. Akhshani, A. Akhavan, S.-C. Lim, and Z. Hassan. An image encryption scheme based on quantum logistic map. *Communications in Nonlinear Science and Numerical Simulation*, 17(12):4653–4661, December 2012.

[3] X. Chai. An image encryption algorithm based on bit level brownian motion and new chaotic systems. *Multimedia Tools and Applications*, 76(1):1159–1175, January 2017.

[4] J.-x. Chen, Z.-l. Zhu, C. Fu, H. Yu, and L.-b. Zhang. A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. *Communications in Nonlinear Science and Numerical Simulation*, 20(3):846–860, March 2015.

[5] J.-x. Chen, Z.-l. Zhu, L.-b. Zhang, C. Fu, and H. Yu. An efficient diffusion scheme for chaos-based digital image encryption. *Mathematical Problems in Engineering*, 2014, March 2014.

[6] Z. Eslami and A. Bakhshandeh. An improvement over an image encryption method based on total shuffling. *Optics Communications*, 286:51–55, January 2013.

[7] J. Fridrich. Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and chaos*, 8(6):1259–1284, June 1998.

[8] C. Fu, B.-b. Lin, Y.-s. Miao, X. Liu, and J.-j. Chen. A novel chaos-based bit-level permutation scheme for digital image encryption. *Optics communications*, 284(23):5415–5423, November 2011.

[9] J. Guckenheimer and P. Holmes. *Nonlinear oscillations, dynamical systems, and bifurcations of vector fields*, volume 42. Springer Science & Business Media, 2013.

[10] G. Jakimoski and L. Kocarev. Chaos and cryptography: block encryption ciphers based on chaotic maps. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 48(2):163–169, February 2001.

[11] L. Kocarev. Chaos-based cryptography: a brief overview. *IEEE Circuits and Systems Magazine*, 1(3):6–21, 3rd Quarter 2001.

[12] C. Li, Y. Liu, L. Y. Zhang, and M. Z. Chen. Breaking a chaotic image encryption algorithm based on modulo addition and xor operation. *International Journal of Bifurcation and Chaos*, 23(4), April 2013.

[13] H. Liu and X. Wang. Triple-image encryption scheme based on one-time key stream generated by chaos and plain images. *Journal of Systems and Software*, 86(3):826–834, March 2013.

[14] Y. Liu, X. Tong, and J. Ma. Image encryption algorithm based on hyper-chaotic system and dynamic s-box. *Multimedia Tools and Applications*, 75(13):7739–7759, July 2016.

[15] Y. Luo, L. Cao, S. Qiu, H. Lin, J. Harkin, and J. Liu. A chaotic map-control-based and the plain image-related cryptosystem. *Nonlinear Dynamics*, 83(4):2293–2310, March 2016.

[16] B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh, and M. R. Mosavi. A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. *Multimedia tools and applications*, 71(3):1469–1497, August 2014.

[17] V. Patidar, N. Pareek, G. Purohit, and K. Sud. Modified substitution–diffusion image cipher using chaotic standard and logistic maps. *Communications in Nonlinear Science and Numerical Simulation*, 15(10):2755–2765, October 2010.

[18] B. Schneier. *Applied cryptography: protocols, algorithms, and source code in C*. john wiley & sons, 2007.

[19] X. Wang and L. Liu. Cryptanalysis of a parallel sub-image encryption method with high-dimensional chaos. *Nonlinear Dynamics*, 73(1-2):795–800, July 2013.

[20] Y. Wang, K.-W. Wong, X. Liao, and G. Chen. A new chaos-based fast image encryption algorithm. *Applied soft computing*, 11(1):514–522, January 2011.

[21] G. Ye and J. Zhou. A block chaotic image encryption scheme based on self-adaptive modelling. *Applied Soft Computing*, 22:351–357, September 2014.

[22] G. Zhang and Q. Liu. A novel image encryption method based on total shuffling scheme. *Optics Communications*, 284(12):2775–2780, June 2011.

[23] L. Y. Zhang, X. Hu, Y. Liu, K.-W. Wong, and J. Gan. A chaotic image encryption scheme owning temp-value feedback. *Communications in Nonlinear Science and Numerical Simulation*, 19(10):3653–3659, October 2014.

[24] Y.-Q. Zhang and X.-Y. Wang. A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. *Information Sciences*, 273:329–351, July 2014.

[25] C. Zhu. A novel image encryption scheme based on improved hyperchaotic sequences. *Optics Communications*, 285(1):29–37, January 2012.

[26] H. Zhu, C. Zhao, and X. Zhang. A novel image encryption–compression scheme using hyper-chaos and chinese remainder theorem. *Signal Processing: Image Communication*, 28(6):670–680, July 2013.

Author Biography

R.Vidhya received the B.E. degree in Computer Science and Engineering from ACCET, Karaikudi in 2013, M.E. degree in Software Engineering from College of Engineering, Guindy in 2015 and also is pursuing her Ph.D. degree from NIT Trichy. Her research interests include Image Security,Cryptography, and Information retrieval.

Dr.M.Brindha was born in Nagercoil, Tamil Nadu, India, in 1983. She received her B.E. degree from Dr. Sivanthi Aditanar College of Engineeing, Tiruchendur, India in the year of 2004; and her M. E. Degree from Government College of Engineering, Tirunelveli, India in the year of 2006. She received her Ph.D. degree from National Institute of Technology, Tiruchirappalli, in 2016. From February 2009 onwards she is working as an Assistant Professor in the Department of Computer Science and Engineering, National Institute of Technology Tiruchirappalli, Tamilnadu, India. Her areas of interest include Multimedia security, Cryptanalytic attacks, Multimedia compression, Chaos Theory, Cellular automata.