SJIF Impact Factor 2022: 8.197| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)

EPRA International Journal of Research and Development (IJRD)

Volume: 7 | Issue: 3 | March 2022 - Peer Reviewed Journal

SELECTIVE CHAOTIC GENERATION AND MULTI-MODALITY DIGITAL IMAGE CRYPTO SYSTEM USING HAAR WAVELETS

K.Nithhyaadevi[1], J.S.Jenin[2], G.Gandhimathi[3]

[1]PG Student, [2]Assistant Professor, [3]Professor and HoD

Department of Electronics and Communication Engineering

Trichy Engineering College, Trichy, Tamil Nadu, India

Article DOI: https://doi.org/10.36713/epra9653
DOI No: 10.36713/epra9653

ABSTRACT

The importance of secured image transmission plays a significant role in this information era. The hackers hack the medical data in the form of images that costs more in terms of claiming insurances. It is necessary to secure the images that cannot be accessed by the unauthorized persons. Among the many types of image crypto systems, the chaos based image crypto systems is best known for its key insensitive to attack or hacking. The properties of the chaos play a major role in the generation of key for the secured transmission and reception. The Haar wavelet transform is yet simpler transform used to compress the input image in terms of approximate and detailed coefficients. The incorporation of the key in the approximate coefficients of the input image provides an efficient encryption when compared to other image crypto schemes. The encryption quality is evaluated using the histogram analysis of the encrypted of cipher image with different keys generated using respective chaotic maps. The framed image crypto system is designed and simulated using MATLAB software package.

KEYWORDS: *image cryptosystems, chaos theory, Haar wavelet transform, encryption, key generation.*

1. INTRODUCTION

Many applications (military communications, medical imaging, etc.,) need to secure their materials in case data exchange over a channel or in storage media. The cryptosystem is the optimal solution for protection and security of digital multimedia. Image encryption has gained a remarkable attention in research because of its several vital applications such as cable TV, confidential chatting, etc. One of the successful techniques for image encryption is the chaotic maps. Chaotic maps attracted the attention of researchers in the field of image encryption because it has a random performance as well as the high sensitivity to the encryption key. These advantages guarantee to achieve Shannon's requirements of diffusion and confusion [1].

In [2], authors introduced the cascade chaotic system (CCS), a general chaotic framework with a simple and effective structure. Chaotic performance of CCS is studied theoretically and experimentally. Random properties of the proposed PRNG are evaluated using two test standards. *T.Zhang et al* proposed a simple and new approach to design S-Box based on an ancient Chinese I-Ching philosophy. IChing is a collection of statements about divination with 64 hexagrams in ancient China. The authors aimed to evaluate the efficiency of this novel method with some acceptable criteria are used to evaluate the designed S-Box [3].

G.Ye proposed an effective and efficient way for protecting the personal images including: (1) large key space; (2) more wave sources to construct the complex of system; (3) key stream is generated dependent on the plain image; (4) use chaotic sequence to find the source point of wave. Chaotic image encryption algorithm can be found for many applications such as military, meteorology, and medical science. Patent is a practical application form of image encryption algorithms [4]. In [5], authors investigated the security of a classic diffusion mechanism (and of its variants) used as the core cryptographic primitive in some image cryptosystems based on the complex dynamic phenomena. Authors theoretically found that regardless of the key schedule process, the data complexity for recovering each element of the equivalent secret key from these diffusion mechanisms is only O(1). The proposed analysis is validated by means of numerical examples [6-8].

In order to overcome the above shortcomings from image encryption based on chaotic maps and DNA cryptography, in this work, authors used the simple theory of the DNA sequence operation to encrypt image information and the combined chaotic maps and DNA sequence addition operation to implement image encryption. Extensive numerical experiment results have revealed that proposed image encryption algorithm offers advantages of unlimited key space and high-level security, since those problematic periodic windows are no longer present within the key space, and it is extremely robust against known-plain-text attack, since the chaotic sequence generated bears no correlation whatsoever due to the folding effect of modulo operation. The algorithm is believed to make truly efficient yet highly secure image encryption a reality [9, 10].

2. PROPOSED IMAGE CRYPTOSYSTEM

This work involves devising an algorithm for encryption of image for transmitting the image. The encryption is done using key. The key is generated using chaotic maps, out of the available chaotic maps, the maps with best chaos are chosen for designing of random sequence. The chaotic sequence is converted into integer format and normalized to be used as a key. The encryption algorithm involves transforming the image into coefficients using 2D orthogonal Haar wavelet transform. The obtained coefficients are approximation coefficients (LL), and detailed coefficients (HL, LH and HH). The approximation coefficients are XORed with the key to produce the diffused coefficients. The diffused approximation coefficients along with the detailed coefficients are subjected to inverse Haar transform to get the sub-cipher image. The sub-cipher image is again XORed with key to get the cipher image. The system is shown in Figure.1.

2.1. CHAOS BASED CRYPTOGRAPHY

The chaos based cryptographic algorithms have several advantages over the traditional pixel based encryption algorithms including high security, speed, reasonable computational overheads and computational power. A chaotic map is a map (namely, an evolution function) that exhibits some sort of chaotic behavior. Chaotic systems are a simple sub-type of nonlinear dynamical systems. They may contain very few interacting parts and these may follow very simple rules, but these systems all have a very sensitive dependence on their initial conditions. Despite their deterministic simplicity, over time these systems can produce totally unpredictable and wildly divergent (aka, chaotic) behavior. The maps used here are Chebyshev map, circle map, Gauss/mouse map, logistic map, piecewise map, and Tent map. The proposed key generation mechanism is shown in Figure.2.

2.2. THE IMAGE ENCRYPTION SYSTEM

The encryption is performed using Haar wavelets. The algorithm requires no additional memory for the inverse wavelet. The detailed encryption process is shown in Figure. 3. Security analysis can be referred as the art of finding the weakness of a cryptosystem and retrieval of either the whole or a part of a ciphered image or finding the secret key without knowing the decryption key of the algorithm. Some of the most common types of attacks to encrypted images are analyzed using different analysis such as histogram Analysis, Entropy Analysis, Key Sensitivity Analysis (NPCR-Number of Pixel Change Rate): An important measure for investigating the performance of an image encryption algorithm with the goal of testing well the resistance works if a differential attack takes place. NPCR shows and computes the change rate of pixels, UACI-Unified Average Changing Intensity), Key Space Analysis and Correlation Analysis.

3. RESULTS AND DISCUSSIONS

The simulated results for the different input images and the encrypted images are tabulated as follows. The histogram analysis is taken to show the uniformity and randomness in the encrypted image using the different keys generated using the respective chaotic maps. The sample results with different chaotic key for Lena image is depicted in Figure.4.

3.1. PERFORMANCE METRICS

The performance metrics such as histogram variance, entropy values, NPCR and UACI values are summarized in Table-1 for Lena and bird images. In our approach, a high variance value of 2573 is obtained for the case of lena image with Gauss chaotic map and minimum variance of 2199 is obtained for the case of Barbara image with Gauss chaotic map key. It is necessary to reduce the value of variance comparatively to the bench mark results. In our approach the information entropy value of 7 is obtained. As per the benchmark results the obtained entropy is slightly lesser, hence it is to be improved by combining different chaotic maps or using a new kind of chaotic map. In our approach we obtained a NPCR value as high as 98 for the case of cameraman image with circle chaotic map key. It is slightly lesser than the benchmark results; hence it is necessary to improve the cryptosystem mechanism. In our approach we obtained a maximum UACI value of 34.3235 for the case of Mandrill image with circle chaotic map key and minimum UACI value of 29.7535 for the case of cameraman image with circle chaotic map key. Hence, it is necessary to design the key generation unit to obtain a consistent UACI value for the all the images.

4. CONCLUSION

An effective cryptosystem plays a major role in any secured applications. Specifically, the design of key is the important part in the cryptosystems. In this paper, the key generation utilizing different chaos maps and encryption process is carried out for grayscale images. Preliminary results are obtained with the developed cryptosystem. All the performance metrics obtained in the presented cryptosystem are slightly lesser than the benchmark results. Hence, it is necessary to modify the key generation mechanism either using hybrid chaotic maps or a new kind of chaotic map.

REFERENCES

1. *Patidar, V., Pareek, N. K., & Sud, K. K. (2009). A new substitution–diffusion based image cipher using chaotic standard and logistic maps. Communications in Nonlinear Science and Numerical Simulation, 14(7), 3056-3075.*
2. *Zhou, Y., Hua, Z., Pun, C. M., & Chen, C. P. (2014). Cascade chaotic system with applications. IEEE transactions on cybernetics, 45(9), 2001-2012.*
3. *Zhang, T., Chen, C. P., Chen, L., Xu, X., & Hu, B. (2018). Design of highly nonlinear substitution boxes based on I-Ching operators. IEEE transactions on cybernetics, 48(12), 3349-3358.*
4. *Ye, G. (2014). A block image encryption algorithm based on wave transmission and chaotic systems. Nonlinear Dynamics, 75(3), 417-427.*
5. *Zhang, L. Y., Liu, Y., Pareschi, F., Zhang, Y., Wong, K. W., Rovatti, R., & Setti, G. (2017). On the security of a class of diffusion mechanisms for image encryption. IEEE transactions on cybernetics, 48(4), 1163-1175.*
6. *Wang, X., & Xu, D. (2014). A novel image encryption scheme based on Brownian motion and PWLCM chaotic system. Nonlinear dynamics, 75(1), 345-353.*
7. *Zhu, C., Xu, S., Hu, Y., & Sun, K. (2015). Breaking a novel image encryption scheme based on Brownian motion and PWLCM chaotic system. Nonlinear Dynamics, 79(2), 1511-1518.*
8. *Hermassi, H., Belazi, A., Rhouma, R., & Belghith, S. M. (2014). Security analysis of an image encryption algorithm based on a DNA addition combining with chaotic maps. Multimedia tools and applications, 72(3), 2211-2224.*
9. *Zhang, Q., Guo, L., & Wei, X. (2010). Image encryption using DNA addition combining with chaotic maps. Mathematical and Computer Modelling, 52(11-12), 2028-2035.*
10. *Lin, R. M., & Ng, T. Y. (2018). Secure image encryption based on an ideal new nonlinear discrete dynamical system. Mathematical Problems in Engineering, 2018.*

FIGURES AND TABLES

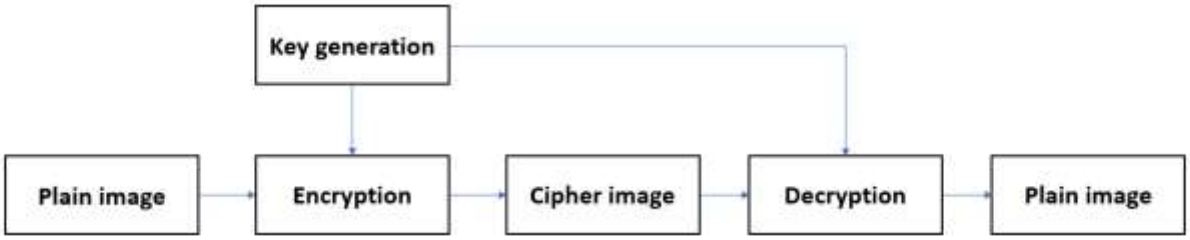


Fig. 1. Typical image crypto system

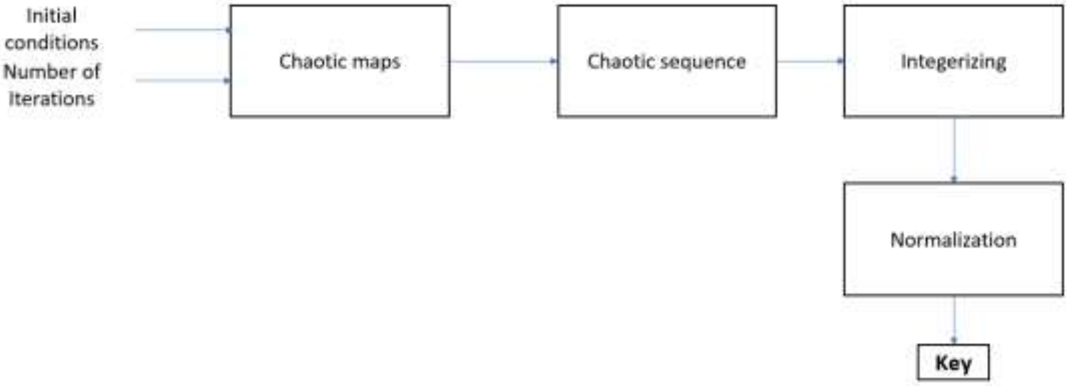


Fig. 2. Key generation mechanism

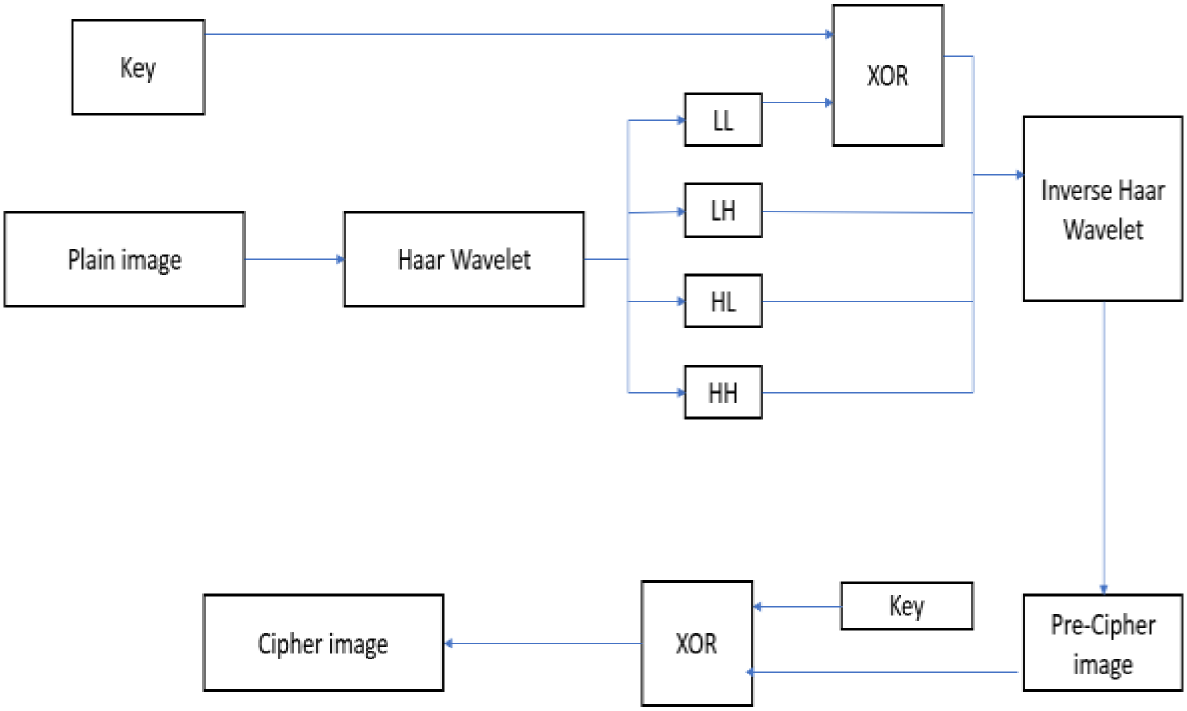
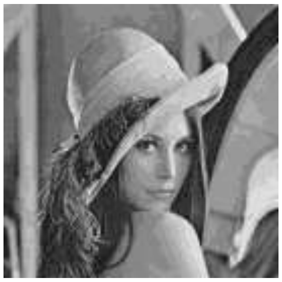
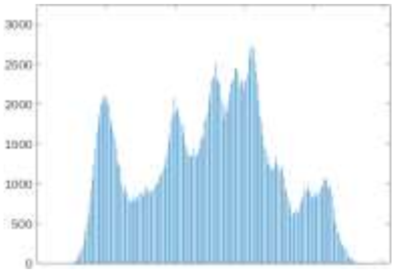


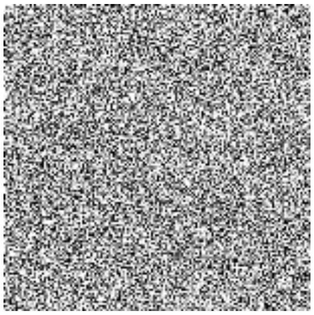
Fig. 3. Proposed encryption algorithm



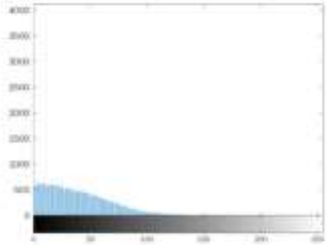
(a)



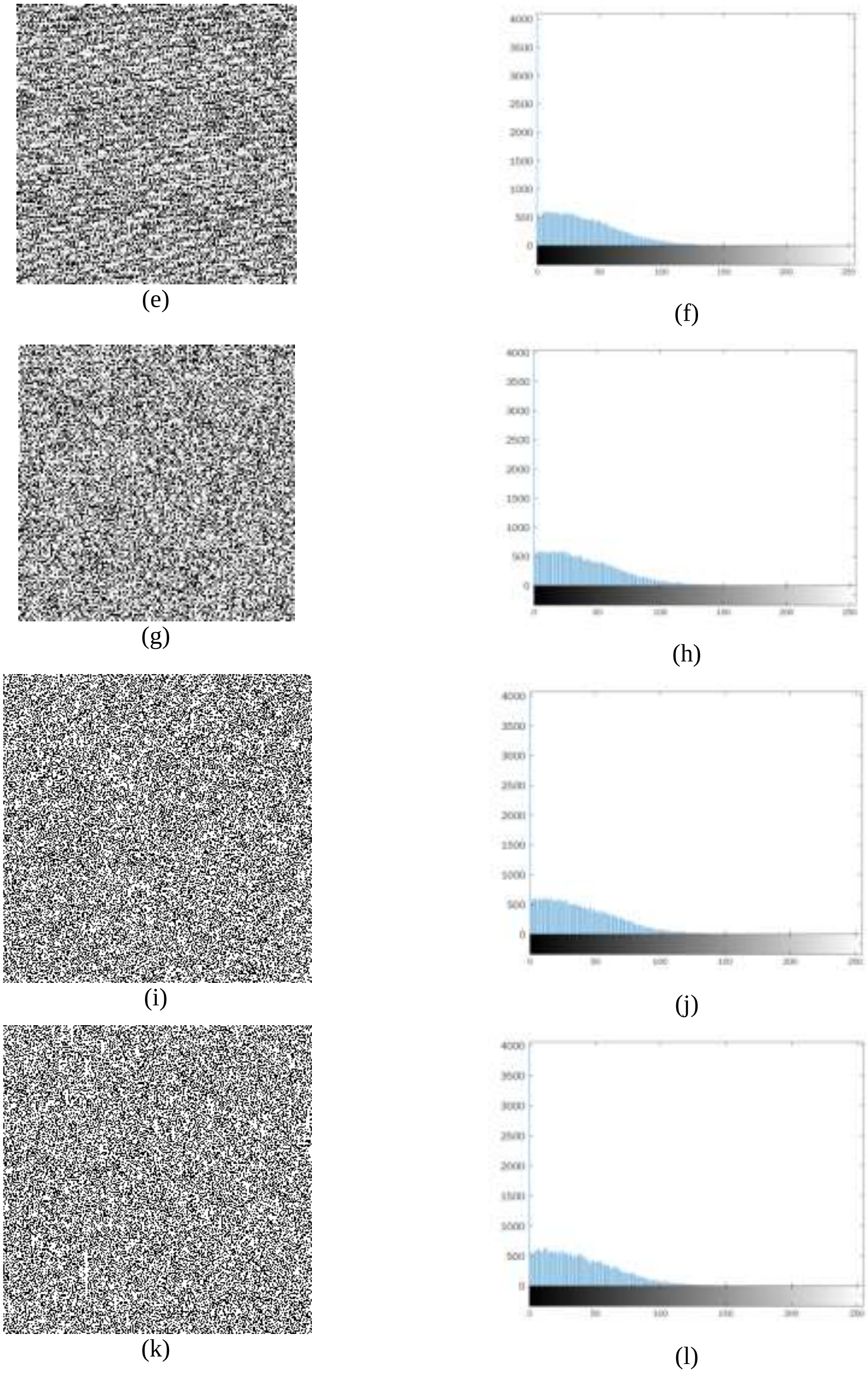
(b)



(c)



(d)



(e)

(f)

(g)

(h)

(i)

(j)

(k)

(l)

Fig.4. Encryption of the lena image with different chaotic maps. (a). input lena image (b). histogram of the input image (c). cipher image with the key generated using Chebyshev map (d). histogram of the cipher image generated in (c) (e). cipher image with the key

generated using circle map (f). histogram of the cipher image generated in (e) (g). cipher image with the key generated using Gauss chaotic map (h). histogram of the cipher image generated in (g) (i). cipher image with the key generated using piecewise chaotic map (j). histogram of the cipher image generated in (i) (k). cipher image with the key generated using Tent chaotic map (l). histogram of the cipher image generated in (k).

Input image	Type of chaotic map	Histogram variance	Entropy	NPCR%	UACI%
Lena	Chebyshev chaotic map	2391	6.9681	92.0294	33.0585
	Circle chaotic map	2380	6.9674	97.9529	30.077
	Gauss chaotic map	2573	6.9632	93.1723	32.3597
	Piecewise chaotic map	2381	6.9655	92.6245	32.7198
	Tent chaotic map	2377	6.9644	93.096	32.5703
Bird	Chebyshev chaotic map	2352	6.9567	92.7634	32.5672
	Circle chaotic map	2360	6.9594	96.5231	30.6904
	Gauss chaotic map	2339	6.9532	93.7857	32.2071
	Piecewise chaotic map	2342	6.9537	93.389	32.2803
	Tent chaotic map	2332	6.9511	93.8956	32.1003

Table-1: Performance metrics such as histogram variance, entropy, NPCR and UACI values for the proposed encryption algorithm.