18SN614 Cryptography and Applications

PROJECT REPORT

Image Encryption Based On Chaotic Maps

By Megha Ajit

[AM.EN.P2CSN19006]

M.Tech Cybersecurity Systems and Networks
Amrita School of Engineering,
Amritapuri campus, Kollam.

Table of Contents

I. Introduction

II. Chaotic Maps

III. Contribution to the Project

IV. Methodology

V. Result

VII. Attacks Used

VII. Conclusion

VIII. Reference

I. INTRODUCTION

Nowadays, the security of private information that is transmitted through the internet has become a major concern. Especially, the digital images that are transmitted through the internet are not secured. Nowadays, medical images and healthcare records are transmitted to the hospitals through internet and it is important to secure these data from attackers. These transmitted images can be accessed or captured by unauthorized users or attackers. So, it is important to maintain privacy and provide security to the transmitted images. In order to provide confidentiality to these images, encryption is needed. But traditional encryption methods like AES and DES are not suitable for image encryption because of some of the properties of images like high redundancy, data size, and strong correlation. Here, a chaotic encryption method is introduced to prevent image information leakage.

II. Chaotic Maps

Chaos is a cryptographic concept which produce random number sequences. These sequences are used for encryption. Chaotic Encryption is found to be more effective since they have many properties like pseudo randomness, periodicity, and also high sensitivity to initial values of the keyspace. These chaotic maps are highly sensitive to the control parameters and initial values. These properties make image encryption stronger.

In the paper " A Novel bit-level image encryption algorithm based on a chaotic map", we used bit-level image encryption based on Piecewise Linear Chaotic Maps (PWLCM). Here, these PWLCM chaotic map generates random secret keys and these random keys are used to encrypt the image for different rounds.

In the paper "A new 1D chaotic system for image encryption", we combined two 1D chaotic maps : logistic map and tent map to generate random secret keys for encryption.

III. CONTRIBUTION:

My contribution towards this project is security analysis for the proposed system. The security analysis that I have done in these projects are as follows:

1. Key Sensitivity Analysis:

A cryptographic system should be sensitive to the secret keys. A small change in the secret key can produce a large change in the cipher image. In this project, I have analyzed the key sensitivity analysis in both encryption and decryption phase. In this proposed algorithm, the keyspace includes initial values x0 and y0. I have made a slight modification in these keyspaces and then compared the encrypted image with the original key and the encrypted image with the modified keyspace. This is done by comparing both the images pixel by pixel and if any of the pixel matches then it will be given as the count and then calculated the percentage match of both cipher images. The results show that both the cipher images are completely different. This means that a slight change in the key can make a large modification in the cipher images.

For the decryption phase, I have made a slight change in the decryption key and try to decrypt the same cipher image, but the correct image can't be obtained because only the correct decryption key can decrypt the plain image. Also, the decrypted image with the original key and decrypted image with the modified key is completely different.

Calculation:

Percentage Match = [Count/(m*n)]100

where,

count is the number of pixel that are equal for both the encrypted images.

m*n = size of image.

2. Differential Attack:

Differential Attack is an attack in which the attacker makes use of the plain text and the corresponding cipher to get the secret key.

To avoid this attack, a good cryptographic system should ensure a small change in the image should produce a significant change in the encrypted and decrypted image. For that, I have selected a pixel randomly and change the pixel value of the plain image and then calculated the Number of pixel change rate (NPCR) and Unified Average Changing Intensity (UACI).

Calculation:

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%$$

where

$$D(i,j) = \begin{cases} 0 & C_1(i,j) = C_2(i,j) \\ 1 & C_1(i,j) \neq C_2(i,j) \end{cases}$$

$$\mathrm{UACI} = \left[\sum_{i,j} \frac{| \; C_1(i,j) - C_2(i,j) |}{M \times N \times 255} \right] \times 100\%$$

where C 1 and C 2 are two images that have the same size M x N.

IV. METHODOLOGY

In the first paper, a chaos-based encryption scheme based on cyclic shift, swapping, and piecewise linear chaotic maps are proposed. Here, first, the plain image is converted to bit plane sequences and the bit plane is divided into two row vectors A1 and A2. Then it is given to the diffusion phase. Diffusion phase ensures that a slight change in the plain image should cause a large change in the cipher image. In this phase, by cyclic shifting and xor operations B1 and B2 are produced. And in confusion phase, swapped the binary elements between the two sequences B1 and B2 with the control of piecewise linear chaotic maps and thus C1 and C2 are produced. Then, converted the C1 and C2 into bitplanes and finally to the cipher images. The decryption process is just reverse of the encryption. And security analysis like key sensitivity analysis, histogram analysis, differential analysis, entropy analysis, and correlation analysis are done. These proved that the proposed image encryption algorithm is secure.

In the second paper, we used logistic map and tent map to generate random secret keys for encryption. Here, random values are inserted to the starting of each row of the image and then the next step is row separation. The rows are separated as arrays and the data values in each row is changed in the substitution process. After that the rows are combined and the image is rotated 90 degrees in counte clockwise direction. Thus the first round is done and will repeat for four rounds and finally we get the encrypted image. In decryption process, the same steps are done in inverse order.

V. RESULTS:

We have tested security analysis for both the papers. Here, various images with different sizes are used for the analysis. Security analysis like key sensitivity, differential attack, histogram analysis, contrast analysis, and information entropy analysis is done.

*VI.*Attacks Used:

(i) Key Sensitivity Analysis:

In this analysis, we have made a slight change in the secret key and compared the encrypted images with the original key and the modified key. And it is found that a slight change in the key has made a large difference in the cipher images. Percentage matched by the two cipher images are very less.

(ii) Differential Attack:

In this analysis, we have made a change in the pixel value of the plain image randomly and calculated the number of pixel change rate. A small change in the plain image produces a large change in the encrypted and decrypted images. And it is found that both the papers show a large pixel change rate which means that a small change in the image can produce a large change in the cipher images.

(iii) Histogram Analysis:

Histogram is a graphical representation of pixel intensity distribution of the image. The uniform histogram representation ensures that the proposed encryption system is secure and can resist any statistical attacks.

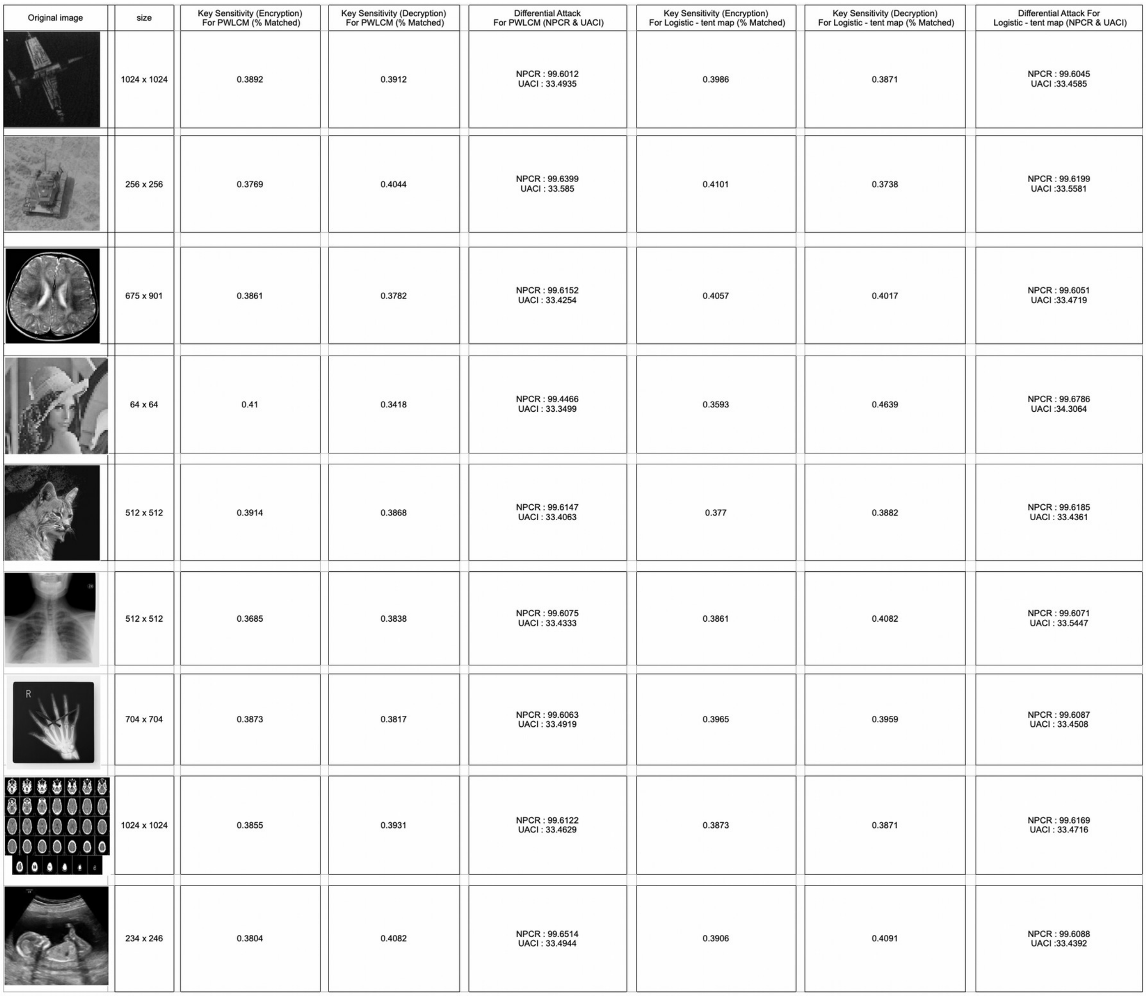
(iv) Entropy Analysis:

Entropy is the lack of predictability i.e, here it is the measure of randomness. We are calculating the entropy for plain image and corresponding cipher images. Maximum entropy of the image should be 8 or closer to 8. If the entorpy is in 7 to 8 range then it is not possible for the attackers to decrypt the cipher images.

(v) Contrast Analysis:

Contrast is used to measure the pixel local variation and pixel distibution of the image. The constrast value of the cipher image is expected to be ~10.

Key Sensitivity and Differential Attack Analysis:



Original image	size	Key Sensitivity (Encryption) For PWLCM (% Matched)	Key Sensitivity (Decryption) For PWLCM (% Matched)	Differential Attack For PWLCM (NPCR & UACI)	Key Sensitivity (Encryption) For Logistic - tent map (% Matched)	Key Sensitivity (Decryption) For Logistic - tent map (% Matched)	Differential Attack For Logistic - tent map (NPCR & UACI)
	1024 x 1024	0.3892	0.3912	NPCR : 99.6012 UACI : 33.4935	0.3986	0.3871	NPCR : 99.6045 UACI :33.4585
	256 x 256	0.3769	0.4044	NPCR : 99.6399 UACI : 33.585	0.4101	0.3738	NPCR : 99.6199 UACI :33.5581
	675 x 901	0.3861	0.3782	NPCR : 99.6152 UACI : 33.4254	0.4057	0.4017	NPCR : 99.6051 UACI :33.4719
	64 x 64	0.41	0.3418	NPCR : 99.4466 UACI : 33.3499	0.3593	0.4639	NPCR : 99.6786 UACI :34.3064
	512 x 512	0.3914	0.3868	NPCR : 99.6147 UACI : 33.4063	0.377	0.3882	NPCR : 99.6185 UACI : 33.4361
	512 x 512	0.3685	0.3838	NPCR : 99.6075 UACI : 33.4333	0.3861	0.4082	NPCR : 99.6071 UACI : 33.5447
R	704 x 704	0.3873	0.3817	NPCR : 99.6063 UACI : 33.4919	0.3965	0.3959	NPCR : 99.6087 UACI : 33.4508
	1024 x 1024	0.3855	0.3931	NPCR : 99.6122 UACI : 33.4629	0.3873	0.3871	NPCR : 99.6169 UACI : 33.4716
	234 x 246	0.3804	0.4082	NPCR : 99.6514 UACI : 33.4944	0.3906	0.4091	NPCR : 99.6088 UACI :33.4392

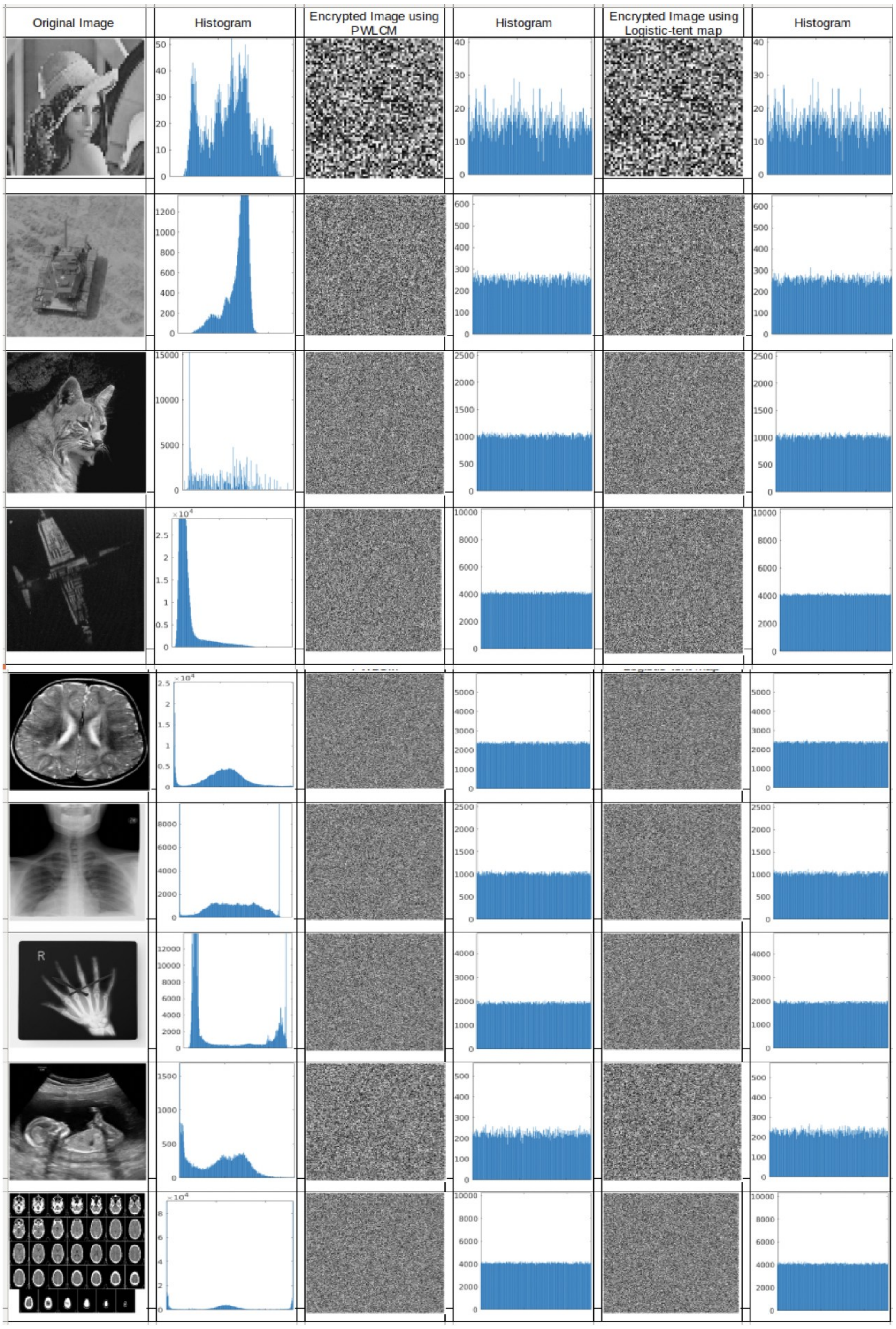
Above table shows key sensitivity and differential attack analysis for both the proposed system.

In key sensitivity analysis, the percentage match obtained for both PWLCM and logistic tent map are almost in 0.3 – 0.4 range, i.e, it proves that a small change in the intial key can make a large difference in the cipher images. This is because here we are using chaotic map for encryption.

In differential attack, NPCR is showing 98 - 99 range i.e, a change in the pixel of the image made large pixel change rates for both PWLCM chaotic map and logistic – tent map.

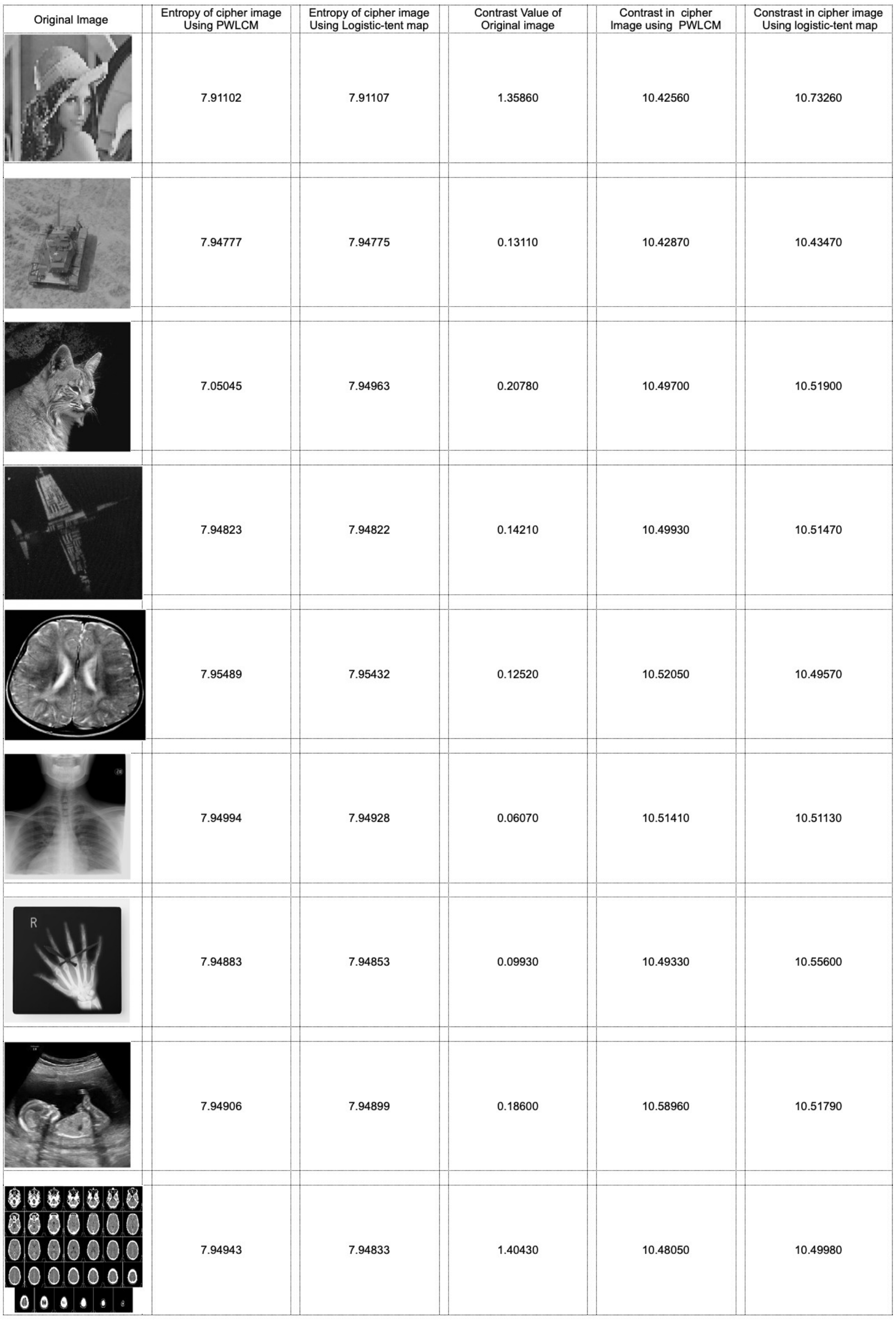
These security analysis proves that the proposed encryption method is secure.

Histogram Analysis:



In above shown fig, the histogram analysis for plain image and encrypted image (for both PWLCM and logistic tent map) are shown. From the fig it is clear that ,for the plain image histogram analysis is not uniform and for most of the encrypted images have uniform histogram representation. This shows that the encryption system is secure and this resist statistical attacks.

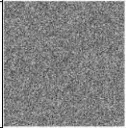
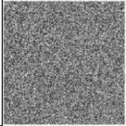
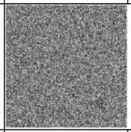
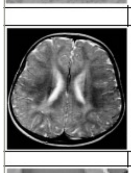
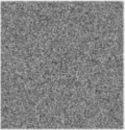
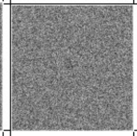
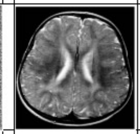
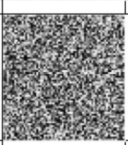
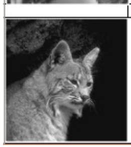
Contrast Analysis:

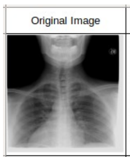
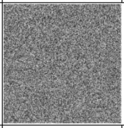
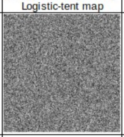
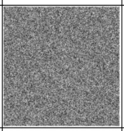
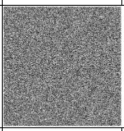
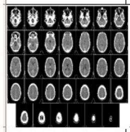
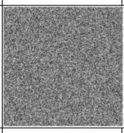
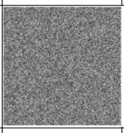
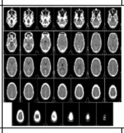
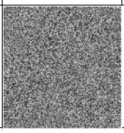
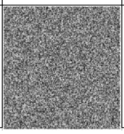
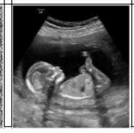


Original Image	Entropy of cipher image Using PWLCM	Entropy of cipher image Using Logistic-tent map	Contrast Value of Original image	Contrast in cipher Image using PWLCM	Constrast in cipher image Using logistic-tent map
	7.91102	7.91107	1.35860	10.42560	10.73260
	7.94777	7.94775	0.13110	10.42870	10.43470
	7.05045	7.94963	0.20780	10.49700	10.51900
	7.94823	7.94822	0.14210	10.49930	10.51470
	7.95489	7.95432	0.12520	10.52050	10.49570
	7.94994	7.94928	0.06070	10.51410	10.51130
	7.94883	7.94853	0.09930	10.49330	10.55600
	7.94906	7.94899	0.18600	10.58960	10.51790
	7.94943	7.94833	1.40430	10.48050	10.49980

The above figure shows the entropy and contrast analysis. Entropy of cipher images for both the PWLCM and logistic-tent map is in the range of 7.9 ~ 8. This ensures that it is difficult for the attackers to decrypt the cipher images as the entropy measure approxemately to 8. Therefore, the probability of transmitted information leakage is also very small.

End to End time:

Original image	Encrypted Image Using PWLCM	Encrypted Image Using Logistic-tent map	Decrypted Image	Total Time taken Using PWLCM (sec)	Total Time taken Using Logistic-tent map (sec)	size
				54.181	74.87	1024 x 1024
				3.877	3.638	256 x 256
				40.255	23.411	675 x 901
				0.67	0.667	64 x 64
				30.758	23.538	512 x 512

Original Image	Encrypted Image using PWLCM	Encrypted Image using Logistic-tent map	Decrypted Image	Time Taken for PWLCM (sec)	Time Taken for Logistic-tent map (sec)	Size
				22.884	9.868	512 x 512
				63.272	23.023	704 x 704
				118.268	57.591	1024 x 1024
				5.24	2.606	234 x 246

The above result shows encryption and decryption of various images (with different sizes) using PWLCM and logistic-tent map and also given the total time taken for both PWLCM and logistic tent map.

VII. CONCLUSION

WE have proposed image encryption system based on PWLCM (piecewise linear chaotic map) and combination of two 1D chaotic maps : logistic map and tent map. Both the chaotic encryption system yields good security i.e, both the chaos system provide complete randomness to the secret key and this resists differential and statistical attacks. And the security analysis proves that both the proposed chaotic system are secure.

VIII. REFERENCE

[1] Xu, Lu, et al. "A novel bit-level image encryption algorithm based on chaotic maps." *Optics and Lasers in Engineering* 78 (2016): 17-25.

[2] Zhou, Yicong, Long Bao, and CL Philip Chen. "A new 1D chaotic system for image encryption." *Signal processing* 97 (2014): 172-182.

[3] Hua, Zhongyun, et al. "2D Logistic-Sine-coupling map for image encryption." *Signal Processing* 149 (2018): 148-161.