CHAPTER 2

LITERATURE SURVEY

2.1 CHAOS BASED RANDOM NUMBER GENERATOR

For a truly random generator, the number of ones and zeros in the output are equal. It is possible to formulate many other statistical properties that describe the key stream generated by a random source. Various test suites are available in the literature. These statistical tests are designed to evaluate the randomness properties of a finite sequence. The chaotic orbit generated by a nonlinear system is irregular, aperiodic, unpredictable, and has sensitive dependence on the initial conditions. These characteristics coincide with the confusion and diffusion properties in cryptography. Therefore, in recent years, the chaotic system has been studied for security in both analog and digital forms.

Chen et al (2010) proposed a nonlinear Digitalized Modified Logistic Map-based Pseudo Random Number Generator (DMLM-PRNG) for enhancing randomness. Two techniques, i.e., constant parameter selection and output sequence scrambling are employed to reduce the computation cost, without sacrificing the complexity of the output sequence. Chaotic map-based PRNGs have been proposed by Addabbo et al 2007 and Callegari et al 2005.

Savi (2007) considered randomness as fluctuations and uncertainties due to noise and investigated its influence on the nonlinear dynamic behavior of coupled logistic maps. The noise effect is included by adding random variations, either to the parameters or to the state variables.
Chang et al (2007) proposed a robust chaotic map, the modified logistic map, which not only exhibits no chaotic window but also uniformly distributes in 0, 1. On the basis of this map, they designed a multi-system hyper-chaotic synchronization system, the asymptotic synchronization of the modified logistic hyper-chaotic system, for secure communication. The system can theoretically achieve, asymptotical synchronization between the transmitter and receiver after finite times in simplex partial coupling transmission. Furthermore, the implicit driving technique always guarantees asymptotical synchronization between the drive and response systems during plaintext transmission.

Rani and Agarwal (2009) proposed to enhance the capabilities of the logistic map via superior iterations. Logistic transformations $x_{n+1} = rx_n(1-x_n)$ for choosing $x_0$ between 0 and 1 and $0 < r \leq 4$ have found a celebrated place in chaos, fractals and discrete dynamics. The stability of logistic map is studied by running computer programs. The logistic map is stable for $0 < r \leq 3.2$ in Picard orbit. In superior orbit, the range of stability of the logistic map increases drastically. Also, the behavior of the map disappears in certain cases.

2.2 STREAM ENCRYPTION SCHEME

Stream encryptions are based on generating an infinite cryptographic key stream, and use that to encrypt one bit or byte at a time. Stream ciphers have relatively low memory requirements. This section gives a brief review on stream encryption schemes.

Chen et al (2004) proposed a 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. This scheme employs the 3D cat map to shuffle the positions of
image pixels, and uses another chaotic map to confuse the relationship between the cipher-image and the plain-image, thereby significantly increasing the resistance to statistical and differential attacks.

A new gray-level image encryption scheme based on phase-encoded exclusive-OR (XOR) operations and a full phase encoding method are proposed by Shin et al (2004). The gray-level image can be sliced into binary images which have the same pixel level, and each of them is encrypted by phase-encoded XOR operations with each phase-encoded binary random image. They combine XORed images and phase-encoded binary random images into an encrypted image and a key image, respectively. Gray-level encrypted data and key data are obtained by the phase-encoding process of the encrypted image and the key image in a space domain.

Guan et al (2005) proposed a chaos-based image encryption algorithm, in which shuffling the positions and changing the grey values of the image pixels are combined to confuse the relationship between the cipher-image and the plain-image. Firstly, the Arnold cat map is used to shuffle the positions of the image pixels in the spatial-domain. The experimental results demonstrate that the key space is large enough to resist the brute-force attack, and the distribution of the grey values of the encrypted image has a random-like behavior.

Zhang et al (2005) proposed an image encryption approach based on chaotic maps, to improve the properties of confusion and diffusion in terms of discrete exponential chaotic maps, and designed a scheme for resisting statistic, differential and grey code attacks.

Pareek et al (2006) proposed an image encryption scheme where 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 weightage to all its bits. Further, in the proposed encryption process, eight different types of operations are used to encrypt of an image and which one of them is used for a particular pixel is taken by the outcome of the logistic map.

Wong et al (2008) proposed to introduce certain diffusion effect in the substitution stage by simple sequential add-and-shift operations. Although this leads to a longer processing time in a single round, the overall encryption time is reduced as fewer rounds are required. Wong et al (2009) proposed a more efficient diffusion mechanism using simple table lookup and swapping techniques as a light-weight replacement of the 1D chaotic map iteration.

Mazloom and Eftekhari-Moghadam (2009) proposed a Coupled Nonlinear Chaotic Map (CNCM), based image encryption algorithm to encrypt color images using CNCM. The chaotic cryptography technique is used as a symmetric key cryptography with a stream cipher structure. In order to increase the security of the proposed algorithm, 240 bit-long secret key is used to generate the initial conditions and parameters of the chaotic map by making some algebraic transformations to the key. These transformations as well as the nonlinearity and coupling structure of the CNCM have enhanced the cryptosystem security.

Wang et al (2009) proposed chaos based image encryption algorithm with variable control parameters. The control parameters used in the permutation stage and the key stream employed in the diffusion stage are generated from two chaotic maps related to the plain-image. As a result, the algorithm can effectively resist all known attacks against permutation-diffusion architectures.

The cryptosystem employing two-dimensional chaotic maps for document encryption is proposed by Xiang et al (2007). Several widely used
two-dimensional chaotic maps are considered and their performances are investigated. Yoon and Kim (2010) proposed an image encryption algorithm using a large pseudorandom permutation which is combinatorially generated from small permutation matrices based on chaotic maps. The random-like nature of chaos is effectively spread into encrypted images by using the permutation matrix.

Akhshani et al (2010) proposed two-dimensional piecewise nonlinear chaotic maps with an invariant measure and then used to design a fast and highly secure symmetric image encryption scheme. These maps have advantages such as invariant measure, ergodicity and the possibility of K-S entropy calculation. In this scheme, its control parameters and initial values can all be used as encryption key in chaotic cryptosystem.

Hongjuna and Xingyuana (2010) designed a stream-cipher algorithm based on one-time keys and robust chaotic maps, in order to get high security and to improve the dynamical degradation. They utilized the piecewise linear chaotic map as the generator of a pseudo-random key stream sequence.

Ye (2010) presented an image scrambling encryption algorithm of pixel bit based on chaos map. The algorithm uses a single chaos map only once to implement the gray scrambling encryption of an image, in which the pixel values ranging from 0 to 255 are distributed evenly; the positions of all pixels are also permutated. In this way, the proposed method transforms drastically the statistical characteristic of original image information and so it increases the difficulty of an unauthorized individual to break the encryption.

A robust image encryption method by using the integral imaging and Pixel Scrambling (PS) techniques is proposed by Piao et al (2009). In this method, pixels of the color image are scrambled with the PS technique and
elemental images for this scrambled image are picked up through a lenslet array. Subsequently, an encrypted image is obtained by scrambling these picked-up elemental images. Since this encrypted image has the hologram-like property of data redundancy resulted from the integral imaging scheme, it can as well be decoded by multiple keys such as the orders of pixel scrambling.

Sun et al. (2010) proposed Spatial Chaos System (SCS), which is investigated by conducting FIPS 140-1 statistic test, and is especially useful for encryption of digital images. It is shown how to adapt a two dimensional (2D) ergodic matrix obtained from SCS to permute the positions of image pixels and confuse the relationship between the cipher-image and plain-image simultaneously.

Kumar and Ghose (2011) proposed an extended substitution-diffusion based image cipher using chaotic standard map and linear feedback shift register. The first stage consists of row and column rotation and permutation which is controlled by the pseudo random sequences which is generated by standard chaotic map and linear feedback shift register, second stage further diffusion and confusion are obtained in the horizontal and vertical pixels by mixing the properties of the horizontally and vertically adjacent pixels, respectively, with the help of chaotic standard map. The number of rounds in both stages is controlled by combination of pseudo random sequence and original image.

Zhang and Liu (2011) proposed a novel image encryption method based on skew tent chaotic map and permutation-diffusion architecture. In the proposed method, the P-box is chosen as the same size of plain-image, which shuffles the positions of pixels totally. The key stream generated by skew tent chaotic map is related to the plain-image.
There has been a large amount of research in stream based encryption, as well.

2.3 BLOCK ENCRYPTION SCHEME

Block encryption is an encryption scheme in which the plain text is broken up into blocks of fixed length, and encrypted one block at a time. Block ciphers can provide integrity protection, and confidentiality. Chaotic block ciphers transform blocks by directly applying the chaotic maps. This section gives a brief review of block encryption schemes.

Amin et al (2010) proposed a chaotic block cipher scheme for image cryptosystems that encrypts block of bits rather than block of pixels. It encrypts 256-bits of plain-image to 256-bits of cipher-image within eight 32-bit registers. The scheme employs the cryptographic primitive operations and a nonlinear transformation function within encryption operation, and adopts round keys for encryption using a chaotic system.

Jakimoski and Kocarev (2001) suggested a class of block encryption ciphers based on chaos, using two well-known chaotic maps: exponential and logistic. They have shown that maps produce ciphers that have acceptable values of differential and linear approximation probabilities. The ciphers use only byte operations that can be easily implemented on various processors.

A block cryptographic scheme based on iterating a chaotic map is proposed by Xiang et al (2006). With random binary sequences generated from the real-valued chaotic map, the plaintext block is permuted by a key-dependent shift approach and then encrypted by the classical chaotic masking technique. Lian et al (2005) proposed a block cipher based on the chaotic
standard map which is composed of three parts: a confusion process based on chaotic standard map, a diffusion function, and a key generator.

Kwok and Tang proposed a fast chaos based image encryption system with stream cipher structure to achieve a fast throughput and to facilitate hardware realization; Further a 32-bit precision representation with fixed point arithmetic is assumed. The major core of the encryption system is a pseudo-random key stream generator based on a cascade of chaotic maps, serving the purpose of sequence generation and random mixing. Unlike the other existing chaos based pseudo-random number generators, the proposed key stream generator not only achieves a very fast throughput, but also passes the statistical tests of up-to-date test suite even under quantization.

A fast image encryption and authentication scheme is proposed by Yang et al (2010). In particular, 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 plays the role of the key for encryption and decryption while the secret hash keys are used to authenticate the decrypted image.

A block encryption for image using combination of confusion and diffusion is proposed by Wang et al (2010). Baker map is used to generate a pseudo-random sequence, and several one-dimension chaotic maps are dynamically selected to encrypt blocks of image. When diffusion is executing, for mutual diffusion of pixels, the confusion is working by the pseudo random order of route and the combination is deep seated.

A block encryption scheme based on dynamic substitution boxes (S-boxes) is considered by Wang et al (2009). The difference trait of the tent map is analyzed. Then, a method for generating S-boxes based on iterating the tent map is presented. The plaintexts are divided into blocks and encrypted
with different S-boxes. The cipher blocks are obtained by 32 rounds of substitution and left cyclic shift.

Wang et al (2011) proposed a fast image encryption algorithm with combined permutation and diffusion. First, the image is partitioned into blocks of pixels. Then, spatiotemporal chaos is employed to shuffle the blocks and at the same time, to change the pixel values. Meanwhile, an efficient method for generating pseudo random numbers from spatiotemporal chaos is suggested, which further increases the encryption speed.

Wang et al (2011) proposed chaotic encryption algorithm based on alternant of stream cipher and block cipher which encrypts the plaintext based on alternant of the stream cipher and block cipher. A pseudo-random number is used to control which encryption mode is chosen. Using this algorithm, multiple kinds of files (such as TXT, DOC, WMA, and JPEG) are encrypted and decrypted, and the security of the proposed cryptosystem is analyzed.

Awad (2011) presented a robust chaos-based cryptosystem for secure transmitted images and four other versions. In the proposed block encryption/decryption algorithm, a 2D chaotic map is used to shuffle the image pixel positions. Then, substitution and permutation operations on every block, with multiple rounds, are combined using two perturbed chaotic maps.

Therefore, the block encryption scheme has been considered as one of the most important topics in encryption, by many researchers.

2.4 CRYPTANALYSIS OF CHAOTIC ENCRYPTION

Research on the security of cryptographic algorithms has been essentially concerned with classical cryptanalysis. Even if the cipher is mathematically sound, he may in this way be able to recover the secret key.
The key is the most important thing in cryptosystems. Once the key is cracked, the cryptosystem will break down. Two important things should be considered when designing a chaotic cryptosystem. The first one is that the distribution of the ciphertext should be sufficiently flat, in order to resist the statistics attack. The other is that the sub-keys should depend on not only the secret key but also the plaintext, to avoid key stream attack.

Jakimoski and Subbalakshmi (2008) analyzed the security and efficiency of some recently proposed schemes for multimedia encryption: key-based Multiple Huffman Tables (MHT), arithmetic coding with key-based interval splitting and Randomized Arithmetic Coding (RAC). They showed that MHT and key-based interval splitting are vulnerable to known-plaintext attacks.

Wang et al (2007) presented a flaw of Xiang’s et al (2006) cryptosystem and a chosen plaintext attack. Furthermore, a remedial improvement is suggested, which avoids the flaw while keeping all the merits of the original cryptosystem. Wang and Yu (2009) analyzed their cryptosystem, and how cryptanalysts could recover the plaintext by the chosen plaintext attack in a short time. Therefore, the authors proposed a remedial improvement which can avoid the flaws, and enhance the security of the cryptosystem.

Cokal and Solak (2009) analyzed the security weaknesses of the Guan et al’s (2005) algorithm. They demonstrated that the secret keys can be revealed using chosen and known plaintext attacks.

Li et al (2009) presented a paper, focused on the security analysis of the image encryption scheme proposed by Pareek et al (2006) and reports the following findings:
(1) There are several types of security problems with the secret key, and each subkey is involved in at least one problem.

(2) One subkey $K_{10}$ can be separately searched with a relatively small computational complexity, even when only one chosen plain-image is given.

(3) The scheme is insecure against chosen-plaintext attack in the sense that using 128 chosen plain-images may be enough to break part of the key. The attack is especially feasible when $K_{10}$ is not too large.

(4) When $K_{10}$ is relatively small and one plain-image is known, a known-plaintext attack can be used to reveal some visual information of any other plain-image encrypted with the same secret key.

Alvarez and Li (2009) described the security weakness of Gao et al. (2006) proposed image encryption algorithm based on a logistic-like new chaotic map. They showed that the chaotic map’s distribution is far from ideal, thus making it a bad candidate as a pseudo-random stream generator. As a consequence, the images encrypted with this algorithm are shown to be breakable through different attacks of variable complexity.

Tong and Cui (2008) proposed encrypting image scheme using the new compound chaotic function by choosing one of the two one-dimensional chaotic functions randomly. Li et al (2009) reported that their scheme can be broken with only three chosen plain-images. In addition, it is found that the scheme has some weak keys and equivalent keys, and that the scheme is not sufficiently sensitive to the changes of plain-images. Furthermore, the
pseudo-random number sequence generated by iterating the compound chaotic function is found not to be sufficiently random for secure encryption.

Rozouvan (2009) proposed a modulo image encryption scheme with fractal keys. Yoon and Yoo (2010) demonstrated that Rozouvan’s scheme is not secure to the following three different classical types of attacks: chosen plaintext, chosen ciphertext, and known plaintext. In the three attacks, only a pair of (plaintext/ciphertext) was needed to break the image encryption scheme.

2.5 QUASIGROUP ENCRYPTION SCHEME

The non-associative property of quasigroups has been recently found to be useful in many information security applications. Quasigroups operations are computationally simple, and can be efficiently used for the protection of voluminous media like images, audio, video and different forms of multimedia. This section presents a practical implementation of a quasigroup based single and multi-level indexed scrambling transformation used in cryptography.

Koscielny (2002) presented a method of generating a practically unlimited number of quasigroups of a (theoretically) arbitrary order using the computer algebra system Maple 7. This problem is crucial to cryptography and its solution permits to implement practical quasigroup-based endomorphic cryptosystems. The order of a quasigroup usually equals the number of characters of the alphabet used for recording both the plaintext and the ciphertext. From the practical viewpoint, the most important quasigroups are of order 256, suitable for a fast software encryption of messages.

Satti and Kak (2009) have shown that quasigroup scrambling constitutes an excellent method of encryption and generation of pseudo-
random sequences. Quasigroups (or Latin squares) provide a powerful method for generating a larger set of permutation transformations by permuting not only the samples but also transforming the amplitudes themselves across their range. By doing this, they provided an immensely large number of keys, even for small alphabets. The randomization obtained is very good.

Pal et al (2010) proposed the suitability of quasigroup based structures for encryption and hashing were established with examples, implementations and favorable observations and results. Construction of large and unstructured quasigroups is useful for design of encryption schemes with large key space. Pal et al (2009) proposed an efficient cryptographic hash function based on random Latin squares and non-linear transformations. This developed scheme satisfies basic as well as desirable properties of an ideal hash function.

Gligoroski (2004) proposed a stream cipher based on quasigroup string transformations in $\mathbb{Z}p^*$. The cryptographical strength of the proposed stream cipher is based on the fact that breaking it would be at least as hard as solving systems of multivariate polynomial equations modulo big prime number $p$ which is NP-hard problem and there are no known fast randomized or deterministic algorithms for solving it. Unlike the speed of known ciphers that work in $\mathbb{Z}p^*$ for big prime numbers $p$, the speed of this stream cipher both in encryption and decryption phase is comparable with the fastest symmetric key stream ciphers.

Error-correcting codes based on quasigroup transformations are proposed by Gligoroski et al (2007). The proposed codes, similar to recursive convolutional codes, the correlation exists between any two bits of a codeword, which can have infinite length, theoretically. However, in contrast to convolutional codes, the proposed codes are nonlinear and almost random:
for code words with large enough length, the distribution of the letters, pair of letters, triple of letters, and so on, is uniform.

Shcherbacov (2009) reviewed, it is possible to change associative systems by non-associative ones and practically in any case this change gives in some sense better results than these by the use of associative systems. Quasigroups in spite of their simplicity, have various applications in cryptology. Many new cryptographical algorithms can be formed on the basis of quasigroups.

Castroa et al (2005) analyzed some test for measuring the strength of cryptographic primitives including block ciphers, stream ciphers and pseudorandom number generators, especially during the design and analysis phase.

Millérioux et al (2008) proposed a connection between chaotic and conventional encryption with special emphasis on two of the most attractive schemes, namely, message embedding and hybrid message embedding. The main point can be stated as follows: the (hybrid) message-embedded cryptosystem is equivalent to a conventional self-synchronizing stream cipher under flatness conditions.

A mammoth number of image encryption schemes have been proposed in the literature, and the key is generated by using various maps and methods. Most of the schemes are linear in nature, have a weak key, equivalent key, less sensitivity in key and cipher image, high computation cost, low security and fail to withstand attacks and low speed. Thus, the proposed schemes attempted to alleviate the aforementioned problems and new maps are designed to generate secret keys for schemes. Cryptanalysis techniques are considered during the design of new encryption schemes.