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: 6 | June 2022 - Peer Reviewed Journal

TWO LEVEL IMAGE CRYPTOSYSTEM USING HYBRID-CHAOTIC KEY AND PRNG KEY FOR MULTI-MODALITY DIGITAL IMAGES WITH DISCRETE WAVELET TRANSFORM

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

[1]PG Student, [2]Assistant Professor, [3]Professor
Department of Electronics and Communication Engineering
Trichy Engineering College, Trichy, Tamil Nadu, India.

Article DOI: https://doi.org/10.36713/epra10450
DOI No: 10.36713/epra10450

ABSTRACT

In this information age, the need of secure picture transmission is critical. Medical data is hacked in the form of photographs, which costs more in terms of insurance claims. It is vital to safeguard photographs so that unauthorised individuals cannot view them. Chaos-based picture crypto systems are the most well-known of the several types of image crypto systems because their keys are invulnerable to assault or hacking. The chaotic features play a significant role in the development of keys for secure transmission and reception. The discrete wavelet transform (DWT) is a more basic transform that compresses the input image by combining approximation 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. A two level image encryption is adopted in this work, where one level is achieved using the hybrid-chaotic sequences and the next level is utilizing the pseudo random noise sequence (PRNG) as the keys. A smaller value of variance value is achieved which shows the higher uniformity of pixel values in encrypted images of our proposed two level image cryptography. Also the better performance metrics in terms of entropy, NPCR, and UACI are achieved compared to a single level image encryption. The developed image crypto system is designed and simulated using MATLAB software package.

KEYWORDS: *two level chaos image cryptosystems, DWT, encryption, hybrid-chaotic maps, and PRNG key generation.*

1. INTRODUCTION

Many applications require material security in the event of data transmission through a network or storage device. The cryptosystem is the best option for safeguarding and securing digital media. Because of its many important uses, such as cable TV, confidential talking, and so on, image encryption has gotten a lot of interest in research. Chaotic maps are one of the most successful picture encryption techniques. Researchers in the field of picture encryption have been drawn to chaotic maps because of their erratic performance and great sensitivity to the encryption key. These benefits ensure that Shannon's conditions for diffusion and confusion are met [1].

The cascading chaotic system (CCS) was introduced in [2], an universal chaotic framework with a simple and effective structure. Theoretically and experimentally, the chaotic performance of CCS is investigated. Two test standards are used to evaluate the proposed PRNG's random characteristics. T.Zhang et al. developed a fresh and easy approach to S-Box design based on the ancient Chinese I-Ching concept. In ancient China, the I-Ching was a compilation of 64 hexagrams containing comments regarding divination. The authors wanted to see how effective this new method is, so they utilized certain accepted criteria to assess the S-Box [3].

G.Ye suggested a method for securing personal photographs that included the following features: (1) a vast key space; (2) additional wave sources to build the complex of system; (3) key stream is generated based on the plain image; and (4) chaotic sequence to discover the wave's source point. Many applications, such as the military, meteorology, and medical science, use a chaotic image encryption technique. A patent is a type of picture encryption method that is used in everyday life [4]. The security of a standard diffusion mechanism (and its modifications) utilized as the basic cryptographic primitive in several picture cryptosystems based on complex dynamic phenomena was examined by the authors in [5.] Theoretically, the data complexity for recovering each piece of the key schedule process is the same regardless of the key schedule process, according to the authors. The data

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: 6 | June 2022 - Peer Reviewed Journal

complexity for recovering each element of the corresponding secret key from these diffusion mechanisms is only O, according to the authors, regardless of the key scheduling method (1). Numerical examples [6-8] are used to validate the proposed analysis.

To address the foregoing issues with picture encryption based on chaotic maps and DNA cryptography, the authors in this paper used the basic theory of the DNA sequence operation to encrypt image data and the combined chaotic maps and DNA sequence addition operation to implement image encryption. Extensive numerical experiment results revealed that the proposed image encryption algorithm has the benefits of unlimited key space and high-level security, because the problematic periodic windows are no longer present within the key space, and it is extremely robust against known-plain-text attacks, because the chaotic sequence generated bears no correlation whatsoever due to the folding effect of modulo operation. The algorithm [9, 10] is thought to make genuinely efficient and secure image encryption a reality.

In this paper, we proposed a two level image crypto system, where one type of encryption is applied in the approximate coefficients of the DWT transform and the next level is applied in the DWT transformed image. There are two different types of keys are used. Hybrid-chaotic keys are used in the first level and PRNG key is used in the second level of encryption.

2. PROPOSED IMAGE CRYPTOSYSTEM

Typical image cryptosystem is shown in Fig.1, where the common keys are utilized in the encryption side and in the decryption side. The intervention of the unauthorized third party can be avoided using the known common key between sender and receiver respectively in the encryption and in the decryption process. This work involves devising a two level image crypto algorithm for encryption of image for transmitting the image. The hybrid-chaotic key is generated from combining the individual chaotic sequences. The hybrid-chaotic key enables a wide range of initial values and provides more randomness to the encryption process. The hybrid-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 DWT. 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 IDWT transform to get the sub-cipher image. The sub-cipher image is again XORed with PRNG key to get the cipher image. This enables more randomness in the encrypted image and hence better performance. A detailed block diagram for the encryption process is depicted in Fig.2 and decryption process is detailed in Fig.3 where it involves reverse operations performed in the encryption process.

2.1. CHAOS AND PRNG 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 Fig.4 and Fig.5. The hybrid-chaotic sequences are generated using the individual chaotic sequence. The different hybrid-chaotic key sets are developed as follows.

The set-1 hybrid-chaotic key is generated by combining Chebyshev map, Circle map and Gauss maps. The set-2 is generated by combining Circle map, Gauss map, and Piecewise maps. The set-3 is generated by combining Gauss map, Piecewise map and Tent map. The set-4 is generated using Piecewise map, Tent map, and Chebyshev maps. The set-5 is generated using Tent map, Chebyshev map, and Circle map.

The PRNG key is generated using linear feedback shift-register (LFSR) where the primitive polynomial decides the required tapping or connections to the LFSR. At each iteration, the contents of the shift-register should be captured that act as the sample value in the key. We used an 8-bit LFSR primitive polynomial to generate 256x256x8 number of samples. Then the generated PRNG is assembled in a 2D manner.

2.2. THE IMAGE ENCRYPTION SYSTEM

The encryption is performed using DWT. The algorithm requires no additional memory for the inverse wavelet. The detailed encryption process is shown in Fig.2 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. The image cryptanalysis is done using the above mentioned four performance metrics such as histogram variance value, entropy value, NPCR and UACI values.

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: 6 | June 2022 - Peer Reviewed Journal

2.3. THE DECRYPTION SYSTEM

The decryption process is exactly the inverse of encryption operations are shown in Fig.4. The decryption process carried out in the same order how the keys are mixed with the input images as in the encryption process. First the cipher image is decomposed to different parts such as LL, LH, HL, HH. The low frequency components is encrypted, hence it is to be decrypted using the same keys what used in the encryption process. First PRNG key is applied to perform the level-1 decryption in the LL component and in the second level; the hybrid-chaotic key is applied to the LL component to get the reconstructed image. The two level image cryptosystem shows a better performance compared to single level image cryptosystem.

3. RESULTS AND DISCUSSIONS

The proposed two level image cryptosystem results in a better performance compared to the single level image crypto system. The following table lists the simulated results for the various input photos and encrypted images. The histogram analysis is used to demonstrate the encrypted image's uniformity and randomness while employing the various keys created by the chaotic maps. Figure.4 shows the example results for Lena image with various chaotic keys.

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 lower variance value of is obtained for all the type of hybrid-chaotic key and PRNG key. It is necessary to reduce the value of variance comparatively to the bench mark results. In our approach the information entropy value approximately 8 is obtained. As per the benchmark results we obtained entropy of 8, which shows that our propose image cryptosystem is a valid cryptosystem. In our proposed approach we obtained a NPCR value as high as 99.59 and low as 99.5621. This NPCR value also indicates that the proposed two level image cryptosystem outperforms well compared to the single level image crypto system. In our approach we obtained a maximum UACI value of 33.8468 and a minimum value of 33.155 is obtained. Hence, the proposed two level image cryptosystem resulted in a better performance metrics than the single level image cryptosystem comparatively, specific results are mentioned in previously published paper by the same author group [11].

4. CONCLUSION

An effective two level image 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 utilized hybrid-chaotic key using different chaotic maps and PRNG key. The performance metrics such as histogram plot, variance value, entropy value, NPCR, and UACI values shows that the proposed two level image cryptosystems outperforms well compared to single level image cryptosystem.

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.*
11. *Nithhyaadevi, K., Jenin, J. S., & Gandhimathi, G. (2022). Selective chaotic generation and multi-modality digital image crypto system using haar wavelets. EPRA International Journal of Research and Development (IJRD), 7(3), 38-43.*

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: 6 | June 2022 - Peer Reviewed Journal

FIGURES AND TABLES

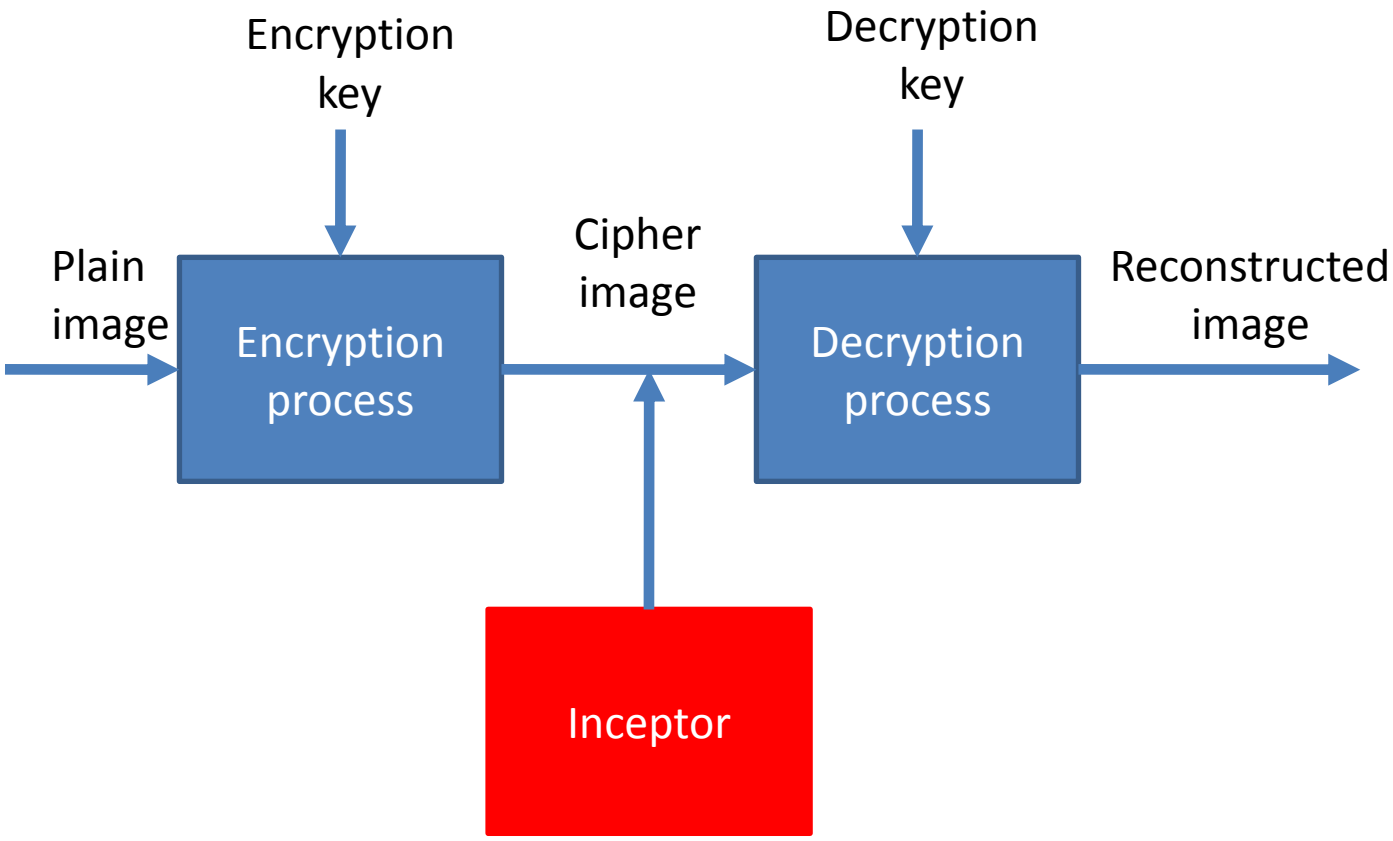


Fig. 1. Typical image crypto system

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: 6 | June 2022 - Peer Reviewed Journal

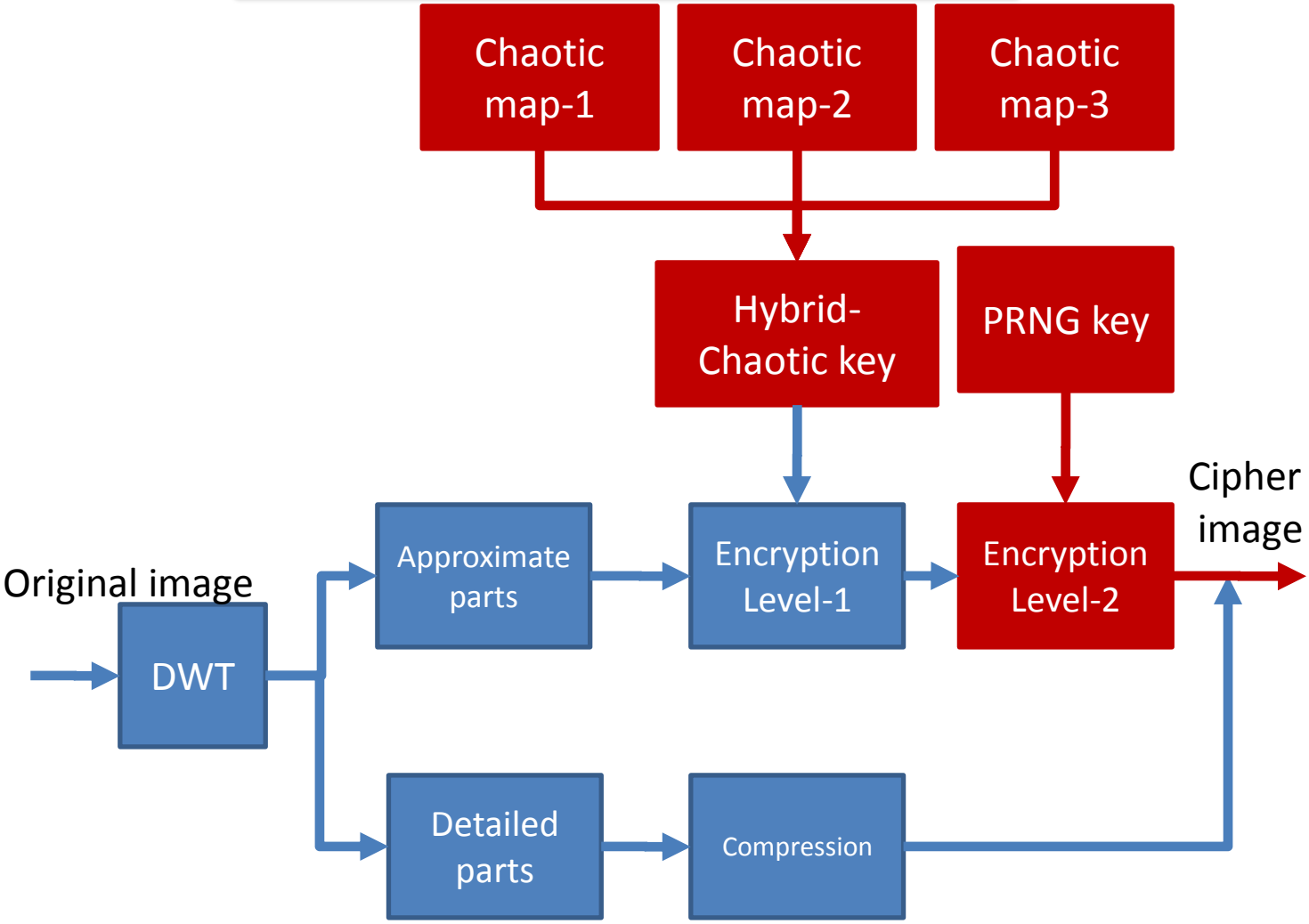


Fig. 2. Proposed encryption process

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: 6 | June 2022 - Peer Reviewed Journal

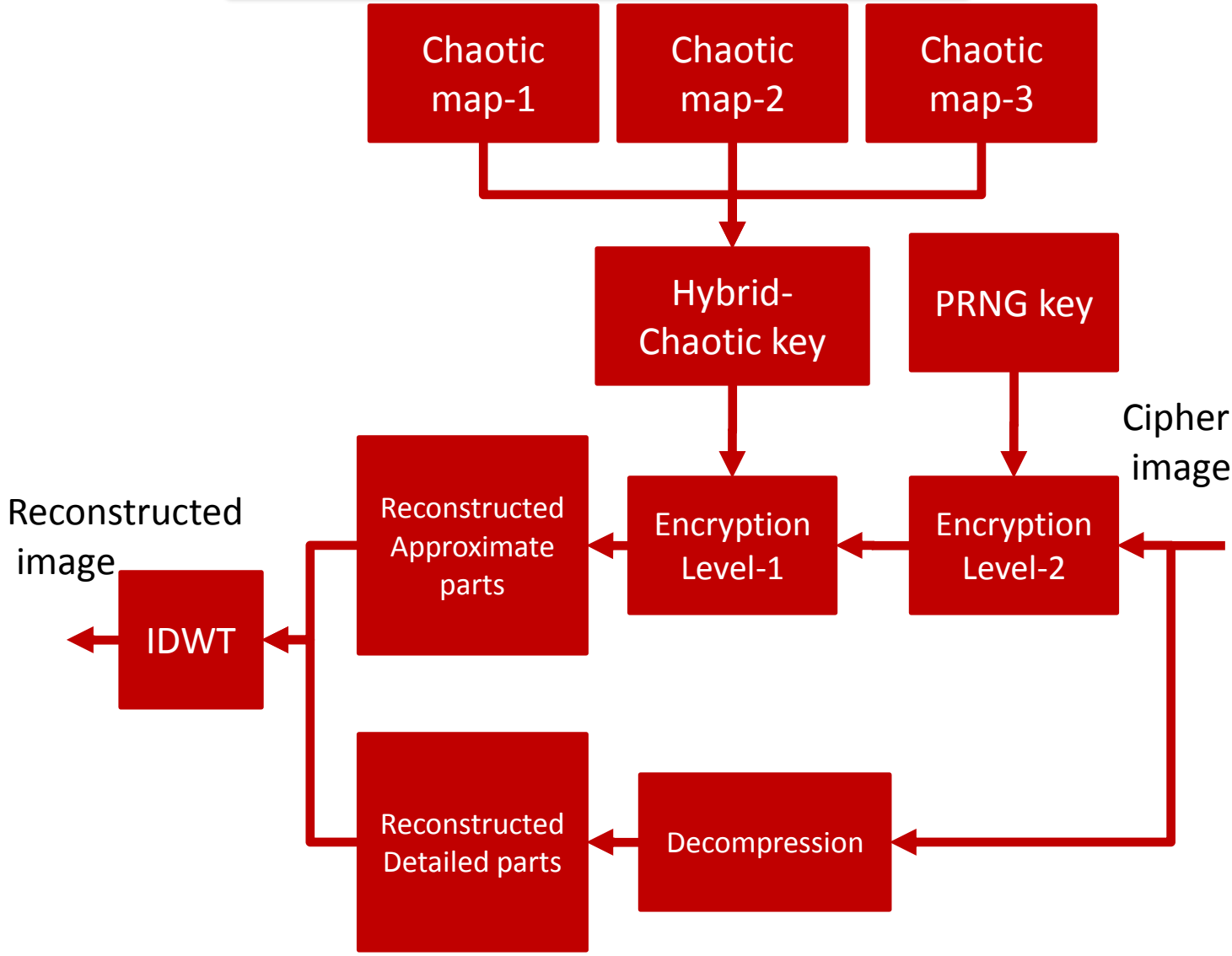


Fig. 3. Proposed decryption process

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: 6 | June 2022 - Peer Reviewed Journal

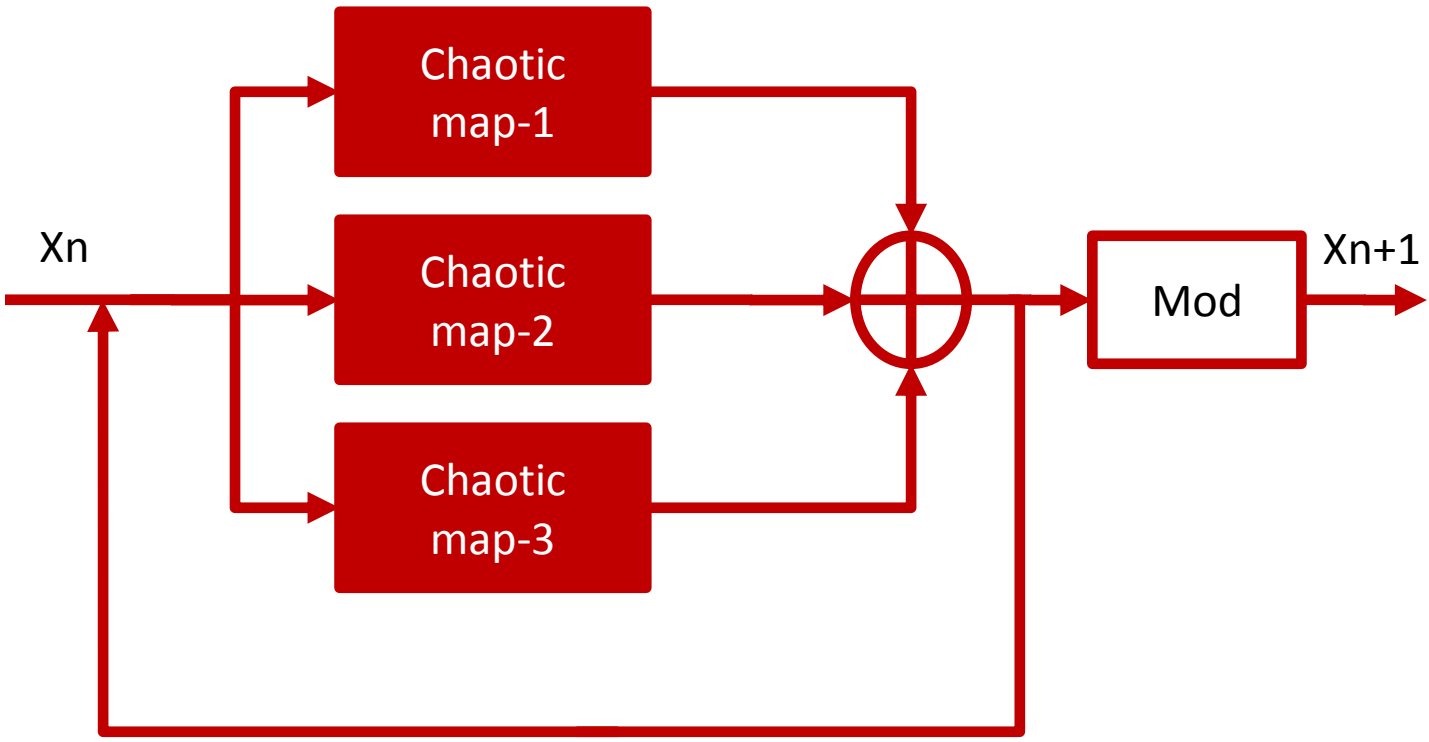


Fig. 4. Proposed hybrid-chaotic key generation mechanism

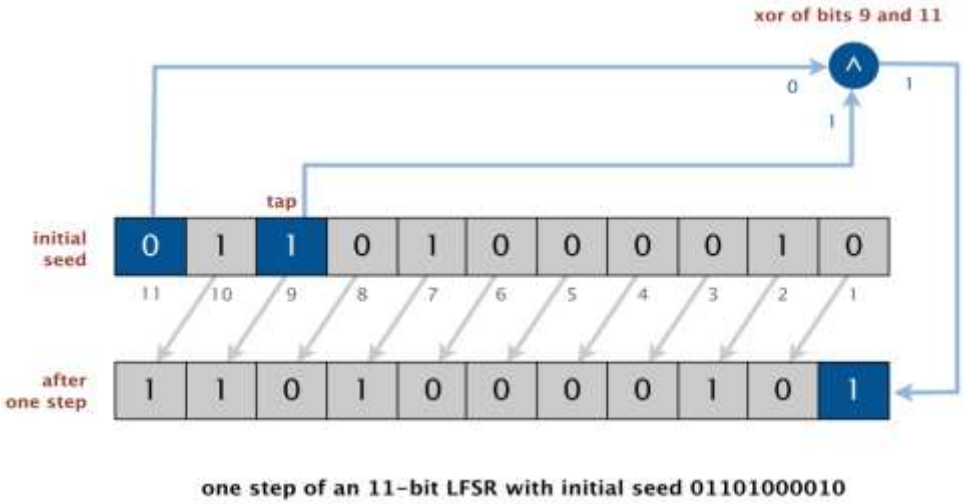
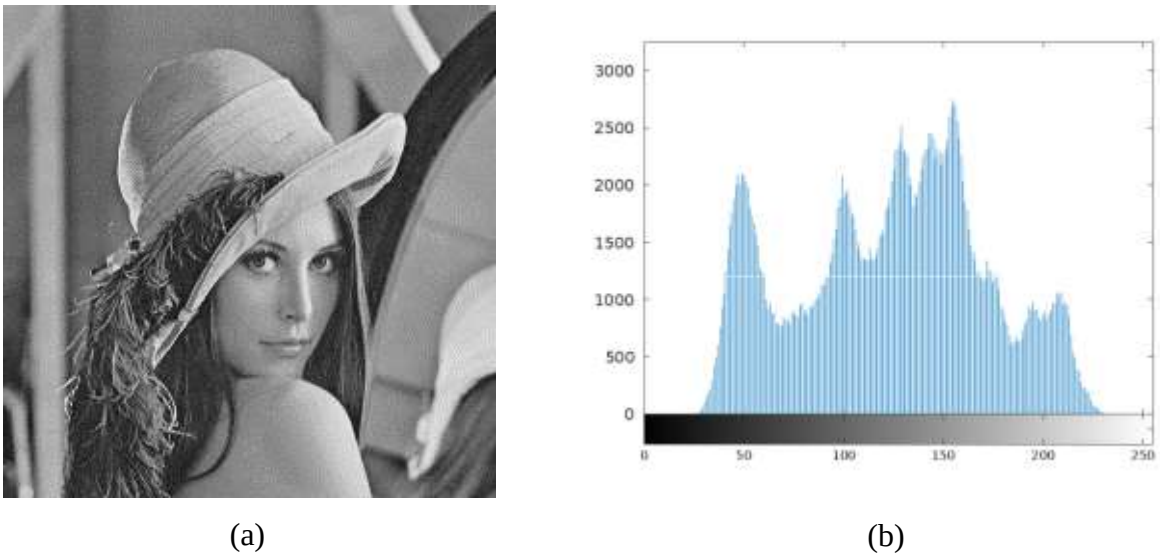


Fig. 5. Typical 11-bit LFSR for PRNG key generation mechanism

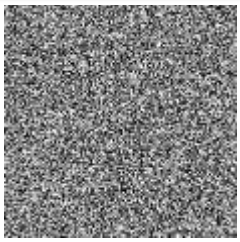
SJIF Impact Factor 2022: 8.197| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 7 | Issue: 6 | June 2022 - Peer Reviewed Journal



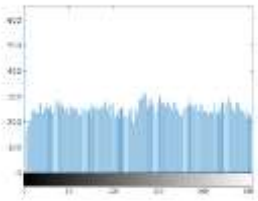
(a) (b)

Fig.6. The standard test input (a). Lena image (b). Histogram plot

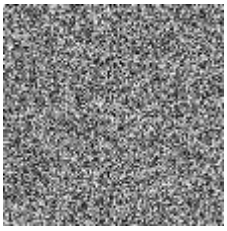
SJIF Impact Factor 2022: 8.197| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 7 | Issue: 6 | June 2022 - Peer Reviewed Journal



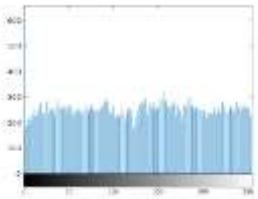
(e1)



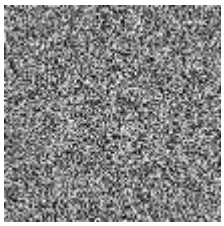
(h1)



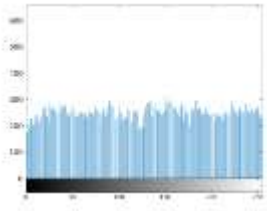
(e2)



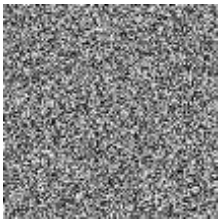
(h2)



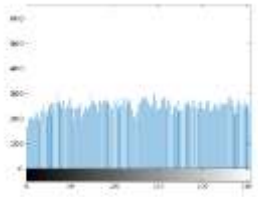
(e3)



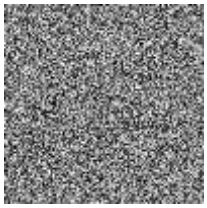
(h3)



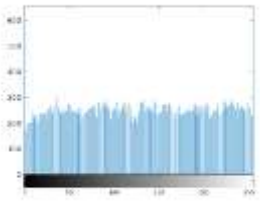
(e4)



(h4)



(e5)



(h5)

Fig.7. Encryption of the lena image with different PRNG key and hybrid-chaotic maps. The labels (e1 to e5) are the encrypted lena image with PRNG key and with the hybrid-chaotic key generated using (set-1 to set-5) respectively. The labels (h1 to h5) show the histogram of (e1 to e5) encrypted images.

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: 6 | June 2022 - Peer Reviewed Journal

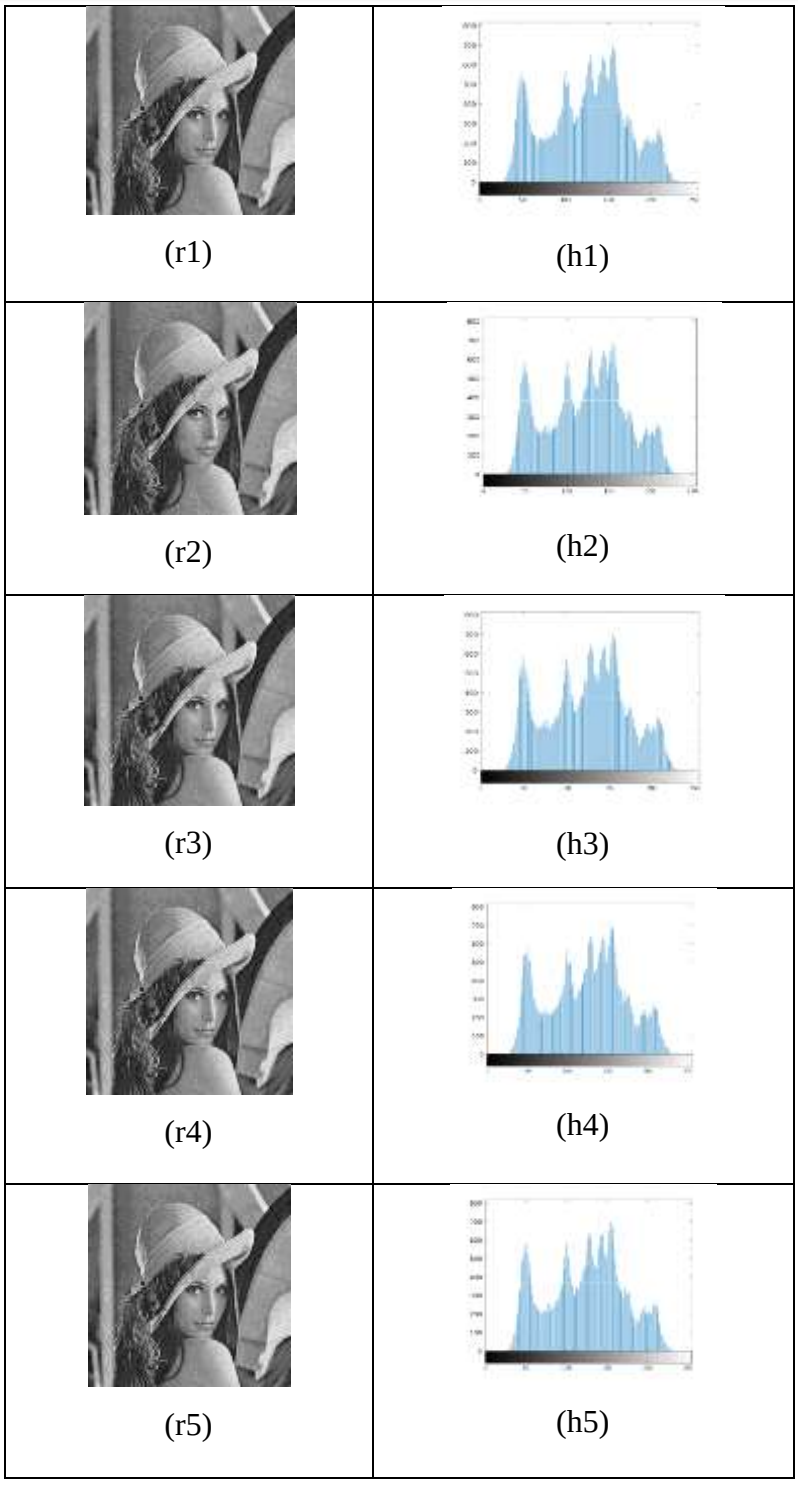


Fig.8. Reconstructed lena image using hybrid-chaotic and PRN key. The labels (r1 to r5) are the reconstructed image with PRNG key and hybrid-chaotic key generated using (set-1 to set-5) respectively. The labels (h1 to h5) show the histogram of (r1 to r5) reconstructed images.

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: 6 | June 2022 - Peer Reviewed Journal

Input image	Type of hybrid-chaotic map	Histogram variance	Entropy	NPCR%	UACI%
Lena	Type-1	846.6588	7.9767	99.5941	33.588
	Type-2	860.3444	7.9754	99.5621	33.8012
	Type-3	859.5561	7.9755	99.5819	33.8157
	Type-4	846.9568	7.9762	99.5636	33.6378
	Type-5	850.4199	7.9765	99.5941	33.8468
Bird	Type-1	823.8926	7.9659	99.588	33.176
	Type-2	833.4004	7.9659	99.588	33.2033
	Type-3	835.3973	7.9654	99.5895	33.2478
	Type-4	832.2385	7.9658	99.5941	33.1954
	Type-5	832.9087	7.966	99.588	33.155

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