Empirical Analysis of Robust Chaotic Maps for Image Encryption

Sonal Ayyappan, C Lakshmi

Abstract*: The rate of transferring data in the form of text, image, video or audio over an open network has drastically increased. As these are carried out in highly sophisticated fields of medicine, military and banking, security becomes important. In-order to enhance security for transmission, encryption algorithms play a vital role. So as to enhance the proficiency of the existing encryption methods and for stronger anti attack abilities, chaotic based cryptography is essential. Chaotic based encryption has advantages of being sensitive to initial conditions and control parameters. Images have features like bulk data capacity and high inter pixel correlation. Transmission of such medical data should be highly confidential, integral and authorized. Hence chaos-based image encryption is an efficient way of fast and high-quality image encryption. It has features like good speed, complexity, highly secure, reasonable computational overhead and power. In this paper a comprehensive analysis and an evaluation regarding the capabilities of different discrete time domain chaotic maps were carried out on a proposed image encryption method. The experimental results show high efficiency for the proposed image encryption technique.

Keywords*: Chaotic maps, Cryptography, Image encryption, Security Analysis, Measurement Metrics.

I. INTRODUCTION

Since the previous two decades, communication through networks has progressed so much. Data in electronic form is stored, transmitted and maintained on open channels for communicating. These channels are prompt to illegal usage of vital information. Nowadays these communications are very common in the field of telemedicine. Here lot of medical records including of patient's personal privacy records may be transmitted through these open channels. When compared to ordinary images, medical images contain huge amount of sensitive contents. These if tampered a bit can bring negative results while examining. Therefore, before any access to these medical images' security issues like confidentiality, integrity and authentication are to be ensured [1]. Encryption is one solution for ensuring these security issues. It is a process of converting an original record to a cipher record using keys in cryptographic algorithms before transmission. This ensures unauthorized access between the sender, receiver and user unauthorized modification and surety of sender and receiver [2]

Revised Manuscript Received on September 1, 2020.
***** Correspondence Author
Sonal Ayyappan*, Department of Computer Science and Engineering, SRMIST, Chennai, India. Email: sonala@srmist.edu.in
C Lakshmi, Department of Software Engineering, SRMIST, Chennai, India. Email: lakshmic@srmist.edu.in

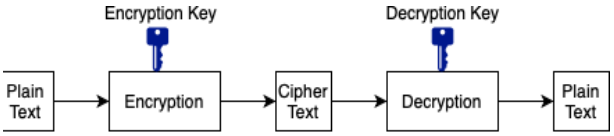

Fig: Encryption Process

Images are represented as 2-dimensional arrays of data. Hence to apply encryption algorithms it must be considered as one-dimensional array of data[3]. One-dimensional image array consumes more space when compared to one dimensional text data which leads to compression. It results in reduced space and reduced time for transmission. But this may cause loss of some data which may be agreeable for general images but may be costly for medical images. This results to wrong diagnosis of these medical images [4]. This paper is organized as follows: Section 2 illustrates the related works, Section 3 introduces the various chaotic maps used and its properties, Section 4 shows the proposed method for implementation, Section 5 explains evaluation metrics, Section 6 explains the experimental results and Section 7 discusses the Conclusion.

II. RELATED WORKS

Commonly used encryption algorithms like AES, DES, RSA [5-13] are not feasible for medical image encryptions. Usually image and text differentiation can be captured by studying correlation pattern of the pixels. Hence encryption techniques based on chaos theory became suitable for this purpose. Technical Research areas of mathematics, physics, engineering etc. [14] have made use of chaotic theory since 1970s. Lorenz [15] was the person to first describe about chaotic theory in his paper written in 1963. He developed the Lorenz attractor which coupled nonlinear differential equations. He also described the complex behavior of chaotic structures in nonlinear deterministic systems. Chaos commonly means a disordered state. Hence chaotic systems are likely to have properties such as 1). High sensitivity to initial conditions and control parameters 2). Unpredictability of its periodic orbits 3). It can be mixed topologically [16]. 4). High encryption rate is made possible due to the simplicity of the hardware and software implementation. The aforementioned properties exhibit important cryptographic principles like confusion, diffusion, balance and avalanche properties [17, 18]. Hence chaos-based encryption can deal the intractable problem of fast and highly secured image encryption due to the mixing and sensitivity properties of chaotic systems thereby improving encryption quality by providing good speed, essential complexity, high security reasonable computational workload and power [19].

The theory of continuous chaotic dynamic systems in cryptography was first applied by Pecora [20]. Later synchronization of chaos was shown by Kocarev [60], Partitz [61], Hayes [21], Chua [22], Murali [62]. Similarly, the theory of discrete chaotic dynamic systems in cryptography was first applied by Mathews [23]. A one-dimensional chaotic map demonstrating the chaotic behavior for a range of control parameters and initial conditions were derived by Mathews. This map generates a pseudorandom number sequence for encryption messages. Later Wheeler [24] corrected Mathews work proving that when these maps were implemented on a digital computer it produced short unpredictable cycles. Habutsu[25] built a piecewise linear chaotic tent map cryptosystem where the key was evolved from the parameter and tent map for encryption and decryption using tent map. His approach works mostly for dynamic chaotic structures where system parameters are highly sensitive to the map properties. But Biham[26] indicated that Habutsu's system could be attacked using a chosen cipher text attack and known plain text attack.Bianco [63] in 1990 implemented a cryptosystem where the logistic map was used to produce a floating-point number sequence, then converted it into binary and X-ORed with the plaintext. Multiple iteration of a chaotic map technique was introduced by Kotalski and Szczepanski[27]. Later Baptista [28] cryptosystem used a secrete key which was a combination of chaotic map's initial condition and parameters. The process was slow and lengthy. Till 1999 chaotic maps were one dimensionally experimented. Kotulski [64] introduced usage of two of chaotic maps. One coordinate represented the evolution of a message and the second represented the change of secrete key at each iteration step. Alvarez [29] used two identical discrete chaotic systems for a symmetric cryptosystem. Wong [30] concentrated in developing a faster chaotic encryption scheme with a dynamic lookup table instead of pseudorandom numbers. Many more enhancements were implemented in the previous decade. The enhancements included new permutation methods [31-33], better diffusion schemes [34, 35] and improved key generation [36-38]. Chaos based encryption approaches were also being applied in medical applications [39, 40]. In this chaos based visual encryption and bit level medical image encryption was developed. Another enhancement was the use of compressive sensing [41, 42] and its matrix used as a secrete key [43]. The authors of [44] proved the computational secrecy of chaotic system mechanism. In [45] 3-dimensional chaotic map implementation was introduced thus increasing the complexity of the cryptosystem. Nowadays researchers are implementing chaotic maps in a combination of the above said methods and have proven better results [46, 47].

III. CHAOTIC MAPS

In Discrete Time Domain Chaotic Cryptosystem, the key for encryption is formed by the combination of control parameters and initial conditions or either using any one. Chaotic maps have their own strengths and weaknesses. Here the usage of a 256 key on different maps for encrypting medical images is being analyzed. An image when encrypted using a chaotic map shows chaotic behavior on the application of certain control parameters. A brief summarization of the maps under consideration is discussed below along with the initial conditions and control parameters applied.

i). Arnold Cat Map[48]: It is chaotic map used for image encryption by shuffling the pixel positions. The resultant image is a permuted one with the original pixels scrambled using the following equation:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} mod\ N \qquad (1)$$

Where N = height and width of the image
x,y = pixel position of original Image
x',y' = pixel position in transformed image
p,q = control parameter
p = q =1

ii). Baker's Map[49]: It is a two-dimensional map mathematically described by:

$$x_{n+1}, y_{n+1} = \begin{cases} 2x_n, \frac{y_n}{2} & 0 \le x_n < \frac{1}{2} \\ 2x_n - 1, \frac{y_n}{2} + \frac{1}{2} & \frac{1}{2} \le x_n \le 1 \end{cases} \qquad (2)$$

iii). Bogdanov Map[50]: It is a chaotic map named after Rifkat Ibragimovich Bogdanov, a Soviet Russian mathematician and relates to Bogdanov-Takens bifurcation.

$$x_{n+1} = x_n + y_{n+1}$$

$$y_{n+1} = y_n + \varepsilon y_n + k x_n(x_n - 1) + \mu x_n y_n \qquad (3)$$

$$\varepsilon = \mu = 0, k = 1.2$$

iv). Chebyshev map[51]: The Chebyshev polynomials are defined by

$$x_{n+1} = \cos\left(k\cos^{-1}(x y_n)\right)$$

$$y_{n+1} = \cos\left(l\cos^{-1}(y_n)\right) \quad l, k \ge 2 \qquad (4)$$

v). Duffing Map[56]: It is discrete real-time dynamic system which shows chaotic behaviour.

$$x_{n+1} = y_n \quad y_{n+1} = -q x_n + p y_n - x_n^3$$

$$p = 2.75, q = 0.3 \qquad (5)$$

vi). Gauss Map[52]: The one dimensional Gauss map is a nonlinear iterated map derived from the Gaussian function.

$$x_{n+1} = \exp(-\alpha x_n^2) + \beta$$

$\alpha = 4.9, \beta =$ -1 to +1 (6)

vii). Gingerbreadman Map[53]: It is a two dimensional discrete- time dynamical system defined by.

$$x_{n+1} = 1 + y_n + |x_n| \qquad y_{n+1} = x_n$$

x=0.5, y=3.7 (7)

viii). Henon Map [53]: It is a two-dimensional discrete time system map defined by

$$x_{n+1} = 1 - a x_n^2 + y_n \qquad y_{n+1} = b x_n$$

a =1.4, b=0.3 (8)

ix). Ikeda Map[54]: It is a two-dimensional discrete time system map defined by

$$x_{n+1} = 1 + u(x_n cost_n - y_n sint_n)$$

$$y_{n+1} = u(x_n sint_n + y_n cost_n)$$

$$t_n = 0.4 - \frac{6}{1+x_n^2+y_n^2} \quad \text{where u} \in [0.5,0.95] \quad (9)$$

x). Kaplan-Yorke Map [59]: It is defined as

$$x_{n+1} = ax_n mod 1 \qquad y_{n+1} = by_n + \cos(4\pi x_n)$$

where a=0<a<=2, 0<b<=1 (10)

xi). Kent Map[55]: It can be equated as

$$x_{n+1} = \begin{cases} x_n/b & 0 \le x \le b \\ \frac{1-x_n}{1-b} & b < x \le 1 \end{cases} \quad (11)$$

xii). Logistic Map [57]: This map results to systems that have delicate dependence on initial conditions defined by

$$x_{n+1} = px_n(1 - x_n) \text{ where p = 3.9999} \quad (12)$$

xiii)Tent Map [59]: This map is given by

$$x_{n+1} = a(1 - x_n) \quad where\ a = 1.888 \quad (13)$$

xiv). Tinkerbell Map[56]: This dynamic system is given by

$$x_{m+1} = x_m^2 - y_m^2 + ax_m + by_m$$
$$y_{m+1} = 2x_m y_m + cx_m + dy_m$$

where a=0.9, b=-0.6013, c=2.0and d=0.5 (14)

xv). Zaslavskii Map[57]: The map is defined by

$$x_{n+1} = x_n + v(1 + \mu y_n) + \varepsilon v\mu[\cos(2\pi x_n)] mod 1$$

$$y_{n+1} = e^{-\tau}[y_n + \varepsilon\cos(2\pi x_n)] \quad \text{where } \mu = \frac{1-e^{-\tau}}{\tau}$$

For this map to be chaotic τ=3.0, v=400/3, ε=0.3 (15)

IV. IMAGE ENCRYPTION

The encryption process has two sections: Key generation and Encryption.

A. Key Generation: For generating the key, one among the 15 chaotic maps is chosen. It is iterated with the initial and control parameters to get 512 values from among which a 256 long key is randomly chosen for encryption. On it, Min_max and gaussian normalization is carried out for standardizing the key.

Input: Chaotic map
Output: Key array of 256 length
Algorithm:

1. Choose chaotic map
2. Iterate the chaotic map to get 512 values -> (x_axis[], y_axis[])
3. Call randomizer with coordinate arrays -> Intermediate key_array
4. Randomly select 256 values from x_axis and y_axis
5. Call min_max on intermediate key_array -> Intermediate key_array
   5.1 Iterate through key_array
   5.1.1 Replace each value with (key_array[i] - min_val) / (max_val - min_val)
6. Call gaussian_normalization on key_array -> intermediate key_array
7. Call key_generation with intermediate key_array ->key_array
   7.1 Convert intermediate key_array into key-value pairs.
   7.2 Sort the key-value pairs by values
   7.3 Extract keys from the sorted pairs.

B . Encryption:
Input: Medical Image, Key array, Blocksize
Output: Encrypted Image
Algorithm:

1. Call encrypt with key_array
2. Resize input image
3. for i = 0 to N do // N = length of the resized input image
   for x = 0 to N do
   for y =0 to (N/blocksize) do
   for i =0 to blocksize do
   current_y = (y * blocksize) + i
   key_value = key_array[i]
   target_y = (y * blocksize) + key_value
   new_pixelintensity = input_image[current_y][x] XOR key_value
   target[target_y][x]=new_pixelintensity
   target_image = circular_shift(target,x,key_array[x%blocksize],,N)
   End for
   End for
   for y =0 to (N/blocksize) do
   for i =0 to blocksize do
   current_y = (y * blocksize) + i
   key_value = key_array[i]
   target_y = (y* blocksize) + key_value
   new_pixelintensity = input_image[x][current_y] XORkey_value
   target[x][target_y]=new_pixelintensity
   target_image= circular_shift(target,x,key_array[x%blocksize],N)
   End for
   End for
   End for
   End for
4. circular_shift(image, x, n, row_column, N)
   if row_column equals 0
   Copy xth row into temp []
   shift_count = (n) / 2
   if x is even
   Right circular shift temp by shift_count
   else:
   Left circular shift by shift_count
   replace row in image with temp
5. Repeat step 1 for columns

Decryption is performed in the reverse order of the encryption algorithm proposed here

V. EVALUATION METRICS

Evaluation metrics are measures used to estimate the effectiveness of our proposed algorithm. Some of them are as follows:

A. ***Differential Analysis***: It is done to find how sensitive is the encryption algorithm to the slightest change that occurs in an input image. It is analyzed using the following:
i). Number of Pixel Change Rate (NPCR)[58] – It measures the amount of pixel change occurred due to a differential attack in percentage. It is defined by:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W*H} * 100 \quad (16)$$

Where

$$D(i,j) = \begin{cases} 0 & if\ I(i,j) = I'(i,j) \\ 1 & if\ I(i,j) \neq I'(i,j) \end{cases}$$

H = Height of the image
W = Width of the image
D(i,j) = Has value 0 if the corresponding pixel in I and I' are same and 1 if they are different.
I(i,j) = Encrypted original image
I'(i,j) = Encrypted attacked image

ii). Unified Average Changing Intensity (UACI) [63] – It measures the average intensity change occurred in an image due to differential attacks. It is defined by:

$$UACI = \frac{\sum_{i,j} I(i,j) - I'(i,j)}{255*W*H} * 100 \quad (17)$$

B. *Statistical Analysis:*

It is carried out to analyze the adjacent pixels in an encrypted image resulting in the extend of robustness of the technique used. It is analyzed using the following:

i). Histogram Analysis[63]:

It shows the pixel distribution in an image with the gray scale levels. The histogram for the original plain image is not uniform but for the encrypted image it should be uniform throughout depicting that all pixels are uniformly distributed in the image space. It is used to make the statistical attacks difficult in an image.

ii). Correlation coefficient[63] - It finds the correlation between the adjacency pixels in an image. It is computed by:

$$R_{x,y} = \frac{C(x,y)}{\sqrt{D(x)}.\sqrt{D(y)}} \quad (18)$$

where

$$C(x,y) = \frac{\sum_{i=1}^{K}(x_i - E(x))(y_i - E(y))}{K} \quad (19)$$

$$D(x) = \frac{1}{K}\sum_{i=1}^{K}(x_i - E(x))^2 \quad (20)$$

$$D(y) = \frac{1}{K}\sum_{i=1}^{K}(y_i - E(y))^2 \quad (21)$$

C(x,y) = Covariance between x and y
x,y = coordinates of the image
K = Number of pixels in the image
D(x), D(y) = Standard Deviation along x, along
E(x), E(y) = Mean of x_i ,y_i

,

C. *Information Entropy*

It gives the mean bit information in an image i.e each pixel has chances of equal probability over uniform distribution [63]. It is equated as:

$$H(s) = -\sum_{s}(P(s_i) * \log_2 P(s_i)) \quad (22)$$

H(s) = Entropy of the original image
$P(s_i)$ = Probability of the occurrence of s_i

D. *Key Analysis*

Keys [63] play a prominent role in the process of making an encryption technique strong. It should be able to block all kinds of threats thus resulting in a bigger sized key with excessive sensitivity. The key should be designed in such a way that even a bit change in the key will not result in the recoverability of the image.

E. *Mean Square Error*

It gives an error measure between the decrypted image and the original image. It is measure as [63]:

$$MSE = \frac{1}{MN\sum_{x=1}^{M}\sum_{y=1}^{N}[O(x,y) - R(x,y)]^2} \quad (23)$$

M, N = Dimensions of the image
O, R = Original and Decrypted Image

F. *Image Contrast*

It accounts the presence of entities in the image[59]

$$IM = \sum_{i,j=0}^{N-1}(i-j)^2 * m_{i,j} \quad (24)$$

G. *Gray level Co-occurrence Matrix (GLCM)*

It gives a comparative frequency measure for a pair of pixels d distance and θ angle apart [64].

H. *Homogeneity [64]*

It shows the element distribution of GLCM and its diagonal

$$HM = \sum_{i,j=0}^{N-1}\frac{m_{i,j}}{1+|i-j|} \quad (25)$$

Table 1- Analysis of Chaotic maps with different measurement metrics with the proposed algorithm

Name of the Map	Correlation Coefficient	UACI	NPCR	Mean Square Error	Original Image Entropy	Encrypted Image Entropy	Input Image Contrast	Encrypted Image Contrast
Arnold	-0.0013	49.9355	99.5956	0.0531	6.7575	7.9970	0.2278	0.2892
Baker	0.0038	50.0495	99.6109	0.0000		7.9970		0.2894
Bogdanov	0.0007	49.8004	99.6292	0.3433		7.9968		0.2911
Chebyshev	-0.0029	50.0430	99.5926	0.5336		7.9974		0.2903
Duffing	-0.0057	49.7990	99.5956	0.0044		7.9970		0.2897
Gauss	0.0003	49.9706	99.6398	0.1436		7.9971		0.2900
Gingerbreadman	-0.0001	50.0951	99.6460	0.8426		7.9970		0.2895
Henon	0.0013	50.0896	99.5941	0.1292		7.9963		0.2896
Ikeda	-0.0048	49.8382	99.5789	0.9690		7.9972		0.2898
Kaplan-Yorke	0.0037	50.1149	99.6155	0.2161		7.9966		0.2891
Kent	-0.0030	49.9390	99.6384	0.2659		7.9970		0.2898
Logistic	0.0011	49.9732	99.6368	0.2461		7.9967		0.2893
Tent	-0.0021	49.9567	99.6353	0.2309		7.9964		0.2900
Tinkerbell	-0.0066	50.0468	99.6597	0.0858		7.9972		0.2891
Zaslaskii	-0.0068	50.1282	99.6399	0.1812		7.9973		0.2888

GLCM Input Image Contrast	GLCM Encrypted Image Contrast	Input Image energy	Encrypted Image energy	Input Image Homogenity	Encrypted Image Homogenity	Input Image Correlation	Encrypted Image Correlation	Name of the Map
383.444	10855.9971	0.0784	0.0048	0.2389	0.0122	0.9432	0.0021	Arnold
	10896.0257		0.0048	0.2389	0.0123		0.0001	Baker
	11026.1568		0.0048	0.2390	0.0121		-0.0008	Bogdanov
	10971.5706		0.0048	0.2390	0.0123		-0.0013	Chebyshev
	10912.4335		0.0048	0.2390	0.0121		0.0002	Duffing
	10932.656		0.0048	0.2390	0.0122		0.0004	Gauss
	10880.2746		0.0048	0.2390	0.0121		0.0016	Gingerbreadman
	10913.4934		0.0048	0.2390	0.0123		-0.0003	Henon
	10961.5077		0.0048	0.2390	0.0122		-0.0033	Ikeda
	10842.3101		0.0048	0.2390	0.0121		0.0020	Kaplan-Yorke
	10922.5702		0.0048	0.2389	0.0122		0.0001	Kent
	10894.764		0.0048	0.2390	0.0122		-0.0008	Logistic
	10881.5647		0.0048	0.2390	0.0121		0.0050	Tent
	10868.1837		0.0048	0.2390	0.0120		-0.0003	Tinkerbell

I. *Peak Signal to Noise Ratio (PSNR)[63]*

It measures the quality of the decrypted image with the original image defined by:

$$PSNR = 10\log_{10}\frac{(2^n-1)^2}{MSE} \quad (26)$$

n = number of bits in a pixel.

VI. RESULTS AND DISCUSSIONS

A comprehensive evaluation using the metrics defined in the Section V was performed on a medical image. The encryption algorithm was implemented with 15 different discrete time system chaotic maps and was evaluated for the metrics. In case of NPCR, the values obtained for every map is in the range of 99.5 to 99.6, and UACI ranges from 49.799 to 50.09. Further, on computing correlation coefficient the algorithm produces values closer to 0, additionally in range from -0.005 to 0.003. However, mean square error is between from 0 to 1, having minimum for encryption using Baker's Map and maximum for Ikeda Map. Image entropy in all cases are close to 8 as this approach is applicable for 8-bit image. GLCM Features like contrast, correlation, energy and homogeneity for the proposed encryption method is constant for different d (distance) and θ (angle). The PSNR here for the given image results in high value exhibiting precise decryption of the encrypted image.

VII. CONCLUSION

In this paper, the proposed encryption algorithm was applied with 15 chaotic maps, experimented on medical images and essential metrics were evaluated. It was observed that the proposed algorithm with the application of chaotic maps with discrete time behavior gives good results when applied on medical images. Thus, the comprehensive experiment and its evaluation shows that the proposed methodology using chaotic maps can be applied for storing attack resistant encrypted medical images. In future we would like to extend our experiments on continuous time behavior chaotic systems.

REFERENCES

1. M. Li, R. Poovendran, and S. Narayanan, "Protecting patient privacy against unauthorized release of medical images in a group communication environment," *Computerized Medical Imaging and Graphics*, vol. 29, no. 5, pp. 367-383, 2005.
2. S. Arora, J. Yttri, and W. Nilsen, "Privacy and security in mobile health (mHealth) research," *Alcohol research: current reviews*, vol. 36, no. 1, p. 143, 2014.
3. W. Stallings, *Cryptography and network security, 4/E*. Pearson Education India, 2006.
4. F. E. Abd El-Samie *et al.*, *Image encryption: a communication perspective*. CRC Press, 2013.
5. M. F. Ukrit and G. Suresh, "Effective lossless compression for medical image sequences using composite algorithm," in *2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT)*, 2013: IEEE, pp. 1122-1126.
6. G. Bhatnagar and Q. J. Wu, "Chaos-based security solution for fingerprint data during communication and transmission," *IEEE Transactions on Instrumentation and Measurement*, vol. 61, no. 4, pp. 876-887, 2012.
7. V. S. Nemade and R. Wagh, "Review of different image encryption techniques," in *National Conference on Emerging Trends in Computer Technology (NCETCT-2012)*, 2012.
8. A. Srivastava, "A survey report on Different Techniques of Image Encryption," *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, no. 6, pp. 163-167, 2012.
9. F. Han, J. Hu, X. Yu, and Y. Wang, "Fingerprint images encryption via multi-scroll chaotic attractors," *Applied Mathematics and Computation*, vol. 185, no. 2, pp. 931-939, 2007.
10. S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons & Fractals*, vol. 35, no. 2, pp. 408-419, 2008.
11. C.-C. Chang, M.-S. Hwang, and T.-S. Chen, "A new encryption algorithm for image cryptosystems," *Journal of Systems and Software*, vol. 58, no. 2, pp. 83-91, 2001.
12. T. Bandyopadhyay, B. Bandyopadhyay, and B. Chatterji, "Secure Image encryption through key hashing and wavelet transform techniques," *International Journal of emerging technology and Advanced engineering*, vol. 2, pp. 26-31, 2012.
13. B. Acharya, S. K. Panigrahy, S. K. Patra, and G. Panda, "Image encryption using advanced hill cipher algorithm," *International Journal of*
14. *Recent Trends in Engineering*, vol. 1, no. 1, pp. 663-667, 2009.
15. H. Kwok and W. K. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," *Chaos, solitons & fractals*, vol. 32, no. 4, pp. 1518-1529, 2007.
16. F. Dachselt and W. Schwarz, "Chaos and cryptography," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 12, pp. 1498-1509, 2001.
17. E. N. Lorenz, "Deterministic nonperiodic flow," *Journal of the atmospheric sciences*, vol. 20, no. 2, pp. 130-141, 1963.
18. M. Ephin, J. A. Joy, and N. Vasanthi, "Survey of Chaos based Image encryption and decryption techniques," in *Amrita International Conference of Women in Computing (AICWIC'13) Proceedings published by International Journal of Computer Applications (IJCA)*, 2013: Cites
19. J. C. Sprott and J. C. Sprott, *Chaos and time-series analysis*. Citeseer, 2003.
20. B. Schneier, "Applied Cryptology," *John Wiley and Sons ISBN 0-471-12845-7*, 1996.
21. L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Physical review letters*, vol. 64, no. 8, p. 821, 1990.
22. S. Hayes, C. Grebogi, and E. Ott, "Communicating with chaos," *Physical review letters*, vol. 70, no. 20, p. 3031, 1993.
23. L. O. Chua, M. Itoh, L. Kocarev, and K. Eckert, "Chaos synchronization in Chua's circuit," *Journal of Circuits, Systems, and Computers*, vol. 3, no. 01, pp. 93-108, 1993.
24. R. Matthews, "On the derivation of a "chaotic" encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29-42, 1989.
25. D. D. Wheeler, "Problems with chaotic cryptosystems," *Cryptologia*, vol. 13, no. 3, pp. 243-250, 1989.
26. T. Habutsu, Y. Nishio, I. Sasase, and S. Mori, "A secret key cryptosystem by iterating a chaotic map," in *Workshop on the Theory and Application of of Cryptographic Techniques*, 1991: Springer, pp. 127-140.
27. E. Biham, "Cryptanalysis of the chaotic-map cryptosystem suggested at EUROCRYPT'91," in *Workshop on the Theory and Application of of Cryptographic Techniques*, 1991: Springer, pp. 532-534.
28. Z. Kotulski and J. Szczepański, "Discrete chaotic cryptography," *Annalen der Physik*, vol. 509, no. 5, pp. 381-394, 1997.
29. M. Baptista, "Cryptography with chaos," *Physics letters A*, vol. 240, no. 1-2, pp. 50-54, 1998.
30. E. Alvarez, A. Fernandez, P. Garcıa, J. Jiménez, and A. Marcano, "New approach to chaotic encryption," *Physics Letters A*, vol. 263, no. 4-6, pp. 373-375, 1999.
31. K.-w. Wong, "A fast chaotic cryptographic scheme with dynamic look-up table," *Physics Letters A*, vol. 298, no. 4, pp. 238-242, 2002.
32. C. Fu, J.-B. Huang, N.-N. Wang, Q.-B. Hou, and W.-M. Lei, "A symmetric chaos-based image cipher with an improved bit-level permutation strategy," *Entropy*, vol. 16, no. 2, pp. 770-788, 2014.
33. X. Zhang and X. Wang, "Chaos-based partial encryption of SPIHT coded color images," *Signal Processing*, vol. 93, no. 9, pp. 2422-2431, 2013.
34. Y. Zhang and D. Xiao, "An image encryption scheme based on rotation matrix bit-level permutation and block diffusion," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 1, pp. 74-82, 2014.
35. X.-j. Tong, "The novel bilateral–Diffusion image encryption algorithm with dynamical compound chaos," *Journal of Systems and Software*, vol. 85, no. 4, pp. 850-858, 2012.
36. X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Optics and Lasers in Engineering*, vol. 66, pp. 10-18, 2015.
37. J.-x. Chen, Z.-l. Zhu, C. Fu, L.-b. Zhang, and Y. Zhang, "An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach," *Communications in Nonlinear Science and Numerical Simulation*, vol. 23, no. 1-3, pp. 294-310, 2015.
38. J.-X. Chen, Z.-L. Zhu, C. Fu, L.-B. Zhang, and Y. Zhang, "Cryptanalysis and improvement of an optical image encryption scheme using a chaotic Baker map and double random phase encoding," *Journal of Optics*, vol. 16, no. 12, p. 125403, 2014.
39. X. Tong and M. Cui, "Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator," *Signal processing*, vol. 89, no. 4, pp. 480-491, 2009.

40. 39 . C.-F. Lin, C.-H. Chung, and J.-H. Lin, "A chaos-based visual encryption mechanism for clinical EEG signals," *Medical & Biological Engineering & Computing*, vol. 47, no. 7, pp. 757-762, 2009.
41. C. Fu *et al.*, "An efficient and secure medical image protection scheme based on chaotic maps," *Computers in biology and medicine*, vol. 43, no. 8, pp. 1000-1010, 2013.
42. E. J. Candès, J. Romberg, and T. Tao, "Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information," *IEEE Transactions on information theory*, vol. 52, no. 2, pp. 489-509, 2006.
43. D. L. Donoho, "Compressed sensing," *IEEE Transactions on*
44. *information theory*, vol. 52, no. 4, pp. 1289-1306, 2006.
45. E. J. Candes and T. Tao, "Near-optimal signal recovery from random projections: Universal encoding strategies?," *IEEE transactions on information theory*, vol. 52, no. 12, pp. 5406-5425, 2006.
46. Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *2008 46th Annual Allerton conference on communication, control, and computing*, 2008: IEEE, pp. 813-817.
47. 46. G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749-761, 2004.
48. 47 . L. Y. Zhang, K.-W. Wong, Y. Zhang, and Q. Lin, "Joint quantization and diffusion for compressed sensing measurements of natural images," in *2015 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2015: IEEE, pp. 2744-2747.
49. 48. R. K. Sinha, N. San, B. Asha, S. Prasad, and S. Sahu, "Chaotic Image Encryption Scheme Based on Modified Arnold Cat Map and Henon Map," in *2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)*, 2018: IEEE, pp. 1-5.
50. 49 . F. Han, X. Yu, and S. Han, "Improved baker map for image encryption," in *2006 1st International Symposium on Systems and Control in Aerospace and Astronautics*, 2006: IEEE, pp. 4 pp.-1276.
51. 50. V. Subashini and S. Poornachandra, "Chaos Based Image Encryption Using Bogdanov Map," *Journal of Computational and Theoretical Nanoscience*, vol. 14, no. 9, pp. 4508-4514, 2017.
52. 51. B. Stoyanov and K. Kordov, "Novel image encryption scheme based on Chebyshev polynomial and Duffing map," *The Scientific World Journal*, vol. 2014, 2014.
53. 52. A. Sahay and C. Pradhan, "Multidimensional comparative analysis of image encryption using gauss iterated and logistic maps," in *2017 International Conference on Communication and Signal Processing (ICCSP)*, 2017: IEEE, pp. 1347-1351.
54. 53 . S. M. Rani and K. Sudha, "Design and Implementation of Image Encryption Algorithm Using Chaos," *International Journal of Advanced Computer Research*, vol. 4, no. 2, p. 660, 2014.
55. 54. N. Singh and A. Sinha, "Digital image watermarking using gyrator transform and chaotic maps," *Optik*, vol. 121, no. 15, pp. 1427-1437, 2010.
56. 55. X. Wang and Q. Wang, "A novel image encryption algorithm based on dynamic S-boxes constructed by chaos," *Nonlinear Dynamics*, vol. 75, no. 3, pp. 567-576, 2014.
57. 56. B. Stoyanov, "Pseudo-random bit generation algorithm based on Chebyshev polynomial and Tinkerbell map," *Applied Mathematical Sciences*, vol. 8, no. 125, pp. 6205-6210, 2014.
58. 57. R. Hamza and F. Titouna, "A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map," *Information Security Journal: A Global Perspective*, vol. 25, no. 4-6, pp. 162-179, 2016.
59. 58. M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques," *Archives of Computational Methods in Engineering*, pp. 1-29, 2018.
60. 59. A. Omotosho and J. Emuoyibofarhe, "Private key management scheme using image features," *Journal of Applied Security Research*, vol. 10, no. 4, pp. 543-557, 2015.
61. 60 . L. Kocarev, K.S. Halle, K. Eckert, L.O. Chua and U. Par- tilz, Int. J. Bifur. Chaos 2 (1992) 709.
62. 61. U. Parlitz, L.O. Chua, L. Kocarev, K.S. Halle, A. Shang, Int. J. Bifur. Chaos 2 (3) (1992) 973.
63. 62. K. Murali, M. Lakshmanan, L.O. Chua, Int. J. Bifur. Chaos 5 (1995) 563.
64. 63. M.E. Bianco, G.L. Mayhew, US patent No. 5,365,588 (1994).
65. 64. Z. Kotulski, J. Szczepanski, K. Górski, A. Paszkiewicz, A. Zugaj, Int. J. Bifur. Chaos 9 (6) (1999) 1121.

AUTHOR PROFILE

Sonal Ayyappan is a PhD Scholar in the Department of Computer Science and Engineering, SRMIST, Chennai, India. Her area of interest includes image processing and security.

Dr. C Lakshmi is Professor and Head of the Department, Department of Software Engineering, SRMIST, Chennai, India. She has 25 years of teaching experience and has published many papers in reputed national and international journals. Her area of interest include Machine Learning, Artificial Intelligence, Image Processing, Pattern Recognition, Genetic Algorithms and Software Engineering.