Artificial & Computational Intelligence/Published Online: December 2020
https://acors.org/ijacoi/VOL1_ISSUE5_06.pdf

Artificial & Computational Intelligence

A Robust Image Cryptographic Techniques: A Survey

[1]Rashmi Rajput, [2]Manish Gupta, [3]Pankaj Sharma
Department of Computer Science and Engineering
[1]rashmirajput978@gmail.com , [2]manishgupta.2007@gmail.com, [3]pnkjsharma07@gmail.com
Vikrant Institute of Technology & Management, Gwalior, Madhya Pradesh, India

Abstract

Nowadays most of the communication by IoT enabled devices such as mobile phones are in the form of images and these images may contain lots of confidential information. To protect these images from intruders, there is a need of secure image cryptographic algorithm. Most of the IoT enabled devices are having less memory and require faster communication. So there is a need of faster and lightweight image cryptographic algorithm. This work represents a survey of latest research work held to develop fast, secure and lightweight image cryptographic algorithm that will help to do more efficient research in this field.

.

Keywords – Image Encryption, Image Decryption, Lightweight, Cipher text, Crossover, Mutation, Chaos Theory.

1. INTRODUCTION

With the advent of the Internet and the World Wide Web, the amount of digital information to be stored and communicated has grown exponentially beyond imagination. This digital information not only comprises text but also has a large volume of an image, audio/video, and multimedia data, which comparatively is very bulky than the textual information. The images as on date have become an integral and vital component of any useful data and are widely used in several important applications. Few of these crucial applications include Military Image Database & Message Communication, Confidential Video Conferencing, Medical Imaging System & Telemedicine, Online Personal Photograph Albums, Natural Disaster or Catastrophe Alarming Systems, Online Image Identification and Authentication, Reflection Seismology, Electronic Surveillance Systems, Document Imaging, Image 'CAPTCHA', Image Registration, Geographic Information System, etc.

This work contains the latest research work held in cryptographic field to develop a new fast, secure and light weight algorithm.

Rest of the paper is organized as follows: In section 2, Existing techniques related to lightweight image cryptographic algorithm are discussed. In section 3, the overall work is summarized.

2. RELATED WORK

Various researchers are working in the field of image cryptographic techniques to develop a fast, secure and lightweight image cryptographic algorithm by seeking the demand of IoT enabled devices in near future.

Gupta, M., Gupta, K.K. et al. (2020) described the session key based fast, secure and lightweight image encryption algorithm, where single point crossover operator, two point crossover operator and uniform mutation operator is used to generate a secure and unique session key, used for encryption and decryption. Also crossover operator is used in encryption phase to increase the confusion and diffusion for the intruders. Also the code size (In MATLAB) for developing this scheme is below 500, that shows that proposed scheme is light weight in nature. Encryption time

of this work is also very less that shows the proposed algorithm is fast. Since for each image encryption, a new unique session key is developed that shows the proposed scheme is secure.

Usman, M., Ahmed, I. et al (2017) described the lightweight encryption algorithm for Internet of Things. In this work, a novel approach (named as SIT) is proposed, which is based on 64-bit block cipher and requires 64-bit key to encrypt and decrypt the required data. This work uses the hybrid concept of feistal structure and substitution-permutation network. Also this work focuses on the hardware implementation of the proposed scheme in different IoT units.

Stalin, S., Maheshwary, P et al (2019) described the fast and secure medical image cryptographic system based on 4-dimentional chaotic map and DNA sequences. In this work, key sequences and pixel substitution is performed using 4-D chaotic map and in encryption phase, DNA sequences are used for encrypting different blocks.

Samhita, P., Prasad, P. et al (2016) described the novel image encryption technique based on the operators of genetic algorithm, named as crossover and mutation operator. This work also uses the hybrid concept of logistic chaotic map along with crossover and mutation operator. The proposed scheme in this work is based on three steps, where in the first step; the initial population is generated with logistic chaotic map. In second step, a four point crossover operator is used between two adjacent bytes. Finally in last step, mutation operator is used within one byte.

Wang, X., Feng, L. et al (2019) described a novel fast image encryption algorithm based on a new logistic-dynamic Arnold coupled logistic map lattice model, which is used to generate key sequence for increasing confusion and diffusion. By seeking the experimental results, we can analyze that the proposed algorithm is highly secure and efficient one.

Premkumar, R. et al (2019) described the novel 3-D chaos based image encryption using crossover and mutation operator. In this work, multipoint crossover operator is used. Here key is generated by using 3-D compound sine and ICMIC map. Also hybrid operators are used in encryption phase. Proposed scheme is tested on various evaluation parameters.

Talhaoui, M. Z., Wang, X et al (2020) described the fast image encryption technique based on the Bülban chaotic map. Most of the image encryption techniques achieved high level security, but due to slow speed and their complex procedure there techniques are not suitable for real time applications. In this scheme, circular shift of rows and columns are used to break the correlation between adjacent pixels. This technique uses simple chaotic map to generate only few number of random rows and columns.

Vidhya, R. et al (2020) described the novel image encryption scheme based on secure dynamic decision based permutation and BNT (butterfly network topology) based diffusion model. Here BNT model is used because its takes less time. Both models are used to create initial vector of Henon map which in turn used to create random key sequence for every encryption. Experimental results show that the proposed scheme is secured from different kinds of attacks.

Arpacı, B., Kurt, E. et al (2020) described the colored image encryption technique using bit-level scrambling based on hyper-chaotic map. This scheme uses modified chua's circuit (MCC) for the generation of chaotic number. The proposed scheme was tested on various parameters, different kinds of attacks and shows that proposed scheme performance is better than existing schemes.

Banu S, A. et al (2020) described the robust image encryption scheme based on the combination of IWT (Integer wavelet transform), DNA (Deoxyribonucleic acid) scheme for medical images. To generate random keys, this scheme uses a chaotic 3D Lorenz attractor and logistic map. Experimental results show that the efficiency of proposed scheme.

Jeevitha, S. et al (2020) described the novel image encryption algorithm based on DWT block scrambling algorithm for medical image processing. This scheme works in three different stages; first one is DWT-plane decomposition, second one is generation of edge map sequences, and the last one is DWT-level scrambling. This proposed scheme is tested on various parameters and attacks.

Zhang, L. et al (2020) described the image encryption algorithm based on bit planes and chaos. In this scheme, multiple images (k) are decomposed into 8k bit planes.

After that, Chen chaotic system and 2-D logistic map is used to scramble pixel positions. These scrambling are done on different bit planes and finally obtained multiple encrypted images. This proposed scheme is also tested on different parameters and attacks.

Table 1: Comparative chart between existing techniques on various parameters

Existing Techniques	NPCR	Entropy	Horr. Correlation	Vertical Correlation	Diagonal Correlation
Ref [1]	99.64	7.9969	0.0035	0.0050	-
Ref [2]	-	7.9973	-	-	-
Ref [3]	99.64	7.9975	0.0052	0.0031	0.0019
Ref [4]	99.5926	7.9953	-0.0112	-0.0280	0.0018
Ref [5]	99.6009	7.9993	0.0027	0.0003	0.0012
Ref [6]	99.7453	7.924	-0.0002	0.0001	-0.0015
Ref [7]	99.6306	7.9994	0.0039	0.0059	-0.0050
Ref [8]	99.64	7.9994	0.00012	0.00011	0.00178
Ref [12]	99.57	7.9992	0.0046	-0.0040	0.0008

SIT: A Lightweight Encryption Algorithm for Secure

3. CONCLUSION

This work demonstrates the latest image encryption algorithm based on chaotic map, genetic operations, and other novel techniques. By using this work, researchers can give a brief overview of latest work held in image encryption algorithms. Also various parameters like NPCR, UACI, horizontal, vertical and diagonal correlation, information entropy etc are used to check the performance of latest image encryption schemes. These encryption schemes are also tested on different kind of attacks.

REFERENCES

1. Gupta, M., Gupta, K.K. & Shukla, P.K. Session key based fast, secure and lightweight image encryption algorithm". Multimed Tools Appl, 2020.
2. Usman, M., Ahmed, I., Aslam, M., Khan S. and Shah, U., Internet of Things. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 1, 2017.
3. Stalin, S., Maheshwary, P., Shukla, P., Maheshwari, M., Gour, B. and khare, A., Fast and Secure Medical Image Encryption Based on Non Linear 4D Logistic Map and DNA Sequences (NL4DLM_DNA). Journal of medical system(Springer), July 2019.
4. Samhita, P., Prasad, P., Patro, K. and Acharya, B., A Secure Chaos-based Image Encryption and Decryption Using Crossover and Mutation Operator. I J C T A, 9(34) 2016, pp. 17-28.
5. Wang, X., Feng, L., Li, R., Zhang, F.: A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model. Nonlinear Dyn. 1–28, (2019).
6. Premkumar, R. and Anand, S., Secured and compound 3-D chaos image encryption using hybrid mutation and

crossover operator. Multimedia Tools and Applications, Volume 78 Issue 8, Pages 9577-9593, April 2019.

7. Talhaoui, M. Z., Wang, X., Midoun, M.A.: Fast image encryption algorithm with high security level using the Bülban chaotic map. Journal of Real-Time Image Processing (2020), https://doi.org/10.1007/s11554-020-00948-1.
8. Vidhya, R., Brindha, M. A novel dynamic chaotic image encryption using butterfly network topology based diffusion and decision based permutation. Multimed Tools Appl 79, 30281–30310 (2020). https://doi.org/10.1007/s11042-020-09462-9.
9. Arpacı, B., Kurt, E., Çelik, K. et al. Colored Image Encryption and Decryption with a New Algorithm and a Hyperchaotic Electrical Circuit. J. Electr. Eng. Technol. 15, 1413–1429 (2020). https://doi.org/10.1007/s42835-020-00393-x.
10. Banu S, A., Amirtharajan, R. A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach. Med Biol Eng Comput 58, 1445–1458 (2020). https://doi.org/10.1007/s11517-020-02178-w.
11. Jeevitha, S., Amutha Prabha, N. Novel medical image encryption using DWT block-based scrambling and edge maps. J Ambient Intell Human Comput (2020). https://doi.org/10.1007/s12652-020-02399-9.
12. Zhang, L., Zhang, X. Multiple-image encryption algorithm based on bit planes and chaos. Multimed Tools Appl 79, 20753–20771S (2020). https://doi.org/10.1007/s11042-020-08835-4.