Survey and Analysis of Chaotic Image Encryption Schemes

Amitesh Singh Rajput
School of Information Technology,
Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, M.P.
amiteshrajput@gmail.com

Vivek Sharma
School of Information Technology,
Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, M.P.
vivek.rgpv@gmail.com

Abstract – Digital images play an important role in our daily lives and are used in many applications. Hence, there is a need to protect them from unauthorized access and modification. During the past years, several image encryption algorithms have been proposed. Image encryption techniques jumble the pixels of the plain image and reduce the association among the pixels, such that any adversary cannot modify the encrypted image. Chaotic encryption method seems to be much better day by day. The chaos based cryptographic algorithms are one of the emerging and efficient ways to develop secure image encryption techniques. Several schemes have been proposed and analyzed in the past decade based on chaotic maps. Chaotic maps require initial conditions to start iterations and usually initial conditions are derived using the external secret key by providing different weightage to all its bits. A comparative analysis and behavior of the chaotic image encryption schemes proposed in the past decade is presented in this paper such that further enhances in the field of image security can be explored.

Keywords: Chaotic, Cryptographic, Pixels

I. Introduction

Transmission of digital images through internet has been increasing in recent years. Many applications require reliable, fast, and robust security system to store and transmit digital images. Due to special characteristics of digital images like data redundancy and strong correlation between adjacent pixels, it is difficult for traditional ciphers like IDEA, AES, DES and RSA to deal with real-time digital image encryption as they require high computational power. To achieve good combination of speed and high security, chaotic encryption techniques are preferred compared to other methods. Chaotic systems have certain essential properties such as randomness, sensitivity to initial condition, and ergodicity. A tiny difference in initial values or system parameters leads a major change in the generated chaotic sequences. A chaotic state variable goes through all states in its phase space; these states are usually distributed uniformly. These properties of chaotic systems make them a good candidate for cryptography [8, 9]. During the past years, several image encryption schemes have been proposed based on chaotic maps.

Congxu Zhu et. Al. [1] proposed a new scheme based on the Logistic-Sine map (LSM) chaotic system. Another scheme proposed by Himan Khanzadi et. Al. [2] consists of an algorithm for image encryption using the random bit sequence generator based on chaotic maps. In [3], Adrian-Viorel Diaconu et. Al. [3], presented a scheme to a newly designed image cryptosystem that uses the Rubik's cube principle in conjunction with a digital chaotic cipher. Tiegang Gao et. Al. [4], uses hyper chaos to encrypt the image and the scheme is cryptanalyzed by [7]. In [5], Guodong Ye et. Al. proposed an efficient image encryption algorithm using the generalized Arnold map. Along with encryption, authentication mechanisms are also included and a fast image encryption and authentication scheme is proposed by Huaqian Yang et. Al. [6]. The rest of the paper is organized as follows: section II describes the literature survey of some of the schemes proposed in the past decade. In section III, comparative analysis of the schemes discussed in the previous section is shown in a tabular manner. Finally section IV concludes the paper.

DOI-10.18486/ijcsnt .2015.4.1.04
ISSN-2053-6283

II. Literature Survey

In recent years, a variety of chaos-based image cryptosystems have been proposed. Usually, plain image dependent key is used for encryption/decryption. To achieve a satisfactory level of security, at least two rounds of the substitution-diffusion process are required so that a change in any pixels of the plain-image spreads over the whole cipher-image.

A. A Novel Image Encryption Scheme based on the LSM Chaotic System

Congxu Zhu, Yuping Hu and Xinran Zhou [1], proposed a new scheme based on the Logistic-Sine map (LSM) chaotic system. The LSM is introduced by combing the Logistic map (LM) and Sin map (SM). It is presented in the paper that the chaotic range of LSM is much larger than that of the Logistic or Tent maps and complexity characteristics of Logistic map, Sine map and Logistic-Sine map are analyzed based on C0 algorithm. A novel image encryption scheme based based on the LSM chaotic system is proposed by [1]. Initially, the image picel positions are shuffled through swapping the positions randomly by using chaotic values. The plaintext feedback technique is used to relate permutation sequences with plain-images. Then, round dependent diffusion procedure with LSM is introduced to diffuse the image, which is composed of two rounds. The experimental results and analysis shows that the proposed scheme has fine capability to resist brute-force attacks, statistical analysis attacks and differential attacks and can be used for secure image communications.

B. Image Encryption Using Random Bit Sequence Based on Chaotic Maps

Himan Khanzadi, Mohammad Eshghi and Shahram Etemadi Borujeni [2], proposed an algorithm for image encryption using the random bit sequence generator based on chaotic maps. To generate random bit sequence, chaotic logistic and tent maps are used and pixels of the plain image are permuted using these chaotic functions. The image is partitioned into eight bit map planes and in each plane, bits are permuted and substituted according to random bit and random number matrices. Based on the chaotic random Ergodic matrix, the pixels and bit maps permutation are evaluated. Performance of the scheme is evaluated using chi-square test, correlation coefficient, number of pixel of change rate (NPCR), unified average changing intensity (UACI), and key space. The histogram of encrypted image is approximated by a uniform distribution with low chi-square factor. Experimental results and analysis shows that the scheme exhibits good properties to resist attacks. Total key space is 2∧2,160, which is large enough to resist any bruteforce attack.

C. An Improved Secure Image Encryption Algorithm Based on Rubik's Cube Principle and Digital Chaotic Cipher

Adrian-Viorel Diaconu and Khaled Loukhaoukha [3], presented a scheme to a newly designed image cryptosystem that uses the Rubik's cube principle in conjunction with a digital chaotic cipher. The original image is shuffled on Rubik's cube principle and then rows and columns of the scrambled image are XORed using a chaos-based cipher. For shuffling and ciphering procedures, different keys are used and each row and column's inherent properties were used to compute the number of circular shifts. Experimental results and analysis show that the proposed image encryption scheme achieves good encryption and can resist any cryptanalytic attacks.

D. A new Image Encryption Algorithm based on Hyper Chaos, 2008

In [4] Tiegang Gao *et al*, proposed a scheme using hyper chaos to encrypt the image, which consists of two parts. In the first part, total shuffling of the image pixels take place whereas in the second part, encryption of the shuffled image takes place using the hyper chaos. To change the gray values of the image pixels, hyper chaos is used. First part contains the row transformation based on the logistic map using which, the rows of the plain image are shuffled. Then column transformation takes place which is also dependent on the logistic map in which columns of the row-transformed image are then further shuffled. After the shuffling phase, the image pixels are dispersed randomly and hence the image becomes encrypted but the histogram of the shuffled image remains same as that of the histogram of the plain image. Hence, hyper chaotic system is used for further encryption of the image. The algorithm is described in Fig 1.

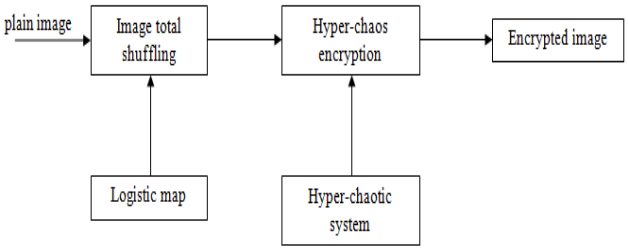

Fig.1. Encryption Algorithm proposed by [4]

DOI-10.18486/ijcsnt .2015.4.1.04
ISSN-2053-6283

Cryptanalysis of the above scheme [4] is presented by Rhouma Rhouma and Safya Belghith [7]. According to Rhouma Rhouma and Safya Belghith, three couples of plaintext/cipher text were enough to break the cryptosystem in a chosen cipher text and chosen plaintext attacks scenarios.

E. An efficient chaotic image encryption algorithm based on a generalized Arnold map

Guodong Ye and Kwok-WoWong [5], proposed an efficient image encryption algorithm using the generalized Arnold map. The conventional confusion-diffusion architecture is adopted, in which the keystream used depends on the plain-image. Two stages, i.e., permutation and diffusion are composed in the algorithm. To substantially reduce the correlation between adjacent pixels, a total circular function rather than the traditional periodic position permutation is used in the permutation stage. Whereas, double diffusion functions like positive and opposite module are utilized with a novel generation of the keystream in the diffusion. Experimental result and analysis show that the scheme can resist known- and chosen-plaintext attacks. In future, the scheme can be extended to adopt other chaotic systems by simply changing the generation of the chaotic sequences in the confusion stage. As mentioned by the authors, the scheme can also adopt high-dimensional chaotic systems such as Chen's system, spatial chaotic system, and 3D cat map. The system also tried to encrypt during attacks from other sources.

F. A fast image encryption and authentication scheme based on chaotic maps

Proposed by Huaqian Yang, Kwok-Wo Wong, Xiaofeng Liao, Wei Zhang and Pengcheng Wei [6]. Along with encryption, authentication mechanisms are also included and a fast image encryption and authentication scheme is proposed. A keyed hash function is introduced to generate a 128-bit hash value from both the plain-image and the secret hash keys. The hash value acts the role of key for encryption and decryption while the secret hash keys are used to authenticate the decrypted image. Plain-image pixels are permuted using a modified standard map. Permutation and diffusion processes are performed simultaneously in a single scan of plain-image pixels and the value is altered while relocating a pixel. Experimental results and analysis show that satisfactory security performance is achieved in only one overall round and the speed efficiency is also improved.

III. Comparison and Analysis

The schemes discussed in the previous section are compared and analyzed here in this section. The security of image encryption schemes can be determined by some tests. These tests include key space tests, statistical tests and differential tests. We have considered only those tests in which plain image 'lena' is used such that uniformity for comparison can be achieved. Based on the test parameters, table 1 below shows the comparison between various schemes discussed in the previous section.

Table 1: Comparison of schemes presented in the previous section

S. No.	Parameter	[1]	[2]	[3]	[4]	[5]	[6]
1	Histogram distribution	Fairly Uniform	Fairly Uniform	Fairly Uniform	Fairly Uniform	Fairly Uniform	Fairly Uniform
2	Key Space	2^{212}	2^{2160}	2^{192}	10^{70}	-	2^{128}
3	Correlation of adjacent pixels (Horizontal)	0.0005	0.0005	0.0006	-0.0142	0.0770	-0.0020
	Vertical	-0.0019	0.0041	0.0002	-0.0074	-0.07236	-0.0161
	Diagonal	0.0005	0.0048	0.0043	-0.0183	-0.06153	0.0178
4	NPCR	99.5987	99.6100	99.6120	-	99.9200	99.6185
5	UACI	33.3087	33.3500	30.5997	-	34.7500	33.4795

It can be analyzed from table 1 that the schemes exhibit good properties to resist different attacks. Some schemes [1] and [3] possess good properties to resist statistical attacks as their correlation values are very close to zero as compared to other ones. Whereas on the other side, other schemes [2], [5] and [6] have good resistance to differential attacks. Scheme [4] possesses weak statistical properties and cryptanalysis of the scheme is presented by [7]. Thoughtfully, all the schemes possess reasonable properties to and can be improved in future such that further enhances in the field of image security can be advanced.

IV. Conclusion

As we know that images play an important role in our daily lives and securing them is very important. Chaotic maps are involving day-by-day and provide good reason to be used for image cryptography. Survey and comparative analysis of the chaotic image encryption schemes proposed in the past decade is presented in this paper such that further advances in the field of image security can be enhanced.

References

[1] Congxu Zhu, Yuping Hu and Xinran Zhou, A Novel Image Encryption Scheme based on the LSM Chaotic System, International Journal of Security and Its Applications Vol.8, No.6 (2014), pp.61-70.

[2] H. Khanzadi, M. Eshghi and S.E. Borujeni, Image encryption using random bit sequence based on chaotic maps, Arabian Journal for Science and engineering , vol. 39, no. 2, pp. 1039-1047, 2014.

[3] A. Diaconu and K. Loukhaoukha, "An improved secure image encryption algorithmbased on Rubik's cube principle and digital Chaotic Cipher,"Mathematical Problems in Engineering, vol. 2013, Article ID 848392, 10 pages, 2013.

[4] Tiegang Gao, Zengqiang Chen, "A new image encryption algorithm based on hyper-chaos", Physics Letters A 372 (2008) 394–400.

[5] G. Ye and K.W. Wong, "An efficient chaotic image encryption algorithm based on a generalized Arnold map", Nonlinear Dynamics, Springer, (2012), pp. 2079-2087.

[6] H. Yang, K.-W. Wong, X. Liao, W. Zhang, P. Wei, Communications in Nonlinear Science and Numerical Simulation 15 (2010) 3507.

[7] Rhouma Rhouma, Safya Belghith, "Cryptanalysis of a new image encryption algorithm based on hyper-chaos", Physics Letters A 372 (2008) 5973–5978.

[8] Schneier B. "Applied cryptography: protocols algorithms and source code in C". New York (USA): Wiley; 1996.

[9] Menezes AJ, Oorschot PCV, Vanstone SA. "Handbook of applied cryptography". Boca Raton (FL): CRC Press; 1997.

[10] Matthew R (1989) "On the derivation of a chaotic encryption algorithm." Cryptologia 8(1):29–42.

[11] Alligood, K.T., Sauer, T.D., Yorke, J.A., "Chaos: An introduction to Dynamical Systems" Textbooks in Mathematical Sciences, Springer, New York (1997).

[12] S.S. Bedi, ShekharVerma & G.S. Tomar, "An Adaptive Data Hiding Technique for Digital Image Authentication", International Journal of Computer Theory and Engineering, Vol. 2, No. 3, pp 338-344, June, 2010.

[13] Borujeni, S.E, Eshghi,M. "Chaotic image encryption design using tompkins-paige algorithm" Hindawi Publishing Corporation, Mathematical Problem in Engineering vol. 200, p. 22 (2009).

Amitesh Singh Rajput received Bachelor of Engineering degree in Information Technology from Rajiv Gandhi Proudyogiki Vishwavidyalaya in 2010 and Master of Technology degree in Information Technology from Rajiv Gandhi Proudyogiki Vishwavidyalaya in 2014. He is currently working as Assistant Professor in School of Information Technology, University Teaching Department, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India. His recent research interests include Image processing, Cryptography and Cloud Computing.

Vivek Sharma received Bachelor of Engineering degree in Electronics & Communications from Rajiv Gandhi Proudyogiki Vishwavidyalaya in 2003 and Master of Technology degree in Computer Science & Engineering from Barkatullah University in 2011. He is currently working as Assistant Professor in School of Information Technology, University Teaching Department, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India. His recent research interests include Image processing, Mobile Ad-hoc Network and Mobile Computing.