ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 2, No 6, June 2013

Image encryption based on chaotic algorithms: An overview

Arun S Menon[1], Sarila K S[2]
[1] KVM College of Engineering and IT, Alappuzha, Kerala, India
[2]St.Mary's Training College, Kottayam, Kerala, India

Abstract— **In this review paper, we have discussed about image encryption based on chaotic algorithms. In recent years, a variety of effective chaos based image encryption schemes have been proposed. The typical structure of these schemes has the permutation and the diffusion stages performed alternatively. The confusion and diffusion effect is solely contributed by the permutation and the diffusion stage respectively. A number of image encryption algorithms based on chaotic maps have been proposed. Chaotic key based algorithm (CKBA) is based on a one dimensional logistic map. Enhanced chaotic key based algorithm for image encryption enhanced CKBA results by attaining a much higher security level.**

***Index Terms*—Image encryption, chaotic key based algorithm .**

I. INTRODUCTION

Nowadays, communication networks such as mobile networks and the internet are well developed. However they are public networks and are not suitable for the direct transmission of confidential messages. To make use of the communication networks already developed and to keep the secrecy simultaneously, cryptographic techniques need to be applied. Traditional symmetric ciphers such as data encryption standard (DES) are designed with good confusion and diffusion properties. These two properties can also be found in chaotic systems which are usually ergodic and are sensitive to system parameters and initial conditions. In recent years, a number of chaos based cryptographic schemes have been proposed. Some of them are based on one dimensional chaotic maps and are applied to data sequence or document encryption. For image encryption, two dimensional or higher dimensional chaotic maps are naturally employed as the image can be considered as a two dimensional array of pixels. A chaos based image encryption scheme should compose of two processes: chaotic confusion and pixel diffusion. The former permutes the pixels of a plain image with a 2D chaotic map while the latter alternates the value of each pixel in a sequential manner. This architecture formed the basis of a number of chaos based image ciphers proposed subsequently.

II. CHAOTIC KEY BASED ALGORITHM

A. Digital Chaotic Systems

There are many different understandings and implementations of chaotic systems in digital computers. When chaos is realized in digital computers, the chaotic systems will be discretized both spatially and temporally. That is, they will become discrete time and discrete-valued chaotic systems defined in discrete time and on finite spatial lattice. Generally speaking, there are two major ways to discretize continuous chaotic systems in digital computers as follows. **Implicit discretization** (Type-I): The continuous chaotic system is numerically realized in digital computers in a direct form, under fixed-point or floating-point finite precision. Apparently, continuous chaotic systems studied by most researchers using digital computers fall into this type of discretization. **Explicit discretization** (Type-II): The continuous chaotic equation is re-defined in digital forms (such as in integer form) to explicitly realize the discretization, or the equation itself is originally defined in a digital form.

For chaotic systems discretized in an explicit way, the finite-field or number theory may be available for the theoretical study of the dynamics. In fact, mixing integer maps widely-used in classical cryptography can also be considered as examples of Type-II discretized chaotic maps. In most cases, continuous chaotic systems are discretized in a direct way via numerical algorithms in digital computers, where a quantization function G(·) is always involved. The most frequently-used quantization functions in digital computers are round off, floor (or called truncation) and ceiling functions.

Given a 1-D discrete-time continuous chaotic map F : X ! X, its Type-I digital version FG is shown as FG = G_F : XG ! XG, where XG is the finite version of the real interval X and G : X ! XG is a quantization function. Generally, it is almost impossible to use finite-field or number theory to study the dynamics of Type-I discretized chaotic systems, due to the non-invertible combination of F and G. Note that the

quantization function G is also used in the definitions of some Type- II discretized chaotic systems.

A natural way to understand discretized chaotic systems with a quantization function G is to consider them as "discretized chaotic systems perturbed by (deterministic) quantization errors in discrete iterations, where " is the distance between two neighboring points in the lattice or the magnitude of the quantization perturbation. As a whole, the corresponding computerized chaotic systems with a binary quantization function are called digital chaotic systems.

III. Chaotic Cryptography

A. Chaos vs. Cryptography

Chaos theory is established since 1970s from many different research areas, such as physics, mathematics, biology and chemistry, etc. The most well-known characteristics of chaos are the so called "butterfly-effect" (the sensitivity to the initial conditions), and the pseudo-randomness generated by deterministic equations. Many researchers have pointed out that there exists tight relationship between chaos and cryptography. Many fundamental characteristics of chaos, such as the mixing property and the sensitivity to initial conditions, can be connected with "confusion" and "diffusion" property in good ciphers. Considering chaos theory has developed well in recent decades, chaos may become new ciphers.

The first scientific paper about chaotic cryptography was published in 1989, in which, a novel stream cipher based on one dimensional chaotic map. The chaos synchronization technique was firstly reported and the secure communications via chaos synchronization. From then on, chaotic cryptography has developed from different areas, chiefly physics, electrical and electronics engineering, computer science, and applied mathematics. Many digital chaotic ciphers and analog chaotic secure communication approaches have been proposed; the cryptanalytic works also have been developed to estimate the security of the proposed chaotic ciphers. It has been known that many proposed chaotic cryptosystems can be broken by some cryptanalytic methods, such as most analog chaotic secure communication approaches and some digital chaotic ciphers.

B. Fast Chaotic Ciphers

There are two general ways to design digital chaotic ciphers:

1. Generating pseudo-random key stream using chaotic systems to encrypt the plaintext.
2. Using the plaintext and/or secret key, as the initial conditions and/or control parameters, iterating/inverse-iterating chaotic systems for n times to obtain the ciphertext.

The first way corresponds to the stream cipher and the second to the block ciphers. Investigate currently known digital chaotic ciphers, we can find the following three facts:

1) Most chaotic block ciphers require iterating the employed chaotic systems for many times to make the ciphertext independent of the plaintext, which will markedly reduce the encryption speed.
2) Most chaotic stream ciphers employ one single chaotic system to generate pseudo-random numbers to mask the plaintext, which may weaken the capability to potential attacks.

C. The Original CKBA

A number of image encryption algorithms based on chaotic maps have been proposed. Chaotic-Key Based Algorithm (CKBA) is based on a one-dimensional Logistic map. The image encryption methods based on chaotic maps attract considerable attention due to their potential for digital multimedia encryption. In essence, CKBA is a value transformation cipher.

The encryption of an M * N image I by CKBA is realized as follows. Select two secret 8-bit keys k1 and k2, and a secret 16-bit initial condition x(0) of a one-dimensional chaotic system. Iteratively run the chaotic system to produce a sequence of 16-bit numbers. If I(x; y) is an 8-bit pixel value in the plaintext image I, with 0 _ x < M and 0 _ y < N, the corresponding cipher-text pixel is defined by the following rule:

$$I'(x,y) = \begin{cases} I(x,y) \oplus k_1, & \text{if } b'(x,y) = 3; \\ I(x,y) \oplus \overline{k_1}, & \text{if } b'(x,y) = 2; \\ I(x,y) \oplus k_2, & \text{if } b'(x,y) = 1; \\ I(x,y) \oplus \overline{k_2}, & \text{if } b'(x,y) = 0, \end{cases} \quad (1)$$

where $b'(x,y) = 2b(l) + b(l+1)$ and $l = 2(x + yM)$.

As a security requirement, although the keys k1 and k2 are chosen at random, it is required that the Hamming distance between them be 4. Finally, a quick observation shows that the decryption process is the identical mapping since XOR is an involution. the security of the aforementioned algorithm was highly overestimated. Furthermore, the original scheme is subject to well-defined chosen/known-plaintext attacks. That is, CKBA can be completely broken if only one plaintext image and its corresponding cipher-text image are known. Suppose we have the images I and its CKBA encryption I' obtained by using secret key (k1; k2; x(0)). By virtue of the algorithm's definition, I' can be obtained from I by XOR-ing it with a particular image mask Im. Consequently, the image mask Im can be obtained simply by XOR-ing images I and I'. This mask can then be used to completely decrypt all other

images of same or smaller size for which the same keys k1, k2, and x(0) were used. In applied cryptography, a cryptosystem that is susceptible to chosen/known-cipher-text attacks is not recommended in general. Having to change the key from image to image is a big drawback for many applications. Additionally, such cipher cannot maintain security when applied to videos (sequences of images). Therefore a cipher that can resist these kinds of attacks is much more preferable.

An improvement to CKBA based on increasing the key sizes, but as they noted, this only improves the resistance to a cipher-text-only attack, and does nothing to prevent the chosen/known-cipher-text attacks. Once a mask image is obtained, everybody can decrypt all images of same or smaller size that were encrypted with that same key by a simple XOR operation. Images of larger sizes could be decrypted partially, or fully when applying the brute force key recovery method . The main drawback of value substitution approaches such as CKBA is their susceptibility to chosen/known-cipher-text attacks via the substitution mask. Therefore, performing a substitution only, i.e, using only an S-box alone, is not recommended from a cryptanalytic point of view. However, if we change this simple substitution by a substitution followed by a variable pseudo-random permutation of the bits within each pixel value, we would have created an SP-network which is much harder to cryptanalyze. Note that performing only a permutation transformation to pixel values is not sufficient either, since the pixel values whose binary representation consists of all zeros or all ones will not be changed at all. Furthermore, an additional weakness exist in the systems where S-box consists of only one cryptographic primitive and where only one iteration of SP-network is performed during the encryption. Namely, such systems are subject to differential cryptanalysis. To resist the differential chosen-plaintext attack, it is necessary to further enhance the SP-network and to introduce multiple-round iteration.

1) *Logistic Map*

The logistic map is a polynomial mapping of degree 2, often cited as an archetypal example of how complex, chaotic behaviour can arise from very simple non-linear dynamical equations. This nonlinear difference equation is intended to capture two effects.

- reproduction where the population will increase at a rate proportional to the current population when the population size is small.

- starvation (density-dependent mortality) where the growth rate will decrease at a rate proportional to the value obtained by taking the theoretical "carrying capacity" of the environment less the current population.

However, as a demographic model the logistic map has the pathological problem that some initial conditions and parameter values lead to negative population sizes. This problem does not appear in the older Ricker model, which also exhibits chaotic dynamics.

2) *Chaos and logistic map*

The relative simplicity of the logistic map makes it an excellent point of entry into a consideration of the concept of chaos. A rough description of chaos is that chaotic systems exhibit a great sensitivity to initial conditions -- a property of the logistic map for most values of r between about 3.57 and 4 (as noted above). A common source of such sensitivity to initial conditions is that the map represents a repeated folding and stretching of the space on which it is defined. In the case of the logistic map, the quadratic difference equation describing it may be thought of as a stretching-and-folding operation on the interval (0,1). This stretching-and-folding does not just produce a gradual divergence of the sequences of iterates, but an exponential divergence, evidenced also by the complexity and unpredictability of the chaotic logistic map. In fact, exponential divergence of sequences of iterates explains the connection between chaos and unpredictability: a small error in the supposed initial state of the system will tend to correspond to a large error later in its evolution. Hence, predictions about future states become progressively (indeed, exponentially) worse when there are even very small errors in our knowledge of the initial state.

Since the map is confined to an interval on the real number line, its dimension is less than or equal to unity. Numerical estimates yield a correlation dimension of 0.500 ± 0.005, a Hausdorff dimension of about 0.538, and an information dimension of 0.5170976...for r=3.5699456... (onset of chaos). Note: It can be shown that the correlation dimension is certainly between 0.4926 and 0.5024. It is often possible, however, to make precise and accurate statements about the likelihood of a future state in a chaotic system. If a (possibly chaotic) dynamical system has an attractor, then there exists a probability measure that gives the long-run proportion of time spent by the system in the various regions of the attractor. In the case of the logistic map with parameter $r = 4$ and an initial state in (0,1), the attractor is also the interval (0,1) and the probability measure corresponds to the beta distribution with parameters $a = 0.5$ and $b = 0.5$. Unpredictability is not randomness, but in some circumstances looks very much like it. Hence, and fortunately, even if we know very little about the initial state of the logistic map (or some other chaotic system), we can still say something about the distribution of states a long time into the future, and use this knowledge to inform decisions based on the state of the system.

IV. Enhanced Chaotic Key Based Algorithm

A. The Enhanced CKBA (ECKBA)

Let I be an M*N image with b-byte pixel values, where a pixel value is denoted by I(i), 0 <i < M*N*b, scanned in the raster order. Let Cμ be a one-dimensional chaotic map with a real coefficient μ obtained by normalizing a 32-bit integer μ_{I32} to a chaotic interval. Let x(0) be the initial condition for C_ obtained by normalizing a 32-bit integer $x(0)_{I32}$ to a point range defined for Cμ. For a given n-bit segment x, let l(x) denote its low significant half and h(x) its high significant half. In addition, we define an S-box transformation as follows:

$$\sigma_r(u,v) = \begin{cases} u \oplus v, & \text{if } r \text{ is even;} \\ u + v \bmod 256, & \text{if } r \text{ is odd,} \end{cases} \quad (2)$$

$$\sigma_r^{-1}(u,v) = \begin{cases} u \oplus v, & \text{if } r \text{ is even;} \\ u - v \bmod 256, & \text{if } r \text{ is odd,} \end{cases} \quad (3)$$

where u and v are two bytes.

Finally, let Π_i, 0 _ i < 8! be a permutation of degree 8 whose index in the full symmetric group S8 sorted in lexicographical cartesian order is i. Without loss of generality assume that 4|r and r|MNb, where r specifies the number of rounds. The proposed encryption scheme is realized by Algorithm 1 in the Appendix. In the algorithm we make use of the following notation: if X_{I32} denotes a 32-bit integer variable, then x automatically denotes its normalized floating-point representation that corresponds to the relevant real interval, and vice versa.

B. 1-D Piecewise Linear Chaotic Map (PWLCM)

A piecewise linear map (PWLM) is a map composing of multiple linear segments, where limited breaking points are allowed. A typical example of PWLM is the skew tent map. Because not all PWLM exhibit chaotic behaviors, our attention is on a special class of PWLCM with the onto property. The main reason is that chaotic maps used in many digital applications belong to this class. A uniform invariant density function means that a uniform input will generate a uniform output, and that the chaotic orbit from almost every initial condition will lead to the same uniform distribution. However, these are not always true for digital chaotic maps. Assume that a 1D PWLCM is realized in a discrete space with 2n states, and take 2n different states as inputs of the chaotic map. The number of different outputs after one digital chaotic iteration will be smaller than 2n since any 1D PWLCM is a multi-to-one map (m > 1). That is to say, for a digital 1D PWLCM, generally discrete uniform inputs cannot generate discrete uniform outputs, or a uniform random variable will become non uniform after digital chaotic iterations.

1) Applications in chaotic cryptography

1D PWLCM have been widely used to construct digital chaotic ciphers. The theoretical results about the proposed dynamical indicators P1 _ Pn of digital 1D PWLCM will be very useful for the design and performance analyses of such chaotic ciphers. A digital 1D PWLCM have a deterministic relation with all linear segments' slopes. Also, it is possible to determine some information, such as the resolutions, of these slopes by observing the values of the n dynamical indicators. This can be used to discern weak keys in some digital chaotic ciphers and to develop weak-key-based cryptanalytic methods. A chaotic cipher was presented based on the digital 1D PWLCM.

2) Applications in chaotic PRNG

Digital 1D PWLCM have been used to construct PRNG, and many of them are specially designed for digital chaotic stream ciphers. Because of the non-uniformity of digital 1D PWLCM, pseudorandom numbers generated by digital 1D PWLCM will not satisfy a uniform distribution. For example, if the digital 1D PWLCM (2) with p = 1/4 is selected and the lowest 2 bits of the chaotic orbits are used to generate pseudo-random bits, we can see that they will always be zeros, 000….. . Unfortunately, in many chaotic PRNG, this risk exists. To enhance the uniformity of the generated pseudorandom numbers, some remedies should be employed and the perturbation-based algorithm is recommended since it can provide a better performance than other remedies. Because there still exists non uniformity even after perturbation, stronger control parameters will have more effects on chaotic PRNG than the weaker ones. If possible, we suggest only using the strongest control parameters, e.g. those in Vn, which is not a hard constraint in most situations.

In the following, we discuss two different structures of chaotic PRNG and explain the roles of digital 1D PWLCM in them. In secure applications of chaotic PRNG, if digital 1D PWLCM are used with bit extracting post-process, we suggest extracting middle bits of the chaotic orbit(s) to generate pseudorandom numbers, for the following two reasons:

1) The dependence of higher significant bits of the sequent chaotic states is somewhat larger than the one of lower bits8.
2) The dynamical degradation of digital 1D PWLCM mainly exhibits on lower significant bits and the pseudo-random perturbation is mainly influenced them.

Another acceptable solution is to combine bits at different positions of the concerned pseudo-orbit. Generally, combinations of different bits are strongly nonlinear operations, which can dramatically increase the complexity of pseudo-random numbers without too much computational

load. Also, accumulating multiple (and even all) previous states of the employed chaotic system can provide much better performance. In this structure, the digital chaotic system is used as a nonlinear post processing part of the conventional PRNG to enhance complexity of the pseudo-random numbers generated by the conventional PRNG, for example, to enhance the linear complexity of the m-sequence. When digital 1D PWLCM are used in the second structure, the distribution of the pseudo-random numbers generated by the conventional PRNG will not be influenced by much since digital 1D PWLCM have a nearly uniform distribution. Thus, this structure can also be used in those applications that require pseudorandom numbers with a non-uniform distribution. Obviously, a digital chaotic system can also be considered as a smoothing filter with a nonlinear transformation.

V. Conclusion

Enhanced chaotic key based algorithm for image encryption algorithm resembles some similarity with CKBA result, but attains a much higher security level. The enhanced security comes from the following changes to the original; a larger key space, a more chaotic one dimensional map and the use of a multi-round SP network. By using large key size, it will get more defenses from brute force attack, the chaotic one dimensional map will improved the balance property and SP network will increase the security of the entire algorithm.

References

[1] B. Furht and D. Socek. Multimedia security: encryption techniques. In IEC Comprehensive Report on Information Security, International Engineering Consortium, Chicago, IL, pages 335.349, 2004.

[2] S. Li, G. Chen, and X. Zheng. Chaos-based encryption for digital images and videos, in B. Furht and D. Kirovski (Eds.), Multimedia Security Handbook, Vol. 4 of Internet and Communications Series, Ch. 3, CRC Press, December 2004.

[3] B. Furht, D. Socek, and A.M. Eskicioglu. Fundamentals of multimedia encryption techniques, in B. Furht and D. Kirovski (Eds.), Multimedia Security Handbook, Vol. 4 of Internet and Communications Series, Ch.3, CRC Press, December 2004.

[4] L. Tang. Methods for encrypting and decrypting MPEG video data efficiently. In Proceedings of the 4th ACM International Multimedia Conference, pages 219.230, 1996.

[5] H. Cheng and X. Li. Partial encryption of compressed images and videos. In IEEE Transactions on Signal Processing, volume 48, pages 2439.2451, 2000.

[6] J.-C. Yen and J.-I. Guo. A new chaotic key-based design for image encryption and decryption. In Proceedings of 2000 IEEE International Conference on Circuits and Systems (ISACS 2000), volume 4, pages 49.52, 2000.

[7] B. Bhargava, C. Shi, and S.-Y. Wang. MPEG video encryption algorithms. Multimedia Tools and Applications, Kluwer Academic Publishers, Vol. 24, No. 1, pages 57.79, 2004.

[8] L. Qiao, K. Nahrstedt, and I. Tam. Is MPEG encryption by using random list instead of zigzag order secure? In IEEE International Symposium on Consumer Electronics, Singapore, 1997.

[9] T. Seidel, D. Socek and M. Sramka. Cryptanalysis of video encryption algorithms. In Proceedings of The 3rd Central European Conference on Cryptology (TATRACRYPT '03), Bratislava, Slovak Republic, June 26-28 (2003), Tatra Mt. Mathematical Publications, Vol. 29, pages 1.9, 2004.

[10] S. Li and X. Zheng. Cryptanalysis of a chaotic image encryption method. In Proceedings of 2002 IEEE International Symposium on Circuits and Systems (ISCAS 2002), volume 2, pages 708.711, 2002.

[11] D.R. Stinson. Cryptography: theory and practice. CRC Press, second edition, 2002.

[12] A. Lasota and M.C. Mackey. Chaos, fractals, and noise. Stochastic aspects of dynamics. Springer-Verlag, New York, 2nd Ed., 1997. [13] H. Zhou. A design methodology of chaotic stream ciphers and the realization problems in _nite precision. Ph.D. thesis, Department of Electrical Engineering, Fudan University, Shanghai, China, 1996.

[14] S. Li, Q. Li, W. Li, X. Mou and Y. Cai. Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding. In Cryptography and Coding - 8th IMA International Conference, volume 2260 of Lecture Notes in Computer *Science*, pages 205.221. Springer-Verlag, Berlin, 2001.

[15] S. Li, G. Chen and X. Mou. On the Dynamical Degradation of Digital Piecewise Linear Chaotic Maps. accepted by the Tutorial-Review section of International Journal of Bifurcation and Chaos in August 2004, tentatively scheduled for publication in vol. 15, no. 10, 2005.

[16] S.S. Magliveras. A cryptosystem from logarithmic signatures of _nite groups. In Proceedings of the 29th Midwest Symposium on Circuits and Systems, pages 972.975. Elsevier, Ampsterdam, 1986.