Volume 65, Issue 5, 2021
Journal of Scientific Research
of
The Banaras Hindu University

A Random Dual-Security based An Image Encryption Scheme for IoT

Manish Gupta[*1], Kamlesh Kumar Gupta[2], and Piyush Kumar Shukla[3]

[*1]UIT-RGPV Bhopal, manishgupta.2007@gmail.com
[2]RJIT Tekanpur, kamlesh_rjitbsf@yahoo.co.in
[3]UIT-RGPV Bhopal, pphdwss@gmail.com

Abstract: **Due Nowadays, the demand for IoT-enabled devices is increasing exponentially and the communications between these devices are mostly in the form of color and gray-scale images. In the same sequence, the demand for IoT applications is also increasing, so it is a challenging task to protect the IoT applications from attackers. Therefore, an efficient encryption algorithm is required due to the limitation of IoT-enabled devices in terms of computational complexity and memory. In this work, a novel encryption scheme based on dual security is presented. Here in this work, dual security is used where at one level, the following keys (64 80-bit, and 96-bit) are used, which key size will be used for encryption, is unknown to the user during encryption and decryption. That means for each image, a unique random key size will be used for encryption. While at the second level, a new session key (Key size will be decided at level one) is generated for every image encryption, which increases the security at this level. So this two-level security will reduce the chances of a man-in-middle attack. This scheme uses the hybrid of crossover and logistic map which enhance the randomness in the presented scheme. The strength of the presented encryption scheme is estimated by checking the presented technique on various types of cryptographic attacks such as differential attack (NPCR), statistical attack (correlation analysis, entropy, and histogram analysis), noise attack, and prone to the user secret key. The experimental outcomes show that the presented hybrid scheme is secured enough against different cryptographic attacks.**

Index Terms: **Logistic chaotic map, Crossover, Session Key, dual security, Encryption, Decryption, IoT.**

I. INTRODUCTION

Due to the rapidly increasing smart devices such as IoT devices, approximately 70% of internet communication is in the form of gray-scale and color images. Since these communications are on the insecure and public channel, so these images must be secured from the various cryptanalytic attacks.
The existing encryption techniques such as DES, 3-DES, IDEA, and RC6 are not sufficient enough in a constrained environment because of lightweight, less memory, and low computational capability. To enhance the performance of image cryptographic systems without trade-off the security levels, a cryptographic system based on chaos theory is a well known choice for secure and fast transmission of images over the transmission system.

The main idea of this scheme is to extend an encryption algorithm for IoT enabled applications and devices that require less key size and high performance in terms of time and space complexity. Here we have used different key sizes used for both encryption and decryption. In this work, we have used 1-dimensional logistic map as well as 2-point crossover for increasing more diffusion and confusion in the generated pseudo-random sequences. These pseudo-random sequences are used to produce random unique session keys for both encryption and decryption.

The following is a summary of the entire presented system: In section 3, the presented methodology based on a hybrid of logistic map along with crossover operator is discussed in detail. Experimental results on various parameters are discussed in section 4. In section 5, the overall scheme is concluded.

II. RELATED WORK

As per an extensive literature review, the chaotic maps are of two different types, i.e., 1-dimensional (1-D) chaotic map [1-2] and multi-dimensional chaotic map [3-6]. In a 1-D chaotic map, few parameters and only one variable are used to produce

*Corresponding Author

different sequences randomly. The initial parameters are simply evaluated due to the less complex structure and small key space of 1-D chaotic map. So, it is less secured for color and gray scale image encryptions. While multi-dimensional chaotic map uses more than one initial variable, which improves the security but increases computational complexity.

Other logistic map based image encryption techniques are discussed in [7-9]. Genetic operations based image encryption algorithms are discussed in [10- 12]. Other chaotic maps, such as digital chaotic map [13], Bülban chaotic map [14], and hybrid chaotic map [15] based image encryption algorithms are also discussed here for getting more ideas about chaotic behaviour. Image encryption algorithms are classified based on pixel-level and bit-level. A new scheme is based on digit-level is described in [16]. For testing the proposed algorithm performance, [17-25] image encryption techniques are used. Session key based cryptographic algorithm is discussed in [26].

Recently, The IoT has become a lot of attention before researchers. Most of the objects in IoT enabled devices are wearable sensor devices, environmental sensors, and mobile devices. It is recorded from various sources that around ten billion devices by 2020 [27] will be connected to each other via Internet. For example, As per the estimation of a Cisco company, total connected devices per person would be 6.58 by 2020, i.e., around fifty billion devices in total [28]. But computation and storage capabilities of IoT enabled terminals are still severely limited [29].

The data (In the form of images) stored in these IoT terminals are strongly related to the user's private information, which are more sensitive and needs to be protected [30–32]. In the current scenario, users are more sensitive to protect privacy while using IoT technology [33–35].

III. Methodology

This work presented an efficient dual security based encryption scheme. In the first level of security, random key size (64-bits, 80-bits, and 96-bits) is used which is not known to the user. While in second level of security, a unique session key is used for cryptographic purpose and this unique random session key is produced by using the hybridization of crossover and logistic chaotic map. The presented encryption algorithm completes in 03 different phases, given below-

3.1 Key Generation Phase

This phase generates a secure unique session key by using the hybrid concept of crossover and logistic chaotic map. The details about logistic chaotic map and crossover are discussed in 3.1.1 and 3.1.2 sections respectively.

3.1.1 Logistic map

It is described by the following quadratic recurrence relation –

$$x_{m+1} = f(x) = a\, x_m (1 - x_m) \quad (1)$$

Where $a \in (1, 4)$ and $x_m \in (0, 1)$

3.1.2 2-Point Crossover Operator

In this section, two different crossover points are generated by using algorithm 1to create more diffusion in generated binary strings. Here for each image transmission, two-different crossover points are taken randomly.

3.2 Encryption Phase

This phase described the encryption process of presented scheme. Since in key generation three different keys, each having 64, 80, and 96-bit key in size, are generated. So image information will be encrypted by using any of the above key sizes. The key size will be selected by the random function that will be unknown to the user and also for encrypted image information; a new key size will be used each time for securing information from a man-in-middle attack. This two-level security will improve the efficiency of the presented algorithm. At the very first level, the presented scheme will select the key size and at the second level, a unique session key will be generated each time for encrypting image information. These two levels will work each time for each image encryption.

If a random function selects the 64-bit key size then the following encryption steps are held during the encryption phase. Here the encryption phase completes in two different swaps and 04 different rounds. Each encryption round contains two logical operators EX-NOR, EX-OR, and one user-defined function (f). The first and second swap is performed after the 1st and 3rd encryption rounds, respectively. This user-defined function is also based on a 2-point crossover. Algorithm 1 shows the steps of encryption using a 64-bit key

Algorithm 1

1: Separate the first 64-bits of plain-text into four consecutive blocks (B1, B2, B3, and B4), each having 16-bits in size.
2: Perform EX-NOR operation on block B1 with key K0.
3: Apply crossover function on a block taken from step 2. Now perform EX-OR operation between a block taken after performing crossover function and block B3.
4: Perform EX-NOR operation on block B4 with key K0.
5: Apply crossover function on a block taken from step 4. Now perform EX-OR operation between a block taken after performing crossover operation and a block B2.
6: Repeat the above steps for K1, K2, and K3.

Else if the random function selects the 80-bit key size then the following encryption steps are held during the encryption phase. In this case, the encryption phase completes in two different swaps and 05 different rounds. Algorithm 2 shows the encryption process using an 80-bit key.

Algorithm 3:

1: Separate the first 64-bits of plain-text into four consecutive blocks (B1, B2, B3, and B4), each having 16-bits in size.
2: Perform EX-NOR operation on block B1 with key K0.
3: Apply crossover function on a block taken from step 2. Now perform EX-OR operation between a block taken after performing crossover function and block B3.
4: Perform EX-NOR operation on block B4 with key K0.
5: Apply crossover function on a block taken from step 4. Now perform EX-OR operation between a block taken after performing crossover operation and a block B2.
6: Repeat the above steps for K1, K2, K3, and K4.

3.3 Decryption phase: The reverse procedure of encryption is performed in this phase.

IV. Simulated Results and Analysis

In this section, experiments on various parameters are performed for evaluating the efficiency of the presented scheme. 2 GB RAM and i3 processor are taken for simulations. MATLAB 2015 software is used for experiments. In this work, an 8-digit hexadecimal symmetric key "0123456789012345" is used for experimental purpose. The following lenna image is taken for experiment purpose. Figure 1 show the encryption and decryption process of presented scheme. Table 1 shows the simulated results using presented scheme on different parameters.

(Lenna Image)

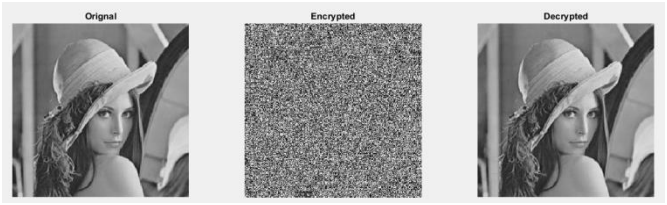

Figure 1: Encryption and decryption process

4.1 Key sensitivity analysis

Any encryption scheme is said to be secured if it is very much sensitive to the key. That means minor changes in the used key should reflect a greater change in the decoded image. For this, a well-known test, the Avalanche test, is used. According to the avalanche test, 1-bit flip in the key will change at least 50% bits in the decoded image. Figure 2 shows the presented scheme is key sensitive.

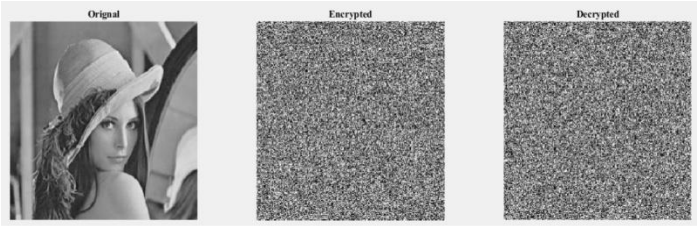

Figure 2: Key sensitivity test

4.2 Resistance to statistic attack

4.2.1 Histogram analysis

Histogram analysis is generally used to guess the similarities between the encrypted and the plain image. In this work, the histogram of encrypted image represents the uniform sharing of different pixels that shows the presented scheme is secured enough from statistical attacks. Figure 3 shows that the presented scheme is secured from statistical attack.

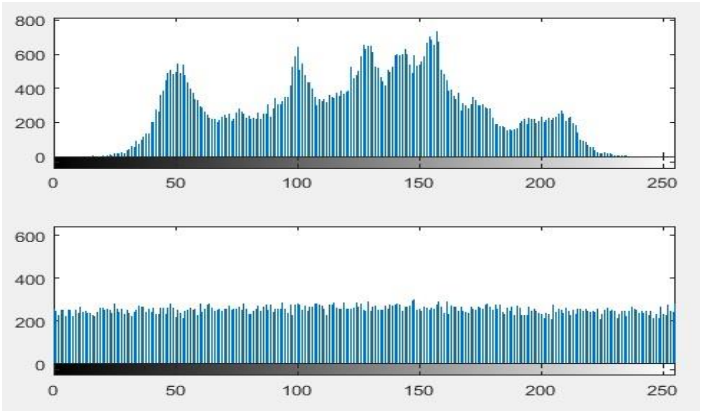

Figure 3: Histogram analysis of lenna image (Original and Encrypted)

4.2.2 Correlation analysis

The following equations are used to evaluate the correlation among adjacent pixels in cipher and plain image both.

$$\mathrm{COV}(w,x) = \mathrm{F}\big(w - \mathrm{F}(w)\big)\big(x - \mathrm{F}(x)\big) \quad (2)$$

$$\mathrm{R}_{wx} = \frac{\mathrm{Cov}(w,x)}{\sqrt{\mathrm{D}(w)}\sqrt{\mathrm{D}(x)}} \quad (3)$$

For numerical calculations, the following equations are used, where w and x represent the adjacent pixels value in a image.

$$F(w) = \frac{1}{M}\sum_{i=1}^{M} w_i \quad (4)$$

$$D(w) = \frac{1}{M}\sum_{i=1}^{M}(w_i - F(w))\big(x - F(x)\big) \quad (5)$$

$$COV(w,x) = \frac{1}{M}\sum_{i=1}^{M}(w_i - F(w))\big(x_i - F(x)\big) \quad (6)$$

In figure 3, it is cleared that there is no correlation (Vertical, horizontal, and diagonal) among adjacent pixels.

4.3 Resistance to differential attack:

The NPCR is used to compare the amount of different pixels in the two images as a percentage of the total number of pixels. A good encryption algorithm should have a higher NPCR value.

The following equation is used to evaluate the NPCR value-

$$NPCR = \frac{\sum_{i,k} B(i,k)}{H \times W} * 100\ \% \quad (7)$$

Where H is used for the height and W for the width of the image.

B (i, k) is defined as

$$B(j,i) = \begin{cases} 0, & \text{if } P1(i,k) = P2(i,k) \\ 1, & \text{Otherwise} \end{cases} \quad (8)$$

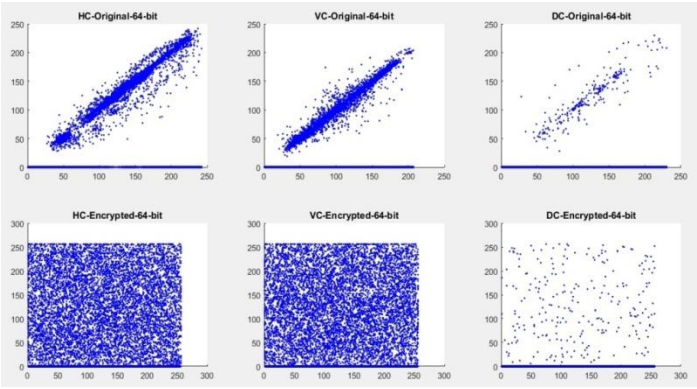

Figure 4: Correlation analysis (Horizontal, Vertical, and Diagonal)

Table 1: Simulated results of Lenna Image

Parameters	**Iteration 1**	**Iteration 2**	**Iteration 3**	**Average**
Entropy (Plain Image)	7.4509	7.4509	7.4509	7.4509
Entropy(Cipher Image)	7.9967	7.9963	7.9975	7.9968
NPCR	99.62	99.60	99.66	99.63
Horr. Correlation	0.0081	0.0023	0.0079	0.0061
Vert. Correlation	0.0084	0.0027	0.0073	0.0061
Diag. Correlation	0.0514	0.0404	0.0295	0.0404
Encryption Time	0.0087	0.0053	0.0074	0.0071

4.4 Comparison with existing techniques

This section shows the comparative chart between existing schemes and presented scheme. This comparative chart is shown in table 2.

Existing Techniques	**Key space**	**NPCR**	**Horr. Corr.**	**Verti. Corr.**	**Diago. Corr.**	**Entropy**
Ref. [13]	2^{440}	99.6185	– 0.0059	– 0.0146	0.0211	7.9992
Ref. [14]	2231	99.5956	0.0335	– 0.0174	– 0.0295	7.9976
Ref. [15]	>2100	99.6306	0.0039	0.0059	– 0.0050	7.9994
Ref. [16]	>10140	99.22	0.0036	0.0007	0.0053	7.9920
Presented work	296	99.66 (max)	0.0023(min)	0.0027(min)	0.0056(min)	7.9975(max)

V. CONCLUSION

A novel cryptographic scheme based on dual security is presented in this paper, which is most secure from different attacks such as differential attacks, noise attacks etc shown in experimental results. The main contributions in this scheme are –

a) This scheme provides dual security, one because of the selection of key size (It will be done during run time) and another due to the hybridization of crossover and logistic chaotic map. This dual security makes the presented scheme more efficient.
b) Also, a 2-point crossover operator is used in the encryption phase for enhancing diffusion in the presented scheme.
c) The presented scheme is lightweight because of its code length, i.e. 582 (In MATLAB).

Future work is to use the presented scheme in real world scenario.

REFERENCES

[1] Talhaoui, M. Z., Wang, X., & Midoun, M. A. (2020). A new one-dimensional cosine polynomial chaotic map and its use in image encryption. *The Visual Computer*, 1-11..

[2] Panwar, K., Purwar, R. K., & Jain, A. (2019). Cryptanalysis and improvement of a color image encryption scheme based on DNA sequences and multiple 1D chaotic maps. *International Journal of Bifurcation and Chaos*, *29*(08), 1950103.

[3] Elamrawy, F., Sharkas, M., & Nasser, A. M. (2018). An image encryption based on DNA coding and 2DLogistic chaotic map. *International Journal of Signal Processing*, *3*.

[4] Sharma, M. (2020). Image encryption based on a new 2D logistic adjusted logistic map. *Multimedia Tools and Applications*, *79*(1), 355-374.

[5] Ye, G., Jiao, K., Pan, C., & Huang, X. (2018). An effective framework for chaotic image encryption based on 3D logistic map. *Security and Communication Networks*, *2018*.

[6] Stalin, S., Maheshwary, P., Shukla, P. K., Maheshwari, M., Gour, B., & Khare, A. (2019). Fast and secure medical image encryption based on non linear 4D logistic map and DNA sequences (NL4DLM_DNA). *Journal of medical systems*, *43*(8), 267.

[7] Luo, Y., Yu, J., Lai, W., & Liu, L. (2019). A novel chaotic image encryption algorithm based on improved baker map and logistic map. *Multimedia Tools and Applications*, *78*(15), 22023-22043.

[8] Yang, B., & Liao, X. (2018). A new color image encryption scheme based on logistic map over the finite field Z N. *Multimedia Tools and Applications*, *77*(16), 21803-21821.

[9] Rostami, M. J., Shahba, A., Saryazdi, S., & Nezamabadi-pour, H. (2017). A novel parallel image encryption with chaotic windows based on logistic map. *Computers & Electrical Engineering*, *62*, 384-400.

[10] Mondal, B., Behera, P. K., & Gangopadhyay, S. (2020). A secure image encryption scheme based on a novel 2D sine–cosine cross-chaotic (SC3) map. *Journal of Real-Time Image Processing*, 1-18.

[11] Hikal, N. A., & Eid, M. M. (2018). A new approach for palmprint image encryption based on hybrid chaotic maps. *Journal of King Saud University-Computer and Information Sciences*.

[12] Mondal, B., & Mandal, T. (2020). A secure image encryption scheme based on genetic operations and a new hybrid pseudo random number generator. *Multimedia Tools and Applications*, 1-24.

[13] Lin, C. Y., & Wu, J. L. (2020). Cryptanalysis and Improvement of a Chaotic Map-Based Image Encryption System Using Both Plaintext Related Permutation and Diffusion. *Entropy*, *22*(5), 589.

[14] Ye, G., Jiao, K., Huang, X., Goi, B. M., & Yap, W. S. (2020). An image encryption scheme based on public key cryptosystem and quantum logistic map. *Scientific Reports*, *10*(1), 1-19.

[15] Wang, X., Guan, N., Zhao, H., Wang, S., & Zhang, Y. (2020). A new image encryption scheme based on coupling map lattices with mixed multi-chaos. *Scientific reports*, *10*(1), 1-15.

[16] Ping, P., Fan, J., Mao, Y., Xu, F., & Gao, J. (2018). A chaos based image encryption scheme using digit-level permutation and block diffusion. *IEEE Access*, *6*, 67581-67593.

[17] Wang, X., Feng, L., Li, R., & Zhang, F. (2019). A fast image encryption algorithm based on non-adjacent

dynamically coupled map lattice model. *Nonlinear Dynamics*, *95*(4), 2797-2824.

[18] Tang, J., Yu, Z., & Liu, L. (2019). A delay coupling method to reduce the dynamical degradation of digital chaotic maps and its application for image encryption. *Multimedia Tools and Applications*, *78*(17), 24765-24788.

[19] Talhaoui, M. Z., Wang, X., & Midoun, M. A. (2020). Fast image encryption algorithm with high security level using the Bülban chaotic map. *Journal of Real-Time Image Processing*, 1-14.

[20] Liu, Y., Zhang, J., Han, D., Wu, P., Sun, Y., & Moon, Y. S. (2020). A multidimensional chaotic image encryption algorithm based on the region of interest. *Multimedia Tools and Applications*, 1-37.

[21] You, L., Yang, E., & Wang, G. (2020). A novel parallel image encryption algorithm based on hybrid chaotic maps with OpenCL implementation. *Soft Computing*, 1-15.

[22] Roy, S., Rawat, U., Sareen, H. A., & Nayak, S. K. (2020). IECA: an efficient IoT friendly image encryption technique using programmable cellular automata. *Journal of Ambient Intelligence and Humanized Computing*, 1-20.

[23] Li, R. (2020). Fingerprint-related chaotic image encryption scheme based on blockchain framework. *Multimedia Tools and Applications*, 1-21.

[24] Dagadu, J. C., Li, J. P., & Aboagye, E. O. (2019). Medical image encryption based on hybrid chaotic DNA diffusion. *Wireless Personal Communications*, *108*(1), 591-612.

[25] Liu, H., Zhao, B., & Huang, L. (2019). A novel quantum image encryption algorithm based on crossover operation and mutation operation. *Multimedia Tools and Applications*, *78*(14), 20465-20483.

[26] Gupta, M., Gupta, K. K., & Shukla, P. K. (2020). Session key based fast, secure and lightweight image encryption algorithm. *Multimedia Tools and Applications*, 1-26.

[27] Nordrum, A. (2016). The internet of fewer things [news]. *IEEE Spectrum*, *53*(10), 12-13.

[28] Evans D., "Internet of things research study," Cisco, Tech. Rep., April 2011, http://www.cisco.com/c/dam/en us/about/ac79/docs/innov/IoT IBSG 0411FINAL.pdf, Accessed on 22 June 2017.

[29] Liu, B., Li, Y., Zeng, B., & Lei, C. (2016). An efficient trust negotiation strategy towards the resource-limited mobile commerce environment. *Frontiers of Computer Science*, *10*(3), 543-558.

[30] Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102.

[31] Jurcut, A., Niculcea, T., Ranaweera, P. *et al.* Security Considerations for Internet of Things: A Survey. *SN COMPUT. SCI.* **1,** 193 (2020). https://doi.org/10.1007/s42979-020-00201-3.

[32] Wu, D., Si, S., Wu, S., & Wang, R. (2017). Dynamic trust relationships aware data privacy protection in mobile crowd-sensing. *IEEE Internet of Things Journal*, *5*(4), 2958-2970.

[33] Li, J., Liao, X. & Puech, N. Security and privacy in IoT communication. *Ann. Telecommun.* **74,** 373–374 (2019). https://doi.org/10.1007/s12243-019-00718-6.

[34] Yeh, KH., Su, C., Deng, R.H. *et al.* Special issue on security and privacy of blockchain technologies. *Int. J. Inf. Secur.* **19,** 243–244 (2020). https://doi.org/10.1007/s10207-020-00496-6.

[35] Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2020). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers*, 1-22.

***