Survey: Image Encryption using Chaotic Cryptography Schemes

Mintu Philip
Department of Computer Science
Toc H Institute of Science and Technology
Kochi, Kerala, India

Asha Das
Department of Computer Science
Toc H Institute of Science and Technology
Kochi, Kerala, India

ABSTRACT
Chaotic Encryption Method seems to be much better than traditional encryption methods used today. Chaotic encryption is the new direction of cryptography. It makes use of chaotic system properties such as sensitive to initial condition and loss of information. Many chaos-based encryption methods have been presented and discussed in the last two decades. In order to reach higher performance, these methods take advantage of the more and more complex behavior of chaotic signals. This paper contributes by comparing and analyzing the performance of the past chaotic image encryption schemes.

General Terms
Security, cryptography, Encryption Algorithms et. al.

Keywords
Chaotic algorithm, logistic map, perturbation, Baker map, cipher

1. INTRODUCTION
Cryptography is the science of protecting the privacy of information during communication under hostile conditions. In the present era of information technology and proliferating computer network communications, cryptography assumes special importance. Cryptography is now routinely used to protect data, which must be communicated and/or saved over long periods, to protect electronic fund transfers and classified communications.

Current cryptographic techniques are based on number theoretic or algebraic concepts. Chaos is another paradigm, which seems promising. Chaos is an offshoot from the field of nonlinear dynamics and has been widely studied. A large number of applications in real systems, both man-made and natural, are being investigated using this novel approach of nonlinear dynamics. The chaotic behavior is a subtle behavior of a nonlinear system, which apparently looks random. However, this randomness has no stochastic origin. It is purely resulting from the defining deterministic processes. The important characteristics of chaos are its extreme sensitivity to initial conditions of the system.

2. CHAOTIC IMAGE ENCRYPTION
The chaotic image encryption can be developed by using properties of chaos including deterministic dynamics, unpredictable behavior and non-linear transform. This concept leads to techniques that can simultaneously provide security functions and an overall visual check, which might be suitable in some applications. Digital images are widely used in various applications, that include military, legal and medical systems and these applications need to control access to images and provide the means to verify integrity of images.

3. BLOCK ENCRYPTION
Block encryption is an encryption scheme in which the clear text is broken up into blocks of fixed length, and encrypted one block at a time. This section gives a brief review on past block encryption schemes.

Goce Jakimoski and Ljupˇ co Kocarev proposed a block encryption [1] that uses a systematic procedure to create chaos based ciphers. Two well-known chaotic maps, exponential and logistic, defined on the unit interval by $x \rightarrow \alpha^x \bmod 1$ and $x \rightarrow 4x(1-x)$, respectively, are used for this purpose.

Yaobin mao, Guanrong Chen and Shiguo Lian proposed an algorithm [2] in which the two-dimensional baker map is extended to be three-dimensional and is then used to compose a fast and secure image encryption scheme.

Haojiang Gao, Yisheng Zhang, Shuyun Liang, Dequn Li presents a new nonlinear chaotic algorithm (NCA) [3] which uses power function and tangent function instead of linear function. Its structural parameters are obtained by experimental analysis. And an image encryption algorithm in a one-time-one-password system is designed.

Su Su Maung, and Myitnt Myint Sein proposed a fast encryption scheme [4] based on chaotic maps is proposed. Firstly the dynamical 8×8 S-box is produced by using logistic map and 2D standard map. Secondly a sequence of pseudo-random bytes is generated by using 2D chaotic cat map to index the entries of the S-box. The output bytes from the S-box are XOR-ed with the plaintext to produce the cipher text.

Musheer Ahmad and M Shamsher Alam proposed an image encryption algorithm [5] based on three different chaotic maps. The plain image is first decomposed into 8x8 size blocks and then the block based shuffling of image is carried out using 2D Cat map. The shuffled image is encrypted using chaotic sequence generated by one dimensional logistic map.

Fengiian Wang, Yongping Zhang, Tianjie Cao presented an algorithm [6] that produces chaotic stream based on logistic map. The system parameter of logistic map is produced by m-sequence, and using another m-sequence's perturbation to increase the period of logistic mapping sequence. An output feedback mechanism is also provided in the system.

4. STREAM ENCRYPTION

Stream ciphers are based on generating an "infinite" cryptographic key stream, and using that to encrypt one bit or byte at a time.

Jui-Cheng and Jiun-In Guo proposed a paper on image encryption/decryption algorithm [7] and its VLSI architecture. According to a chaotic binary sequence, the gray level of each pixel is XORed or XNORed bit-by-bit to one of the two predetermined keys. Its features are as follows: (1) low computational complexity, (2) high security, and (3) no distortion.

The algorithm [8] proposed by Po-Han Lee, Soo-Chang Pei, and Yih-Yuh Chen uses a known chaotic dynamical system to generate a sequence of pseudo-random bytes, and then applies certain permutations to them, using the discretized version of another two-dimensional chaotic map.

Socek, D., Shujun Li, Magliveras, S.S. and Furht, B. enhanced the CKBA algorithm [9] three-fold: 1) we change the 1-D chaotic Logistic map to a piecewise linear chaotic map (PWLCM) to improve the balance property, 2) we increase the key size to 128 bits, and 3) we add two more cryptographic primitives and extend the scheme to operate on multiple rounds so that the chosen/known-plaintext attacks are no longer possible. The new cipher has much stronger security and its performance characteristics remain very good.

Deergha Rao and K. Gangadhar proposed an algorithm [10] to enhance the security of CKBA.

Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah proposed a stream cipher [11] is based on the use of a chaotic logistic map and an external secret key of 256-bit. Use of data-dependent iterations, data-dependent inputs, and the inclusion of three independent feedback mechanisms are additional features of the system.

Shubo Liu, Jing Sun, Zhengquan Xu proposed a novel image encryption algorithm [12] based on logistic map. The system consists of a key stream generator that generates the satisfied random number which is XOR-ed with the plaintext in binary format.

Abir Awad and Abdelhakim Saadane proposed piecewise linear chaotic map (PWLCM) perturbed by a new technique [13]. Both chaotic maps are then used to control three bit-permutation methods having good inherent cryptographic properties.

Ai-hongZhu and Lia Li presented a new algorithm [14] that produced nine chaotic sequences only by one secret-key, six sequences were used to scramble the position of image pixels, and the others were used to confuse and diffuse image pixels value.

5. BLOCK VS STREAM ENCRYPTION

Block encryption techniques [1-6] are slow compared to stream. More memory is required for block cipher, since they work on larger chunks of data and often have feedbacks from previous blocks, whereas since stream ciphers [7-14] work on only a few bits at a time they have relatively low memory requirements. Stream ciphers are prone to weaknesses and more difficult to implement correctly based on usage. Because block ciphers are more susceptible to noise in transmission since they encrypt a whole block at a time (and furthermore have "feedback" modes which are most recommended), that is if one part of the data is altered, all the rest is probably unrecoverable. Whereas with stream ciphers are bytes are individually encrypted with no connection to other chunks of data (in most ciphers/modes), and often have support for interruptions on the line. Also, stream ciphers do not provide integrity protection or authentication, whereas some block ciphers (depending on mode) can provide integrity protection, in addition to confidentiality.

Due to all these reasons, stream ciphers are usually best for cases where the amount of data is either unknown, or continuous - such as network streams. Block ciphers, on the other hand, or more useful when the amount of data is pre-known - such as a file, data fields, or request/response protocols, such as HTTP where the length of the total message is known already at the beginning.

6. PERFORMANCE ANALYSIS OF CHAOTIC IMAGE ENCRYPTION SCHEMES

Various parameters are recommended by researchers to evaluate the performance of chaotic cryptographic scheme used for image encryption. Goce Jakimoski and Ljupˇco Kocarev [1] suggested two parameters: simplicity and security. The cipher use only one byte operation that can be easily implemented on various processors and hardwares. S-Boxes are generated by chaotic maps and descretized procedures presented in this paper are more secure. There exists no more efficient attack to our ciphers than brute force.

Yaobin Mao, Guanrong Chen and Shiguo Lian [2] considered speed, resistance to various known attacks, key space and key sensitivity as performance parameters. The use of 3D Baker map speed up the image encryption process. It is resistant to following attacks: known plain text attack, cipher text only attack, differential and brute force attacks. It has larger key space, about 2^{128}. Key sensitivity is so high such that a one bit difference in key results in 99.59% difference in encrypted image.

Haojiang Gao, Yisheng Zhang, Shuyun Liang, Dequn Li [3] adviced speed, key space, key sensitivity, histogram, pixel correlation and resistance to known attacks as performance measures. The proposed algorithm achieved 0.5s speed, zero correlation, large key space and high key sensitivity. It is resistant to gray code, statistical and brute force attacks.

Su Su Maung, and Myitnt Myint Sein [4] suggested 3 parameters: confusion and diffusion properties, correlation coefficient and histogram. The algorithm achieved good confusion and diffusion properties and histogram of encrypted image are uniform and different from the original one. The correlation coefficient between source and cipher was found to be 0.00041818.

Musheer Ahmad and M Shamsher Alam [5] suggested balance property, key space, correlation coefficient and information entropy as performance parameters. The distribution of gray scale value of image has good balance property. Key space is about 10^{112}. Correlation coefficients are close to zero. Information entropy is close to ideal entropy, so leakage of information is negligible.

Wang, Yongping Zhang, Tianjie Cao [6] considered probability distribution, complexity and cipher sensitivity as performance measures. The probability distribution of cipher text is uniform and resistant to statistical attack. The cipher text has high non-linear mapping with the plain text which makes it more secure. The cipher is highly sensitive to plain text due to additional output feedback.

The algorithm [8] suffers from a drawback that is also inherent in most chaotic systems, namely, the distribution of the admissible random numbers as a function of the parameters involved exhibits a fractal structure, and thus cannot be foretold from one simple glance at the chosen values for the parameters. Issues such as this still remain to be answered.

Since ECKBA [9] introduces additional steps and uses a more complex map than CKBA [9], it is expected that the running time of the encryption/decryption algorithm increases. The precision of CKBA was kept at 16 bit, while that of ECKBA is 32 bits.

Modified chaotic-key based algorithm (MCKBA) [10] is proposed to enhance the chosen/known-plaintext attacks and cipher text-only attacks faced by CKBA.

ECBFSC [11] Simulation results show that the average encryption/decryption speed is 7.46 MB/Sec for encryption and 6.63 MB/Sec for decryption. The peak speed can reach up to 7.6 MB/Sec for encryption and 6.7 MB/Sec for decryption.

The paper proposed by Shubo Liu, Jing Sun, Zhengquan Xu Has [12] a key space size for initial conditions and control parameters is over than 2^{196}.The key stream output speed is up to 571.429 Mbps, which is strongly suitable for the use of most of real-time video and audio applications.

Reduction of correlation coefficients ranges from 64% to 91% with the PWLCM [13]. Ai-hong Zhu Lian Li proposes a new color image encryption algorithm [14] based on Logistic map. The operating time is about 0.125s for 256x256 image and 7.5s for 1944x2596.

7. CONCLUSION

In this paper various chaotic cryptography schemes are studied and their performance is evaluated on four criteria: key space, key sensitivity, correlation coefficient and speed. In this survey, already existing block based image encryption algorithms have been discussed later, encrypting the entire image bit by bit using a fast conventional cryptosystem were discussed.

Techniques which are based on chaotic systems are emphasized, because these systems will improve the security level of encryption algorithm by using properties of chaos including deterministic dynamics, unpredictable behavior and non-linear transform. Newly proposed image encryption techniques and also enhance the security level by introducing more than one chaotic scheme for image encryption algorithms. A new algorithm for encrypting color images was also analyzed.

8. REFERENCES

[1] Jakimoski, G. and L. Kocarev. 2001. "Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps". IEEE Transactions on Circuits and Systems—I: Fundamental Theory and Applications. 48(2): 163-169.

[2] Y.B. Mao, G. Chen, S.G. Lian, "A novel fast image Encryption scheme based on the 3D chaotic baker map," Int. J. Bifurcate Chaos, vol. 14, pp. 3613–3624, 2004.

[3] H. Gao, Y. Zhang, S. Liang, and D. Li, "A new chaotic algorithm for image encryption," Chaos, Solutions &Fractals, vol. 29, no. 2, pp. 393–399, 2006.

[4] Su Su Maung, and Myitnt Myint Sein, "A Fast Encryption Scheme Based on Chaotic Maps", GMSARN International Conference on Sustainable Development: Issues and Prospects for the GMS, 2008.

[5] Musheer Ahmad and M. Shamsher Alam, "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping", Musheer Ahmad et al /International Journal on Computer Science and Engineering, Vol.2(1), 2009, 46-50.

[6] Fengjian Wang, Yongping Zhang and Tianjie Cao "Research of chaotic block cipher algorithm based on Logistic map", 2009 Second International Conference on Intelligent Computation Technology and Automation, 2009**:** 678 – 681.

[7] Jui-Cheng Yen, and Jiun-In Guo, "A New Chaotic Key-Based Design for Image Encryption and Decryption", IEEE International Symposium on ISCAS 2000, Geneva, pp. IV-49-IV-52, May. 2000.

[8] Po-Han Lee,Soo-Chang Pei and Yih-Yuh Chen, "Generating Chaotic Stream Ciphers Using Chaotic Systems", Chinese Journal Of Physics Vol. 41 , No. 6, 2003.

[9] Socek, D., Shujun Li, Magliveras, S.S. and Furht, B, "Short Paper: Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption", First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005:406-407.

[10] Deergha Rao and K. Gangadhar, "Modified Chaotic Key-Based Algorithm for Image Encryption And Its VLSI Realization", International Conference on Digital Signal Processing, 2007.

[11] H.E.H. Ahmed, H.M. Kalash, and O.S.F. Allah, "An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC)

for Image Encryption and Decryption", presented at Informatica (Slovenia), 2007, pp.121-129.

[12] Shubo Liu, Jing Sun, Zhengquan Xu "An Improved Image Encryption Algorithm based on Chaotic System", journal of computers, vol. 4, no. 11, 2009, pp.1091-1100.

[13] Abir Awad, Abdelhakim Saadane, "Efficient Chaotic Permutations for Image Encryption Algorithms", Proceedings of the World Congress on Engineering Vol I, 2010.

[14] Ai-hongZhu, Lia Li, "Improving for Chaotic Image Encryption Algorithm Based on Logistic Map", 2nd Conference on Environmental Science and Information Application Technology, 2010.

[15] G. Chen, Y. Mao, C.K. Chui, "A symmetric image encryption based on 3D chaotic maps", Chaos Solutions Fractals, vol. 21, pp. 749–761, 2004.

[16] S. E. Borujeni, M. Eshghi1, "Chaotic Image Encryption Design Using Tompkins-Paige Algorithm", Hindawi Publishing Corporation, Mathematical Problems in Engineering, Article ID 762652, 22 pages, 2009.

[17] Mazleena Salleh, Subariah Ibrahim, Ismail Fauzi Isnin, "Image encryption algorithm based on chaotic mapping", Journal Teknologi, 2003, pp: 1–12.

[18] Shubo Liu, Jing Sun, Zhengquan Xu, "An Improved Image Encryption Algorithm based on chaotic system", Journal of Computers, vol. 4, no. 11, November 2009, pp: 1091-1100.

[19] Noura, H. El Assad, S. Vlădeanu, C, "Design of a fast and robust chaos-based crypto-system for image encryption", 8th International Conference on Communications (COMM), 2010, pp: 423 – 426.