Volume 65, Issue 1, 2021
Journal of Scientific Research
Institute of Science,
Banaras Hindu University, Varanasi, India.

Session Key based Image Cryptographic Algorithm using Logistic-Sine Map and Crossover Operator for IoT

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

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

Abstract: **Due to the increasing demand for IoT applications in various fields such as healthcare, smart city, smart grids, industrial internet, etc. The privacy and security become a major issue in front of various researchers working in this field. This work proposed a novel image encryption algorithm based on a logistic-sine map and crossover operator of a genetic algorithm. Various 1-D chaotic maps are discussed in the literature review, but in some cases, hybrid 1-D chaotic maps have higher performance than simple 1-D chaotic maps. So 1-D chaotic map along with a crossover operator is used in this work. Here logistic-sine maps and crossover are used to generate the random session key for each image encryption. Also, a crossover operator is used in encryption rounds for increasing confusion and diffusion. Here in this work, for each image encryption, a new session session key is generated. The proposed algorithm is tested on various parameters for effective randomness. Experimental results show that the proposed algorithm performance is better than existing algorithms in terms of randomness and secure enough to resist all the existing cryptanalytic attacks.**

Index Terms: **Image Encryption, Crossover, Logistic-Sine map, Session Key, Random function, Image Decryption, IoT.**

I. INTRODUCTION

Nowadays the uses of IoT applications are increasing exponentially by seeking the demand of these applications in various fields such as healthcare or medical image security, smart city, smart grid, etc. Around 70% of the communication over the internet is in the form of images. Existing algorithms such as AES, IDEA, DES, RC4, RC5 etc are not sufficient enough for IoT devices in terms of less time and space complexity. So for improving security by considering the IoT devices requirements, a chaos-based cryptographic system is one of the best choices for transmission on images using a fast and secure way of transmission. (Elhoseny, M et al., 2018) presented a hybrid security model for secure data transmission in IoT based health care field. (Elhoseny, M et al., 2018) also presnted another secure IoT based model for secure data tranmission.

Recently, The IoT has become a lot of attention before researchers because of various security (Tankard, C. et al., 2015) and privacy issues (Hameed, S. et al., 2019). Most of the objects in IoT such as wearable sensor devices, mobile devices, and environmental sensors. It is recorded that around 50 billion smart devices till 2020 will be connected via the Internet. But the computation and storage capabilities of IoT terminals are still severely limited (Liu, B. et al., 2016).

The data stored in these IoT terminals are closely related to the personal information of users, which are more sensitive and needs to be protected (Shen, J. et al., 2018). (Xiong, J. et al., 2018) introduced a new technique for improving the privacy in IoT applications. (Wu, D. et al., 2017) presented a amother scheme for data privacy. To protect privacy of user's information is one of the major issue concerns behind people to use IoT technology (Peng, S.et al., 2017). Other schemes related to privacy protection (Cai, Z. et al., 2017) and (Wang, H. et al., 2017) are described for IoT enabled devices.

By considering the above issues, this work proposed a session key based novel lightweight and secure image encryption algorithm using logistic-sine map and crossover operator of genetic algorithm. The motivation behind this work is to develop an algorithm which is lightweight, secure, and fast for IoT-

*Corresponding Author

enabled devices. Since IoT devices having less memory and required fast and secure applications, so this work fulfils the requirements of IoT applications.

The whole work is summarized in three different sections; In section 2, presented method is discussed in details. All the experiments are performed in section 3. Finally, in section 4, the whole work is concluded.

II. METHODS AND MODELS

This work presented a novel session key based lightweight image cryptographic system. It is based on two important concepts - the first one is a logistic-sine chaotic map, which is used in the key generation phase of the cryptographic system and the other one is a crossover operator, which is used for increasing diffusion in the presented system. Here, for each image encryption, a new unique session key is generated.

A. Logistic-sine map

The logistic-sine chaotic map (Demir, F. B et al., 2020) uses the concept of both logistic chaotic map and sine chaotic map. So it is also called a hybrid chaotic map. Since its chaotic interval is much higher than both logistic and sine chaotic maps, so we have used this hybrid chaotic map in this work.

Mathematical equations of sine map, logistic map and logistic-sine map are given below-

$$x(i+1) = a * x(i) * (1 - x(i)) \quad (1)$$

$$x(i+1) = \sin(pi * x(i)) \quad (2)$$

$$x(i+1) = \left(a * x(i) * \left(1 - x(i)\right) + ((4 - a)\sin(pi * x(i))/4\right) (mod 1) \quad (3)$$

Here equation (1) is for the logistic map, equation (2) for sine map, and equation (3) for logistic sine map.

B. Crossover Operator

It's a well-known operator of genetic algorithm (Mondal, B. et al., 2020). The main motive to use this operator in this work is to increase the diffusion in the generated sequences. It takes two strings of same length and finds two random crossover points to perform crossover in the generated sequences. Algorithm 1 shows the steps to perform crossover -

Algorithm 1

1. Calculate the length of sequences on which crossover is performed.
2. Find the value of first_index and last_index of sequence.
3. Calculate the random value of crossover points (p1 and p2) by using the following functions:

function1 (p1) = round ((last_index – start index) * rand () + start_index)

function 2(p2) = round ((last_index – start_index) * rand () + start_index)

Now, If the value of function1 is greater than the value of function 2 then swap the values; otherwise not.

4. With the help of these crossover points, divide the sequences into three different sub sequences.

s1 = sequence1 (start_index : p1)
s2= sequence 2 (p1 + 1: p2)
s3= sequence 1 (p2+1 : last_index)

and

t1 = sequence2 (start_index: p1)
t2 = sequence1 (p1 + 1 : p2)
t3 = sequence2 (p2 + 1 : last_index)

5. Finally, combine these sequences to generate new random sequences.

The proposed cryptographic system works as follows-

1. Input color image in .jpg format.

2. Resize the input color image into 256*256 size and convert input image into gray-scale image. In this work, experiments are performed on 256*256 size color images.

3. Input 16-digit symmetric hexadecimal key for encryption/decryption. In this work, "0123456789012345" symmetric key is used to perform experiments.

4. Convert the symmetric key into binary representation.

5. Apply uniform mutation operation on the 64-bit binary symmetric key.

6. Divide input 64-bit symmetric key into four consecutive blocks, named as block 1, 2, 3 and 4.

7. Add one 16-bit random block, named as block 5, to make the symmetric key 80-bit of size.

8. Now divide each block into two different sub-blocks, each having 8-bit in size.

9. Perform two-point crossover operations between two sub-blocks of same block. After performing crossover, two new 8-bit sub blocks are received. Same operations are performed between sub-blocks of each block.

10. Combine these newly generated 8-bit sub-blocks for making new five blocks.

11. Now generate five new blocks using logistic-sine chaotic map by using random initial value.
12. Finally generate five new keys by performing logical operation between blocks generated by crossover operations and logistic-sine map.

13. Now use first 64-bits of input image and perform encryption process by using newly generated keys in five different rounds. Here first generated key is used for round 1; second generated key is used for round2; and so on. After round 1 and round 3, two swaps are performed for increasing diffusion. Each round is also uses one user defined function in the form of crossover.

Step 14: After performing the same process used in step 13 for all 64-bits of input image, an encrypted image received for communications between IoT enabled devices.

Step 15: Perform reverse procedure of encryption to decrypt the image.

The proposed work is secure from brute force attacks because, in this work, we have used a 64-bit symmetric key and using an 80-bit key for encryption and decryption. Also for every image encryption, a new unique session key is generated. So here intruders need to check all the combinations of 64-bit keys, 72-bit key and 80-bit keys for finding the right key for decryption. Also, the above checking for keys finding, will be done for each image because each image is encrypted with a unique session key.

III. RESULTS AND DISCUSSIONS

This section contains the experimental results performed on various parameters such as NPCR, Entropy, Correlation, and Histogram analysis. Here MATLAB 2015 version software, a system having Core i3 processor, and 2GB RAM are used for performing proposed work. Figure 1 shows the original, encrypted, decrypted lenna and baboon image. The following Lenna image is used for performing operations. Figure 2 shows the block diagram of presented scheme.

(Lenna and Baboon Image)

(a) NPCR: The following formulas are used for performing NPCR operation.

The NPCR of the two images is given below-

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} * 100\ \% \tag{4}$$

Where W and H are the Width and Height of the image and D(i, j) is defined as

$$D(i,j) = \begin{cases} 0, & \text{if } C1(i,j) = C2(i,j) \\ 1, & \text{Otherwise} \end{cases} \tag{5}$$

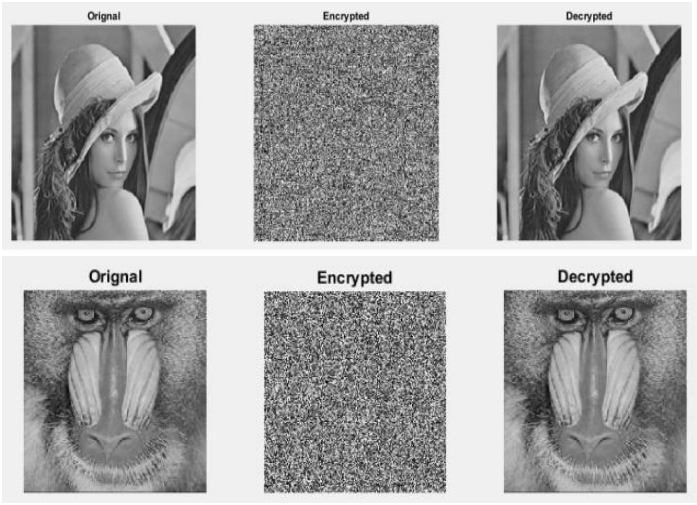


Figure 1: Original, encrypted and decrypted lenna and baboon image

(b) Entropy: It is a statistical measure of randomness that can be used to characterize the texture of the input image. For calculating entropy, the following formula is used –

$$E(m) = \sum_{j=0}^{M-1} p(m_j) \log \frac{1}{p(m_j)} \tag{6}$$

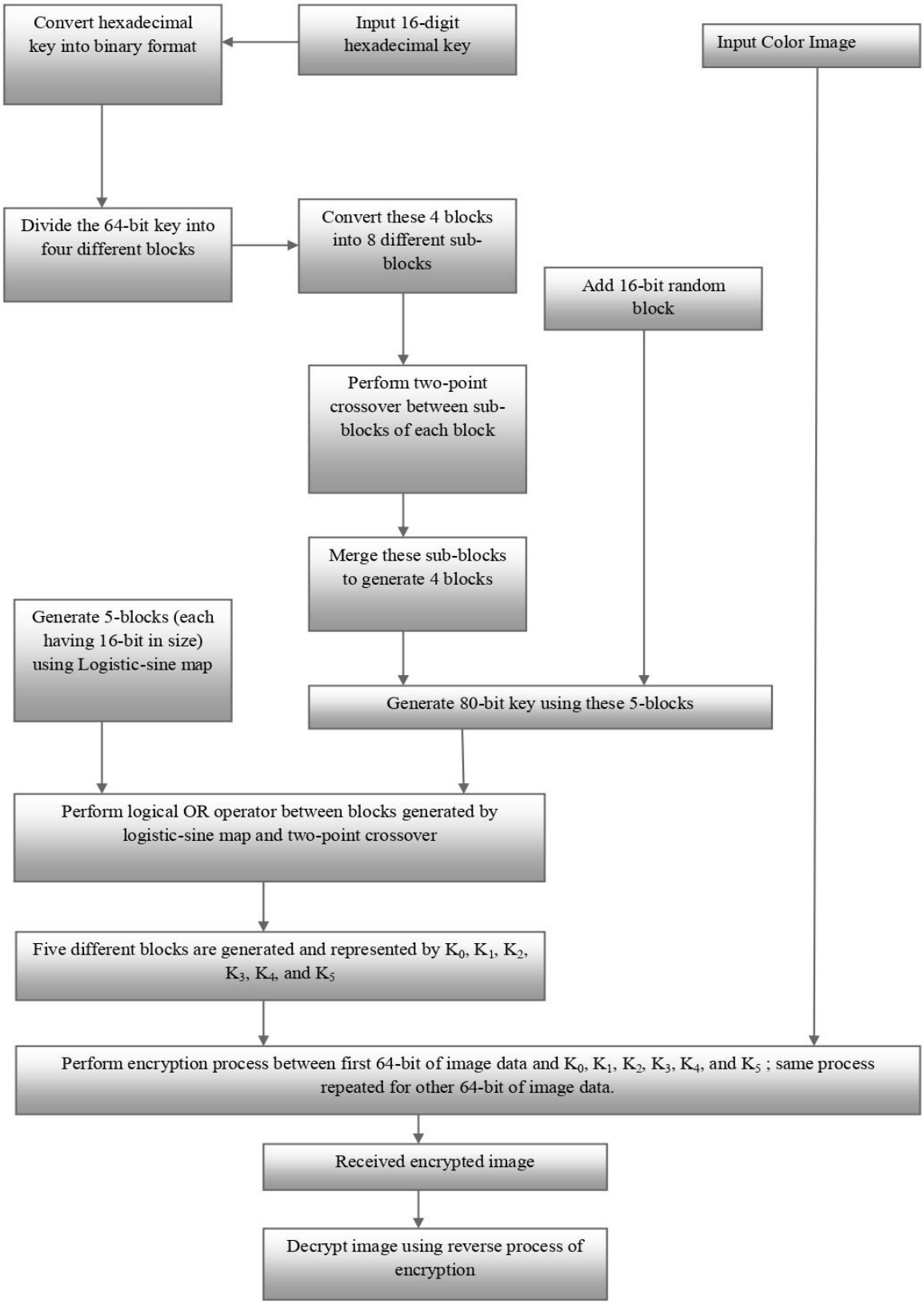


Figure 2: Block diagram of presented scheme

Table 1: Comparative chart of NPCR and Entropy between presented and existing work

Existing schemes	NPCR	Entropy
Liu, Y. et al., 2020	99.22	7.9920
You, L. et al., 2020	99.65	7.9457
Roy, S. et al, 2020	99.78	7.9646
Dagadu, J. et al., 2020	99.64	7.9972
Proposed work (Max)	99.65	7.9975

Table 1 shows the comparative analysis of proposed work and the existing algorithms in terms of NPCR and Entropy. The experiments results in this table shows that effectiveness of proposed work while using less key size comparative to the existing algorithms.

(c) Correlation: The following formulas are used to calculate horizontal, vertical and diagonal correlation –

$$\mathrm{Cov}(w,x) = F\big(w - F(w)\big)\big(x - F(x)\big) \quad (7)$$

$$R_{wx} = \frac{\mathrm{Cov}(w,x)}{\sqrt{D(w)}\sqrt{D(x)}} \quad (8)$$

For numerical computations between the two adjacent pixels values, the following equations are used-

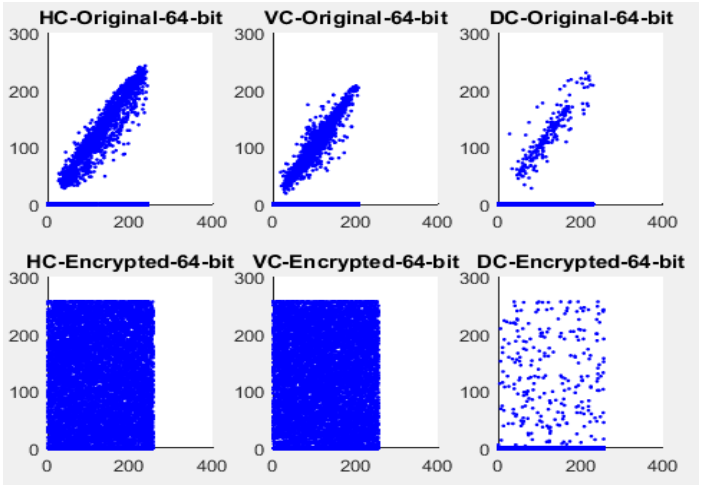
$$F(w) = \frac{1}{M}\sum_{i=1}^{M} w_i \quad (9)$$

$$D(w) = \frac{1}{M}\sum_{i=1}^{M}(w_i - F(w))\big(x - F(x)\big) \quad (10)$$

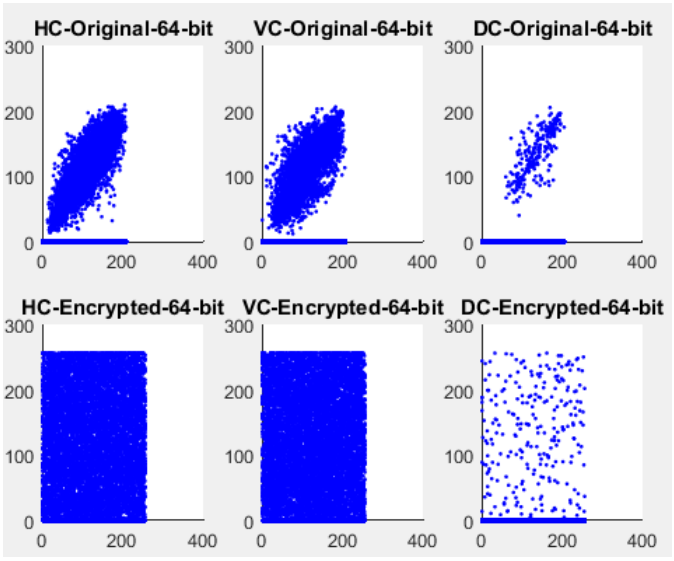
$$\mathrm{Cov}(w,x) = \frac{1}{M}\sum_{i=1}^{M}(w_i - F(w))\big(x_i - F(x)\big) \quad (11)$$

Figure 3 shows the all correlations of original and encrypted (lenna and baboon) image.

(d) Histogram: Statistical similarities between the cipher and original image are measured with the help of histogram analysis. Figure 3 shows the histogram of original and encrypted lenna and baboon image.

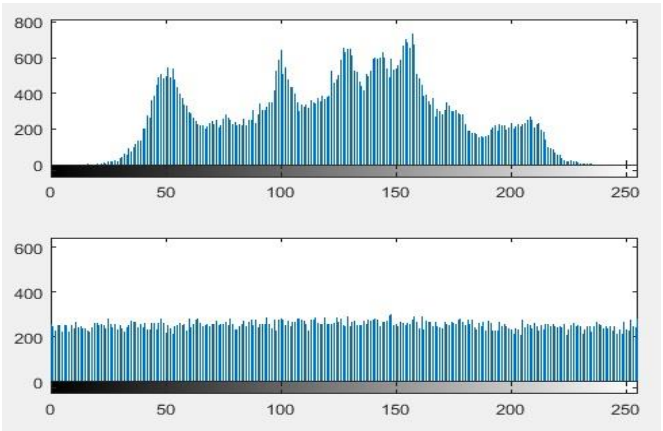


(a)

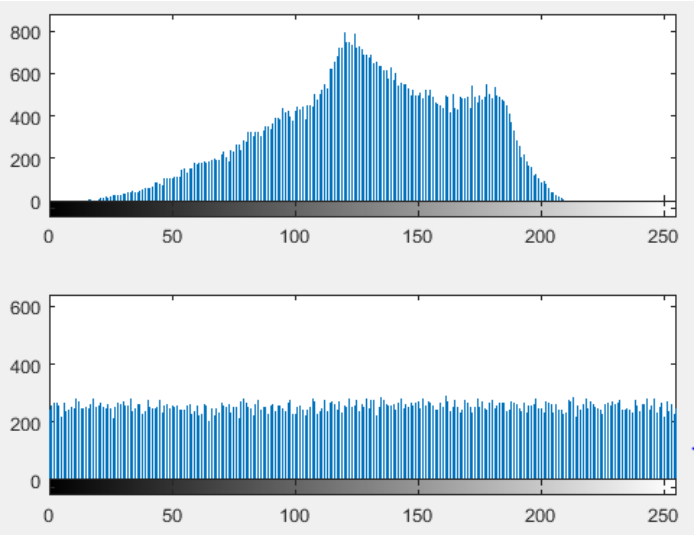


(b)

Figure 3: Horizontal, vertical, and diagonal correlation of original and encrypted (Lenna image (a), Baboon Image (b)).



(a)



(b)

Figure 4: Histogram of the original and encrypted (Lenna image (a), baboon image (b)).

Conclusion And Future Work

This work presented a novel session key based image encryption algorithm using a hybrid of logistic-sine chaotic map and crossover operation of a genetic algorithm. The use of a logistic-sine map increases the randomness in the proposed algorithm and crossover operation is used for increasing confusion and diffusion. Since this work uses 80-bit key for encryption and decryption and also uses less number of encryption rounds, so this encryption algorithm is more suitable for IoT applications because of its light weight and good performance on image data as compared to heavy weight algorithms shown in comparative chart. Future work is to use the proposed algorithm on IoT hardware for testing the practical efficiency of proposed work.

References

Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O. M., Shawkat, S. A., Arunkumar, N., & Farouk, A. (2018). Secure medical data transmission model for IoT-based healthcare systems. *Ieee Access*, *6*, 20596-20608.

Elhoseny, M., Shankar, K., Lakshmanaprabu, S. K., Maseleno, A., & Arunkumar, N. (2018). Hybrid optimization with cryptography encryption for medical image security in Internet of Things. Neural computing and applications, 1-15.

Tankard, C. (2015). The security issues of the Internet of Things. Computer Fraud & Security, 2015(9), 11-14.

Hameed, S., Khan, F. I., & Hameed, B. (2019). Understanding security requirements and challenges in Internet of Things (IoT): A review. Journal of Computer Networks and Communications, 2019.

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.

Shen, J., Wang, C., Li, T., Chen, X., Huang, X., & Zhan, Z. H. (2018). Secure data uploading scheme for a smart home system. Information Sciences, 453, 186-197.

Xiong, J., Ren, J., Chen, L., Yao, Z., Lin, M., Wu, D., & Niu, B. (2018). Enhancing privacy and availability for data clustering in intelligent electrical service of IoT. IEEE Internet of Things Journal, 6(2), 1530-1540.

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.

Peng, S., Yang, A., Cao, L., Yu, S., & Xie, D. (2017). Social influence modeling using information theory in mobile social networks. Information Sciences, 379, 146-159.

Cai, Z., Yan, H., Li, P., Huang, Z. A., & Gao, C. (2017). Towards secure and flexible EHR sharing in mobile health cloud under static assumptions. Cluster Computing, 20(3), 2415-2422.

Wang, H., Zheng, Z., Wu, L., & Li, P. (2017). New directly revocable attribute-based encryption scheme and its application in cloud storage environment. Cluster Computing, 20(3), 2385-2392.

Demir, F. B., Tuncer, T., & Kocamaz, A. F. (2020). A chaotic optimization method based on logistic-sine map for numerical function optimization. Neural Computing and Applications, 1-13.

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.

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.

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.

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.

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.

***