Advances in Engineering Research, volume 86
2nd International Conference on Electrical, Automation and Mechanical Engineering (EAME 2017)

Chaotic Image Encryption Schemes: A Review

Chunhu Li*, Guangchun Luo, Ke Qin and Chunbao Li
School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan, 610054, P.R.C
*Corresponding author

***Abstract*—Image encryption has been a popular research field in recent decades. Chaotic encryption is one of the best alternative ways to ensure security. Many image encryption schemes using chaotic maps have been proposed, because of its extreme sensitivity to initial conditions, unpredictability and random like behaviors. This paper presents a comprehensive survey on chaotic image encryption schemes.**

Keywords-chaotic algorithms; cryptography; image encryption; chaotic maps

I. INTRODUCTION

In 1970s, Chaos theory was proposed, which was used in a number of research areas, such as mathematics, engineering, physics, biology, and so on [1]. The complex behavior of chaotic systems in nonlinear deterministic was described. The first description of a chaotic process was made in 1963 by Lorenz [2], who developed a system called the Lorenz attractor that coupled nonlinear differential equations.

The implementation of chaotic maps in the development of cryptography systems lies in the fact that a chaotic map is characterized by: (a) the initial conditions and control parameters with high sensitivity, (b) unpredictability of the orbital evolution, (c) the simplicity of the hardware and software implementation leads to a high encryption rate. These characteristics can be connected with some very important cryptographic properties such as confusion and diffusion, balance and avalanche properties [3].

Ever since the first chaos based image encryption scheme was introduced by Matthews [4], many chaos-based digital image encryption schemes utilizing chaotic maps have been proposed in the literature. The chaotic encryption has become a hot research topic in recent years. Over the past two decades, researchers have proposed many image encryption schemes. Chaos and cryptography have some common features, the most prominent being sensitivity to variables' and parameters' changes. Shannon in his seminal paper [5] wrote: "In a good mixing transformation functions are complicated, involving all variables in a sensitive way. A small variation of any one (variable) changes (the outputs) considerably."

In the last two decades, a growing number of chaos-based cipher systems have been suggested for use in cryptographic applications. In this paper, we deeply analyze chaotic image encryption schemes.

II. CHAOTIC IMAGE ENCRYPTION SCHEMES

In this section, a few newly proposed techniques for image encryption, based on chaotic schemes which will improve the complexity of algorithm as well as make the key stronger has been introduced.

Robert A. J. Matthews in [4] considered the use of genetic algorithms (GAs) as powerful tools in the breaking of cryptographic systems. They showed that GAs can greatly facilitate cryptanalysis by efficiently searching large key spaces, and demonstrate their use with GENALYST, an order-based GA for breaking a classic cryptographic system.

In [6], Ali Kanso exported the self-shrinking technique used in classical cryptography into chaotic systems to develop chaotic key stream generators capable of generating key streams featuring very good statistical properties, and possessing high level of security. This paper proposes a sample self-shrinking chaos-based key stream generator implemented using a 1-D chaotic tent map. Randomness properties and results of statistical testing of key stream bits generated by applying the self-shrinking technique on chaotic maps with suitable parameters are found encouraging.

Pareek, N. K., Patidar, V. and Sud, K. K.[7] have proposed a new approach for image encryption based on chaotic logistic maps in order to meet the requirements of the secure image transfer. In the proposed image encryption scheme, an external secret key of 80-bit and two chaotic logistic maps are employed. The initial conditions for the both logistic maps are derived using the external secret key by providing different weight age to all its bits.

In [8], a novel image encryption algorithm based on the Jacobian elliptic maps has been studied by Behnia, S., Akhavan, A., Akhshani, A., and Samsudin. In this paper, a new design of a class of chaotic cryptosystems is suggested to overcome the aforementioned drawbacks. This work is the first attempt, to explore the Jacobian elliptic maps as a cryptosystem. Experimental results and security analysis indicate that, the encryption algorithm based on the elliptic chaotic map is advantageous from the point of view of large key space and high level of security.

Omid Mirzaei, Mahdi Yaghoobi and Hassan Irani [9] have researched on a new image encryption scheme, based on a total shuffling and parallel encryption algorithm. Two chaotic systems have been used in the encryption algorithm to confuse the relationship between the plain-image and the cipher-image.

Guanrong Chen, Yaobin Mao and Charles K. Chui[10] have designed a real-time secure symmetric image encryption scheme based on 3D chaotic cat maps. the two-dimensional chaotic cat map is generalized to 3D for designing a real-time secure symmetric encryption scheme. In this paper, the well-

known two-dimensional chaotic cat map has been generalized to three-dimensional, and then used to design a fast and secure symmetric image encryption scheme. This new scheme employs the 3D cat map to shuffle the positions (and, if desired, grey values as well) of image pixels and uses another chaotic map to confuse the relationship between cipher-image and plain-image, thereby significantly increasing its resistance to various attacks such as the statistical and differential attacks. Thorough experimental tests have been carried out with detailed numerical analysis, demonstrating the high security and fast speed of the new image encryption scheme. This scheme is particularly suitable for real-time Internet image encryption and transmission applications.

Xingyuan Wang and Jianfeng Zhao in [11] have done their research work on the chaotic encryption, an enhanced key agreement protocol based on Chebyshev chaotic maps, and a public key cryptographic algorithm is utilized. The proposed key agreement protocol overcomes many drawbacks of the previous key agreement protocols based on chaos, so the security is enhanced effectively.

Junxin Chen, Zhiliang Zhu, Chong Fu, Libo Zhang and Yushu Zhang in [12] proposed an efficient image encryption scheme using lookup table-based confusion and diffusion. In comparison with the traditional chaos-based block ciphers, much less chaotic map iteration and no quantification operation are required in the proposed algorithm. Hence, the scheme has higher operation efficiency and fast encryption speed.

In [13], Akhavan Amir and his copartners studied an implementation of image encryption scheme based on the quantum chaotic map. The aim of this paper is to evaluate that the quantum logistic map can be used in cryptography. This algorithm exploits the interesting properties of three-dimensional quantum logistic map. The logistic map is an important special case in the limit of strong dissipation. By coupling the quantum kicked to a reservoir of harmonic oscillators, dissipative quantum logistic map was constructed by Goggin et al. Considering very lowest-order quantum corrections, the quantum logistic maps is proposed in three-dimensional form. Though chaotic orbits of discrete-time maps are non-periodic in nature, because of finite precision of digital computers the orbits actually turn out to be periodic. So that, the average period of an orbit of a three-dimensional map can be expected to be longer than that of a one dimensional map.

Guodong Ye, Haiqing Zhao and Huajin Chai proposed an efficient and secure image encryption algorithm in [14] using SHA-3 hash function together with double two-dimensional Arnold chaotic maps. Classical encryption architecture, i.e., permutation plus diffusion, is employed in this scheme. To avoid time consumption of sorting operation for pixel position index in permutation stage, a novel wave-line-based confusion is suggested with four random directions of shuffling. The key stream generated by Arnold map is used for vertical and horizontal circular confusions, respectively, in which the initial conditions are updated by the SHA-3 hash values of chaotic matrix and a new vector produced from the plain-image. As a result, the proposed scheme can resist the known-plaintext attack compared with some existing encryption methods. Furthermore, in diffusion stage, a blocking method is designed with the outputs of hash values in the former block permuted image which are used to update again the initial conditions for Arnold map. The current block will influence the next block during the iterations, of which can resist well the chosen-plaintext attack.

Xingyuan Wang and Dahai Xu [15] researchers have explained a new "Selection–Crossover–Mutation" architecture which is based on the modern cryptography from the aspect of genetic mechanisms, mainly draws on the design of the genetic operators. The intertwining logistic map has been used to generate the chaotic sequences owing to its advantages. They take each pixel as an "individual," each bit of it as a gene, first, the "Selection" phrase, use Monte Carlo method to randomly select two individuals according to the chaotic sequences, cross them, swap their genes using the specified crossover operator in the second phrase, and then finally, change the genes of the individuals randomly for the mutation phrase.

III. CONCLUSIONS

Nowadays, it is very important to provide a secret image. In this paper, many of the current important image encryption techniques have been presented and analyzed. In short, all chaotic techniques are useful for image encryption and each chaotic technique is unique in its own way, which may be suitable as an image of secret data. Nowadays, image encryption technique is developing very fast, it needs to continue to propose a new encryption algorithm. These methods are future extended for encryption and compression during the image transmission and the image storage.

ACKNOWLEDGMENT

This work is supported by the foundation of science and technology department of Sichuan province NO.2015SZ0231.

REFERENCES

[1] Schneier B. Applied cryptography. In: Protocol, algorithms and source code. New York: Wiley; 1996.

[2] E. N. Lorenz, "Deterministic nonperiodic flow," Journal of the atmospheric sciences, vol. 20, no. 2, pp. 130–141, 1963.

[3] S. Bruce, "Applied cryptography: protocols, algorithms, and source code in c," John Wiley & Sons, Inc., New York, 1996.

[4] R. A. Matthews, "The use of genetic algorithms in cryptanalysis," Cryptologia, vol. 17, no. 2, pp. 187–201, 1993.

[5] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 28, pp. 656–715, 1949.

[6] A. Kanso, "Self-shrinking chaotic stream ciphers," Communications in nonlinear science and numerical simulation, vol. 16, no. 2, pp. 822–836, 2011.

[7] Pareek, N. K., Patidar, V., & Sud, K. K. (2006). Image encryption using chaotic logistic map. Image & Vision Computing, 24(9), 926-934.

[8] Behnia, S., Akhavan, A., Akhshani, A., & Samsudin, A. (2013). Image encryption based on the jacobian elliptic maps. Journal of Systems & Software, 86(86), 2429-2438.

[9] Mirzaei, O., Yaghoobi, M., & Irani, H. (2012). A new image encryption method: parallel sub-image encryption with hyper chaos. Nonlinear Dynamics, 67(1), 557-566.

[10] Chen, G., Mao, Y., & Chui, C. K. (2004). A symmetric image encryption scheme based on 3d chaotic cat maps. Chaos Solitons & Fractals, 21(3), 749-761.

[11] Wang, X., & Zhao, J. (2010). An improved key agreement protocol based on chaos. Communications in Nonlinear Science & Numerical Simulation, 15(12), 4052-4057.

[12] Chen, J. X., Zhu, Z. L., Fu, C., Zhang, L. B., & Zhang, Y. (2015). An efficient image encryption scheme using lookup table-based confusion and diffusion. Nonlinear Dynamics, 81(3), 1151-1166.

[13] Akhshani, A., Akhavan, A., Lim, S. C., & Hassan, Z. (2012). An image encryption scheme based on quantum logistic map. Communications in Nonlinear Science & Numerical Simulation, 17(12), 4653-4661.

[14] Ye, G., Zhao, H., & Chai, H. (2015). Chaotic image encryption algorithm using wave-line permutation and block diffusion. Nonlinear Dynamics, 83(4), 1-11.

[15] Wang, X., & Xu, D. (2014). Image encryption using genetic operators and intertwining logistic map. Nonlinear Dynamics, 78(4), 2975-2984.