5

Multimedia Security: A Survey of Chaos-Based Encryption Technology

Zhaopin Su, Guofu Zhang and Jianguo Jiang
School of Computer and Information, Hefei University of Technology
China

1. Introduction

In the recent years, with the development of network and multimedia technology, multimedia data, especially image, audio and video data, is used more and more widely in human society. Some multimedia data, including entertainment, politics, economics, militaries, industries, education etc, are necessary to be protected by providing confidentiality, integrity, and ownership or identity. In this regard, to protect multimedia contents, cryptology, which appears to be an effective way for information security, has been employed in many practical applications.

However, number theory or algebraic concepts based traditional ciphers, such as Data Encryption Standard (DES) (Tuchman, 1997), Advanced Encryption Standard (AES) (Zeghid et al., 1996), International Data Encryption Algorithm (IDEA) (Dang & Chau, 2000), and the algorithm developed by Rivest, Shamir and Adleman (RSA) (Cormen et al., 2001), most of which are used for text or binary data, appear not to be ideal for multimedia applications, and the reasons are:

(1) As multimedia data, especially image and video data, are usually very large-sized and bulky, encrypting such bulky data with the traditional ciphers incurs significant overhead, and it is too expensive for real-time multimedia applications, such as video conference, image surveillance, which require real-time operations, such as displaying, cutting, copying, bit-rate control or recompression.

(2) In the case of digital image, adjacent pixels often have similar gray-scale values and strong correlations, or image blocks have similar patterns, while for video data, consecutive frames are similar and most likely only few pixels would differ from frame to frame. Such an extremely high data redundancy of multimedia makes the conventional ciphers fail to obscure all visible information (Furht et al., 2005).

(3) For many real-life multimedia applications, it is very important that very light encryption should be made to preserve some perceptual information. For example, video pay-per-view system (Ballesté, 2004) in which a degraded but visible content could potentially influence a consumer to order certain paid services. This is impossible to achieve with traditional ciphers alone, which most likely degrade the data to a perceptually unrecognizable content.

Very recently, an increasing attention has been devoted to the usage of chaotic theory to implement the encryption process (Alligood et al., 1997; Alvarez et al., 2004; Devaney, 2003; He et al., 2010; Solak, 2005; Yang et al., 1997). The main advantage of these encryptions lies in the observation that a chaotic signal looks like noise for non-authorized users ignoring the mechanism for generating it. Secondly, time evolution of the chaotic signal strongly depends on the initial conditions and the control parameters of the generating functions: slight variations in these quantities yield quite different time evolutions. In other words, this means that initial states and control parameters can be efficiently used as keys in an encryption system. What's more, generating of chaotic signal is often of low cost, which makes it suitable for the encryption of large bulky data (Alvarez & Li, 2006).

Due to these recognized potential benefits, chaos-based multimedia encryption algorithms are of high interest up to now, and have made great progress (Chen et al., 2004; Gao et al., 2006; Li et al., 2002; Lian, 2009; Su et al., 2010; Wang et al., 2011). This chapter focuses on a survey of chaos-based encryption algorithms for image, video and audio respectively.

The organization of this chapter is as follows. In Section 1, backgrounds of chaos-based multimedia encryption technology are first given. Section 2 describes some special requirements of multimedia encryption. To evaluate the performance of multimedia encryption algorithms, Section 3 gives some generic evaluation methods. In Section 4, 5 and 6, the existing chaos-based encryption algorithms are analyzed for image, video and audio, respectively. The last section concludes the chapter.

2. Requirements of multimedia encryption

Due to special characteristics of multimedia data, such as large data volumes, high redundancy, interactive operations, and requires real-time responses, sometimes multimedia applications have their own requirements like security, invariance of compression ratio, format compliance, transmission error tolerance, demand of real-time. In this section, some special requirements of multimedia encryption are summarized.

2.1 Security

For multimedia encryption, security is the primary requirement, thus the usage of chaotic maps should guarantee the security of a multimedia datum. Generally speaking, an encryption algorithm is regarded as secure if the cost for cracking it is no smaller than the one paid for the authorization of video content. For example, in broadcasting, the news may be of no value after an hour. Thus, if the attacker can not break the encryption algorithm during an hour, then the encryption algorithm may be regarded as secure in this application (Lian et al., 2008). Security of an encryption usually consists of its perceptual security, its key space, key sensitivity, and its ability against potential attacks.

(1) Perceptual security: when we use a method to encrypt a multimedia datum, for example an image, if the encrypted image is not perceptual recognized, the encryption is secure in perception.

(2) Key space: it is generally defined as the number of encryption keys that are available in the cryptosystem. Assume k_i denotes a key and K represents a finite set of possible keys, the key space can be expressed as $K = \{k_1, k_2, ..., k_r\}$, where r is the number of key. For

chaos-based encryptions, the chaotic sequence generator should produce chaotic ciphers with good randomness, which can be tested by long period, large linear complexity, randomness and proper order of correlation immunity (Rueppel, 1986).

(3) Key sensitivity: an ideal multimedia encryption should be sensitive with respect to the secret key i.e. the change of a single bit in the secret key should produce a completely different encrypted result, which is called key sensitivity. Generally, key sensitivity of a chaotic cipher refers to the initial states sensitivity and control parameters sensitivity of chaotic map.

(4) Potential attacks: here, we just introduce the common used attacks as following:
- Ciphertext-only attack: it is an attack with an attempt to decrypt ciphertext when only the ciphertext itself is available. The opponent attempts to recover the corresponding plaintext or the encryption key.
- Known-plaintext attack: when having access to the ciphertext and an associated piece of plaintext, the opponent attempts to recover the key.
- Chosen-plaintext attack: it is an attack where the cryptanalyst is able to choose his own plaintext, feed it into the cipher, and analyze the corresponding ciphertext.
- Brute-force attack: it is a form of attack in which each possible key is tried until the success key is obtained. To make brute-force attack infeasible, the size of key space should be large enough.
- Differential attack: it is a chosen-plaintext attack relying on the analysis of the evolution of the differences between two plaintexts.

Therefore, a secure encryption algorithm should be secure in perception, have large key space, high key sensitivity, and resist potential attacks.

2.2 Other requirements

Besides security, there are many other requirements as follows.

(1) Computational complexity: compared with texts, multimedia data capacity is horrendously large. For example, a common 16-bit true-color image of 512-pixel height and 512-pixel width occupies $512 \times 512 \times 16/8 = 512KB$ in space. Thus, a one-second motion picture will reach up to about 13 MB. If a cryptographic system encrypts all of the multimedia data bits equally in importance, the computational complexity may be high, which has often proved unnecessary. As human vision or audition has high robustness to image or audio degradation and noise, only encrypting those data bits tied with intelligibility can efficiently accomplish multimedia protection with low computational complexity.

(2) Invariance of compression ratio: an encryption algorithm with invariance of compression ratio can preserve the size of a multimedia datum, and maintain the same storage space or transmission bandwidth. However, in some practical applications, the encryption stage is allowed to slightly increase the size of a bit stream. In this case, multimedia encryption algorithms should not change compression ratio or at least keep the changes in a small range (Su et al., 2011).

(3) Format compliance: due to the huge amount of multimedia data and their very high redundancy, the data are often encoded or compressed before transmission, which produces the data streams with some format information. The format information will be used by the decoder to recover the multimedia data successfully. Thus, directly encrypting multimedia data as ordinary data will make file format conversion impossible. It is desired that the encryption algorithm preserves the multimedia format. This property of an encryption algorithm is often called format compliance. Generally, encrypting the data except the format information will keep the multimedia format. This will support some direct operations(decoding, playing, bit-rate conversion, etc.) and improve the error robustness in some extent.

(4) Demand of real-time: real-time performance is often required for many multimedia applications, e.g. video conferencing, image surveillance. However, bulk capacity of multimedia data also makes real-time encryption difficult. Therefore, the main challenge is how to bring reasonable delay of encryption and decryption to meet the requirements of real-time applications.

(5) Multiple levels of security: in some image or video applications, multiple levels of security may be needed for the ability to perform more complex multimedia processing. For example, in video pay-per-view system, only those users who have paid for the service can have access to large-size images or video with high resolution, and the others may be able to get some small-size images or video with low resolution and little business value. Most available cryptographic systems are fully or partially scalable, in the sense that one can choose different security levels. Scalability is usually achieved by allowing variable key sizes or by allowing different number of iterations, or rounds. A higher level of security is achieved with larger key sizes or larger number of rounds.

(6) Transmission error tolerance: since the real-time transport of multimedia data often occurs in noisy environments, which is especially true in the case of wireless channels (Gschwandtner et al., 2007; Lin, Chung & Chen, 2008), the delivered multimedia data is prone to bit errors. So, a perfect encryption algorithm should be insensitive and robust to transmission errors.

3. Evaluation methods of multimedia encryption

Generally speaking, a multimedia encryption algorithm is often evaluated by security analysis, time analysis, compression ratio and error robustness.

3.1 Security analysis

Security of an algorithm is generally evaluated by the perceptual experiments, key space analysis, key sensitivity analysis, and the ability against attacks.

The perceptual experimental result is achieved by a group of comparison between the original multimedia data and the encrypted. Besides, some works decrypt the encrypted data to examine the effects of their algorithms.

Key space can be obtained by analyzing the number of key used in the encryption process. For example, a 20-bit key would have a key space of 2^{20}.

Key sensitivity of a chaotic cipher refers to the initial states sensitivity and control parameters sensitivity of chaotic map. Take image encryption as an example, a typical key sensitivity test is performed according to the following steps:

Step 1. First, an original image is encrypted by using the secret key "K1=0123456789ABCDEF", and the resulting image is referred to as encrypted image A.

Step 2. Then, the same image is encrypted by making the slight modification in the secret key i.e. "K2=1123456789ABCDEF", which changes the least significant bit of K1. The resultant image is referred to as encrypted image B.

Step 3. Finally, the above two encrypted images, encrypted by K1 and K2 respectively, are compared, and cross-correlation curve between the two encrypted images is analyzed.

A good cipher can avoid potential attacks. In general, brute-force attack is analyzed by key apace analysis. Known-plaintext attack and chosen-plaintext attack can be tested by comparing the original data and the decrypted. Differential attack test can be achieved through measuring the percentage p of different pixel numbers (see Equation 1 and Equation 2) between two encrypted images, I_1 and I_2 (the width and height is W and H, respectively), whose corresponding plain-images have only one pixel's difference. And the bigger p is, the stronger the ability of the encryption to resist differential attack.

$$p = \frac{\sum_{i,j} D(i,j)}{W \cdot H} \cdot 100\%, i = 0, 1, \cdots, W-1 j = 0, 1, \cdots, H-1 \tag{1}$$

$$D(i,j) = \begin{cases} 0, I_1(i,j) = I_2(i,j) \\ 1, \text{otherwise} \end{cases} \tag{2}$$

3.2 Time analysis

The encryption time analysis is measured in the following three manners:

(1) Absolute encryption time: it refers to the assumed time for encrypting a multimedia datum on a certain running platform, and its measuring unit is second.

(2) Relative encryption time ratio: it refers to the time ratio between encryption and compression.

(3) Computation complexity: it depends on the cost of the chaos-based cipher and the multimedia data volumes to be encrypted.

If the computational cost or assumed time of a multimedia encryption scheme is very little compared with their compression, it is considered to be suitable for real-time applications.

3.3 Compression ratio test

In general, the compression ratio is tested by comparing the original compressed data volumes and encrypted and compressed data volumes. Considering that the compression encoder often produces the data stream with a given bit-rate, the compression ratio test may be measured by the video quality under certain bit rate.

The common measurement of image and video quality is $PSNR$ (Peak Signal-to-Noise Ratio) shown as Equation 3 and Equation 4, where B is the sampling frequency, I and I' represent an original $m \times n$ image and the encrypted one, respectively.

$$PSNR = 10 \cdot \log_{10} \left(\frac{(2^B - 1)^2}{MSE} \right) \tag{3}$$

$$MSE = \frac{1}{m \cdot n} \cdot \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left[I(i,j) - I'(i,j) \right]^2 \tag{4}$$

The common measurement of audio quality is $segSNR$ (Segmented Signal-to-Noise Ratio) shown as Equation 5, where M is the number of frames in the audio file, $s(i)$ is the ith frame of the original audio, $sn(i)$ is the ith frame of the encrypted audio.

$$segSNR = \frac{10}{M} * \log_{10} \frac{sum[s(i)]^2}{sum[sn(i) - s(i)]^2} \tag{5}$$

From Equation 3, Equation 4 and Equation 5, big $PSNR$ and $segSNR$ would appear to indicate that the encryption has good performance and high security.

3.4 Error-robustness test

If an encryption scheme does not change file format, and a slight change in one pixel does not spread to others, it is called transmission error robustness.

The general test method for error-robustness is analyzing the relationship (usually expressed by a curve) between the quality ($PSNR$ for image and video, $segSNR$ for audio) of the decrypted frames and the number of bit-error happened in the encrypted frames. Besides, error-robustness can be tested through correct decryption of an encrypted data, even if a frame or some bytes are corrupted or lost in its transmission.

4. Chaos-based image encryption algorithms

So far, many chaos-based image encryption methods have been proposed. According to the percentage of the data encrypted, they are divided into full encryption and partial encryption (also called selective encryption). Moreover, with respect to the encryption ciphers, the two encryption methods above can also be further classified into block encryption and stream encryption, where compression-combined encryption and non-compression encryption are discussed according to the relation between compression and encryption.

4.1 Full encryption

In the full encryption scheme shown as Fig.1, image as binary large objects or pixels are encrypted in their entirety. Full encryption can offer a high level of security, effectively prevent unauthorized access, and is widely used nowadays. For image encryption, full encryption is often operated without any compression process. Some algorithms have been proposed based on chaotic block ciphers, and some based on chaotic stream ciphers.

Fig. 1. The process of full encryption for a image

4.1.1 Algorithms based on chaotic block ciphers

A chaotic map based chaotic block cipher is a type of symmetric-key encryption algorithm that transforms a fixed-length group of plain-text bits into a group of ciphertext bits of the same length. The fixed-length group of bits is called a block, and the fixed length is the block size. A block cipher encryption algorithm for image might take (for example) a 128-bit block of plain-image as input, and output a corresponding 128-bit block of cipher-image, that is, a plain-image is encrypted block by block. Many algorithms of this kind have been proposed in (Cokal & Solak, 2009; Fridrich, 1997; Guan et al., 2005; Lian et al., 2005a;b; Mao et al., 2004; Salleh et al., 2003; Wang et al., 2011; Xiao et al., 2009). In this section, we just discuss the representative ones.

Fridrich (Fridrich, 1997) presented a symmetric block encryption technique based on two-dimensional chaotic map, such as the standard map, cat map and baker map shown in Equation 6, Equation 7 and Equation 8 (Lian et al., 2005b) (henceforth called B2CP). The B2CP, shown in Fig.2, consists of two parts: chaotic confusion and pixel diffusion, where the former process permutes a plain-Standard image with a two-dimensional chaotic map, and the latter process changes the value of each pixel one by one. In the confusion process, the parameters of the chaotic map serve as the confusion key. In addition, in the diffusion process, such parameters as the initial value or control parameter of the diffusion function serve as the diffusion key. However, security analysis are not efficiently given in their work. Lian et al (Lian et al., 2005b) studied the performance of Fridrich's algorithm and its security against statistical attack, known-plaintext attack, select-plaintext attack, and so on. Furthermore, they proposed some enhancement means to improve the focused cryptosystem, and gave some advices to select suitable chaotic map, diffusion function and iteration time.

$$\begin{cases} x_{j+1} = (x_j + y_j) \bmod N \\ y_{j+1} = (y_j + k \sin \frac{x_{j+1} N}{2\pi}) \bmod N \end{cases} \tag{6}$$

$$\begin{bmatrix} x_{j+1} \\ y_{j+1} \end{bmatrix} = \begin{bmatrix} 1 & u \\ v & uv+1 \end{bmatrix} \begin{bmatrix} x_j \\ y_j \end{bmatrix} (\mathrm{mod} N) \tag{7}$$

$$\begin{cases} x_{j+1} = \frac{N}{k_i}(x_j - N_i) + y_j \bmod \frac{N}{k_i} \\ y_{j+1} = \frac{k_i}{N}(y_j - y_j \bmod \frac{N}{k_i}) + N_i \end{cases} \text{with} \begin{cases} k_1 + k_2 + \cdots + k_t = N \\ N_i = k_1 + k_2 + \cdots + k_{i-1} \\ N_i \le x_j < N_i + k_i \\ 0 \le y_j \le N \end{cases} \tag{8}$$

Mao et al (Mao et al., 2004) proposed a three-dimensional chaotic baker map based image encryption scheme (henceforth called BCBP), which contains confusion and diffusion stage, and aims to obey traditional block cipher's principles. In BCBP (see Fig.3), the standard two-dimensional baker map is first extended to be three-dimensional, and then it is used to speed up image encryption while retaining its high degree of security. Comparing with

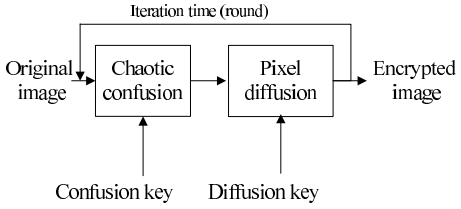


Fig. 2. The image encryption scheme in (Fridrich, 1997)

existing similar schemes which are designed on the two-dimensional baker map, the BCBP has higher security and faster enciphering/deciphering speeds, which makes it a very good candidate for real-time image encryption applications.

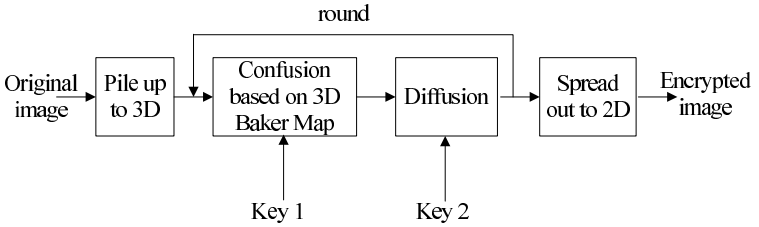


Fig. 3. The image encryption scheme in (Mao et al., 2004)

Lian et al (Lian et al., 2005a) proposed a block image cipher, which is composed of three parts: a chaotic standard map based corner-pixels confusion process which consists of the random-scan process and the chaotic permutation process, a diffusion function realized by a logistic map (Su et al., 2009) (see Equation 9) based diffusion function that spreads changes from one pixel to another, and a chaotic skew tent map (see Equation 10) (Brock, 1986) based key generator, which are used to generate the keys of the confusion process, the random-scan process and the diffusion process, respectively (henceforth called BCDG). The BCDG is of high key-sensitivity, and high security against brute-force attack, statistical attack and differential attack.

$$x_{j+1} = 1 - \mu x_j^2 \tag{9}$$

$$x_{j+1} = \begin{cases} \frac{x_j}{h}, 0 < x_j \leq h \\ \frac{1-x_j}{1-h}, h < x_j \leq 1 \end{cases} \tag{10}$$

In the above three algorithms, chaotic confusion and pixel diffusion are operated separately, which makes the encryption algorithms require at least two image-scanning processes. Thus, these algorithms may waste time on image-scanning.

Wang et al (Wang et al., 2011) improved these algorithms and proposed a fast image encryption algorithm with combined permutation and diffusion (henceforth called BCPD). In BCPD (see Fig.4) , the image is first partitioned into blocks of 8×8 pixels. Then, the pseudorandom numbers, generated from the nearest-neighboring coupled-map lattices (NCML) shown as Equation 11 (Kaneko, 1989), are used to change the pixel values in the blocks. Meanwhile, the blocks are relocated according to the lattice values of the NCML. The generation of pseudorandom numbers from NCML can avoid time-consuming operations

such as multiplication and conversion from floating points to integers, which greatly increases the encryption speed. In addition, the combination of the permutation and diffusion stages makes the image scan required only once in each encryption round, which also improves the encryption speed. Besides, the algorithm can well resist brute-force attack, statistical attack, differential attack, known/chosen-plaintext attacks.

$$x_{n+1}(i) = (1-\varepsilon)f(x_n(i)) + \varepsilon f(x_n(i+1)) \tag{11}$$

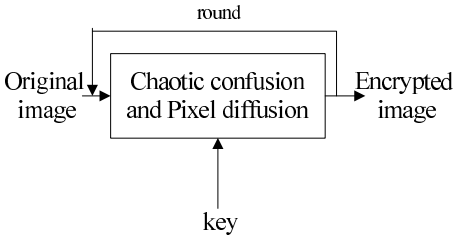


Fig. 4. The image encryption scheme in (Wang et al., 2011)

4.1.2 Algorithms based on chaotic stream ciphers

A chaotic stream cipher is a pseudorandom cipher bit stream (keystream) generated by a chaotic map, which is used to encrypt a plaintext bit by bit (typically by an XOR operation). For image, many algorithms have been proposed (Chen et al., 2004; Gao et al., 2006; Gao & Chen, 2008a;b; Kwok & Tang, 2007; Zhang et al., 2005).

Chen et al (Chen et al., 2004) designed a fast and secure symmetric image encryption scheme based on 3D cat map (see Fig.5) (henceforth called S3CP). In S3CP, 3D cat map is employed to shuffle the positions (and, if desired, grey values as well) of pixels in the image, and a chaotic logistic map based diffusion process among pixels is performed to confuse the relationship between cipher-image and plain-image. Besides, Chen's chaotic system (see Equation 12) (Chen & Ueta, 1999) is employed in key scheming to generate a binary sequence of 128 bits, which guarantees the high security of S3CP.

$$\begin{cases} \dot{x} = a(y-x) \\ \dot{y} = (c-a)x - xz + cy \\ \dot{z} = xy - bz \end{cases} \tag{12}$$

Gao and Chen proposed two image encryption algorithms in (Gao & Chen, 2008a;b)

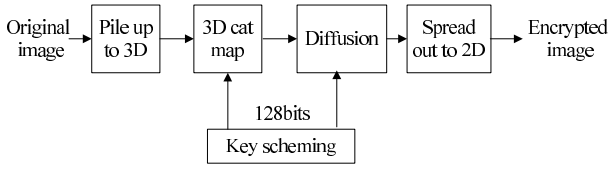


Fig. 5. The image encryption scheme in (Chen et al., 2004)

(henceforth called SGC). In both papers they shuffled the image based on total image shuffling matrix generated by using logistic map, then encrypted the shuffled image with a keystream generated from one or two chaotic systems. The difference between the two encryption schemes is that in (Gao & Chen, 2008a) the keystream is generated by the systems of both Lorenz (see Equation 13) and Chen (see Equation 12) (Chen & Ueta, 1999), while in (Gao & Chen, 2008b) it is generated only by one hyper-chaotic system (see Equation 14). However, researchers in (Rhouma & Belghith, 2008) and (Arroyo & C. Li, 2009) point out that the two algorithms present weakness, and a chosen-plaintext attack and a chosen-ciphertext attack can be done to recover the ciphered-image without any knowledge of the key value.

$$\begin{cases} \frac{dx}{dt} = \sigma(y - x) \\ \frac{dy}{dt} = rx - zx - y \\ \frac{dz}{dt} = xy - bz \end{cases} \tag{13}$$

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) \\ \dot{x}_2 = -x_1 x_3 + dx_1 + cx_2 - x_4 \\ \dot{x}_3 = x_1 x_2 - bx_3 \\ \dot{x}_4 = x_1 + k \end{cases} \tag{14}$$

Zhang et al (Zhang et al., 2005) applied discrete exponential chaotic map in image encryption (henceforth called SDEC). In SDEC, shown in Fig.6, a permutation of the pixels of plain-image is designed, and "XOR plus mod" operation is used. Besides, time varied-parameter piece-wise linear map (TVPPLM) (Qiu & He, 2002) is chosen to generate keystream, which may resist statistic attack, differential attack, and linear attack.

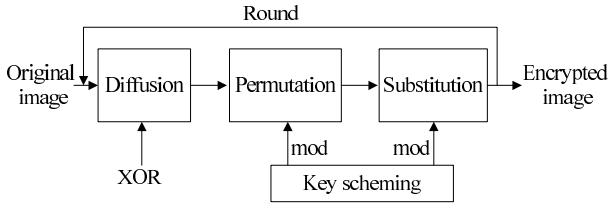


Fig. 6. The image encryption scheme in (Zhang et al., 2005)

Kwok and Tang (Kwok & Tang, 2007) proposed a fast image encryption system based on high-dimensional chaotic maps with finite precision representation (henceforth called SFPR). The core of the encryption system is a pseudo-random keystream generator formed by two chaotic maps (a skewed tent map and high-dimensional cat map), which not only achieves a very fast throughput, but also enhances the randomness even under finite precision implementation. Their experiments show that the SFPR is of high speed, high security, and can be applied in fast real time encryption applications.

Gao et al (Gao et al., 2006) presented an image encryption algorithm based on a new nonlinear chaotic algorithm (see Equation 15) (henceforth called SNCA) which uses power function and tangent function instead of linear function. In addition, the SNCA is a one-time-one password system, that is, it encrypts image data with different keys for different images. Thus the SNCA

is secure against statistic attack, brute-force attack, and chosen/known-plaintext attacks.

$$x_{n+1} = \lambda \cdot tg(\alpha x_n)(1 - x_n)^{\beta} \tag{15}$$

Apart from the aforementioned algorithms, there are many other researchers doing the image encryption algorithms based on chaotic stream ciphers, such as Wong (Wong et al., 2009), Tong (Tong & Cui, 2008), Li (Li et al., 2009), Socek (Socek et al., 2005), and so on.

4.2 Partial encryption

Partial encryption, which is also called selective encryption, only encrypts part of the data. As shown in Fig.7, a plain-image is partitioned into two parts: sensitive data and insensitive data. Only the sensitive data are encrypted, and the other is unprotected.

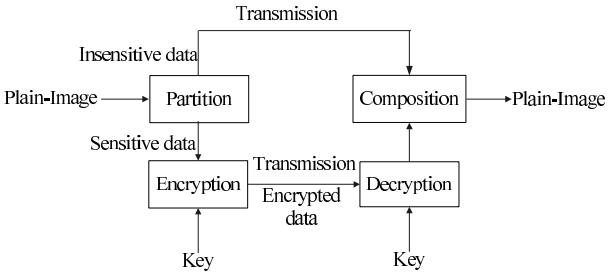


Fig. 7. The process of partial encryption for a image

Considering that image encryption emphasizes on content protection, the focused problem is how to select sensitive data, which is highly sensitive to the understandability of an image. Researchers have proposed many encryption algorithms, such as (Cheng & Li, 2000; Droogenbroeck & Benedett, 2002; Pommer & Uhl, 2003). However, these algorithms are mostly non-chaotic except (El-Khamy et al., 2009; Lian et al., 2004; Lin, Mao & Wang, 2008; Xiang et al., 2007), which are all based on chaotic stream ciphers.

Lian et al (Lian et al., 2004) proposed a partial image encryption algorithm by combining chaotic neural networks with JPEG2000 codec (henceforth called PCNN), which is a compression-combined encryption scheme. In PCNN, sensitive bitstreams, the subband with the lowest frequency, the significant bit-planes, and the cleanup pass, are selected from different subbands, bit-planes or encoding-passes. Besides, they are encrypted by a chaotic sequence in a chained encryption mode. The PCNN is secure against brute-force attack, known-plaintext attack or replacement attack. Additionally, it is time-efficient, does not change compression ratio, supports direct bit-rate control, and keeps the original error-robustness.

Xiang et al (Xiang et al., 2007) proposed a partial gray-level image encryption scheme based on a one-way coupled map lattice (CML, see Equation 16) (henceforth called PCML). The PCML first splits each pixel of image into $n(n < 8)$ significant bits and $(8 - n)$ less significant bits, and then only encrypts the n significant bits by the key-stream generated from CML, which is based on a chaotic skew tent map. The PCML is secure when $n = 4$. However, for an image which has a high correlation between adjacent pixels, the PCML is not secure and can not

resist known-plaintext attack. Besides, as PCML is a non-compression encryption, it can not keep compression ratio and format compliance.

$$x_{t+1}^{i} = (1-\varepsilon)g(x_t^i) + \varepsilon g(x_t^{i-1}) \tag{16}$$

Lin et al (Lin, Mao & Wang, 2008) presented a partial image encryption scheme based on a chaotic skew tent map (henceforth called PSTP). The PSTP integrates chaotic encryption into the process of bit stream generation by an SPIHT (Set Partitioning In Hierarchical Tree) encoder. As structure bits are used for synchronizing the encoding and the decoding in the construction of spatially oriented tree, and more sensitive than the data bits, they are only encrypted so that only few overheads are introduced to the image coder. Meanwhile, the PSTP has good key sensitivity and can well resist the brute-force attack and the known-plaintext attack. However, as PSTP encrypts the format information, it may change the image format.

El-Khamyl et al (El-Khamy et al., 2009) proposed a partial image encryption scheme based on discrete wavelet transform (DWT) and ELKNZ chaotic stream cipher (El-Zein et al., 2008) (henceforth called PDEC, shown in Fig.8). In PDEC, the image first goes through a single-level 2-dimensional discrete wavelet transform (2D DWT) resulting in four coefficient matrices: the approximation (*ca*), horizontal (*ch*), vertical (*cv*), and diagonal (*cd*) matrices. Only *ca* matrix, as the lowest frequency sub-band of the image, is encrypted using the ELKNZ cipher, and the other sub-bands ch, cv, cd are scrambled. The encrypted *ca* matrix and the scrambled ch, cv, cd matrices then undergo 2D inverse discrete wavelet transform (2D IDWT) to produce the encrypted image. The PDEC can provide complete perceptual encryption in the spatial and transform domains, and it is secure against known/chosen plaintext attacks.

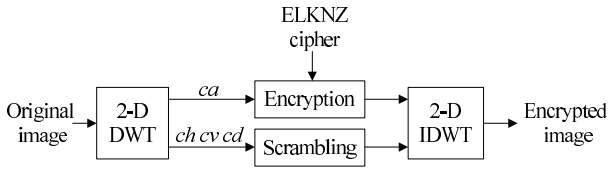


Fig. 8. The image encryption scheme in (El-Khamy et al., 2009)

4.3 Performance comparison

In this section, we compare the performance of different image encryption algorithms mentioned in Section 4.1 and 4.2. Here, various aspects listed in Section 2 are considered, and contrast results are shown in Table 1.

From Table 1, we conclude as follows:

(1) No matter chaos-based image encryption algorithms belong to full encryption or partial encryption, they can guarantee large key space and high key sensitivity, which make them resist brute-force attack. And they can confuse the pixels of an image completely so that the encrypted image is not perceptual recognized, that is, they are secure against ciphertext-only attack.

(2) As full encryption algorithms encrypt an image entirely and treat each bits equally, they have higher computational complexity than partial encryption, and do not provide

	BFA	KPA	CPA	COA	DA	CC	ICR	FC	RT	MLS	TET
B2CP (Fridrich, 1997)	Y	Y	Y	Y	N	H	N	N	N	N	N
BCBP (Mao et al., 2004)	Y	Y	Y	Y	Y	H	N	N	Y	N	Y
BCDG (Lian et al., 2005a)	Y	N	N	Y	Y	H	N	N	N	N	N
BCPD (Wang et al., 2011)	Y	Y	Y	Y	Y	H	N	N	Y	N	N
S3CP (Chen et al., 2004)	Y	N	N	Y	Y	M	N	N	Y	N	N
SGC (Gao & Chen, 2008a;b)	Y	Y	N	Y	N	M	N	N	Y	N	N
SDEC (Zhang et al., 2005)	Y	N	N	Y	Y	M	N	N	N	N	Y
SFPR (Kwok & Tang, 2007)	Y	Y	Y	Y	N	M	N	N	Y	N	N
SNCA (Gao et al., 2006)	Y	Y	Y	Y	N	M	N	N	Y	N	N
PCNN (Lian et al., 2004)	Y	Y	N	Y	Y	L	Y	Y	Y	N	Y
PCML (Xiang et al., 2007)	Y	N	N	Y	N	L	N	N	N	N	N
PSTP (Lin, Mao & Wang, 2008)	Y	Y	N	Y	N	L	Y	N	N	N	N
PDEC (El-Khamy et al., 2009)	Y	Y	Y	Y	N	L	N	N	N	N	N

BFA: against brute-force attack; KPA: against known-plaintext attack
CPA: against chosen-plaintext attack; COA: against ciphertext-only attack
DA: against differential attack; CC: computational complexity; FC: format compliance
ICR: invariance of compression ratio; RT: real-time
TET: transmission error tolerance; MLS: multiple levels of security
Y: yes; N: no; L: low; M: middle; H: high

Table 1. Comparison of chaos-based image encryption algorithms

multiple levels of security. Moreover, they are often operated with any compression process, so they can not keep invariance of compression ratio and format compliance.

(3) If an encryption scheme (such as PCNN) is combined with image compression or coding process, as it only encrypts a small part of image data and does not change statistical characteristics of DCT coefficients, it can keep invariance of compression ratio. Moreover, since it does not encrypt any format information, it can keep format compliance.

(4) Although the block cipher is usually considered faster than stream cipher, it may provide worse security than stream cipher.

(5) Different chaotic maps have different key space, key sensitivity and computational complexity. For example, Table 2 lists the differences among cat map, baker map and standard map. Comparing to cat map and standard map, baker map has the lowest computational complexity, middle key space, and middle key sensitivity. Thus, baker map is preferred as a tradeoff between security and computing complexity.

(6) Although the above image encryption algorithms can not fulfill all the requirements listed in Section 2, they still provide very promising methods that can demonstrate superiority over the conventional encryption methods.

	cat map	baker map	standard map
key space	L	M	H
key sensitivity	H	M	L
computational complexity	M	L	H

Table 2. The differences among cat map, baker map and standard map

5. Chaos-based video encryption algorithms

According to the relation between compression process and encryption, this section partitions chaos-based video encryption algorithms into three types: encrypting the raw video data, encrypting the video data in compression process, and encrypting the compressed video data. As to encrypting the video data in compression process, it means realizing encryption in the encoding process before entropy coding. Encrypting the compressed video data means realizing encryption after entropy-encoding and before package.

5.1 Encrypting the raw video data

In the type of encrypting the raw video data, some algorithms encrypt the raw data completely without considering region-of-interest, and others consider the region-of-interest partially or selectively.

5.1.1 Encryption without considering region-of-interest

Encryption without considering interest regions means to encrypt the video data frame by frame and does not consider the video objects or any other semantic information. Thus, it treats the regions fairly without special considerations.

Li et al (Li et al., 2002) proposed a chaotic video encryption scheme (CVES) for real-time digital video based on multiple digital chaotic systems. In CVES, each plain-block is first XORed by a chaotic signal, and then substituted by a pseudo-random S-box based on multiple chaotic maps. The CVES is secure against brute-force attack, known/chosen-plaintext attacks. Moreover, it is of low computational complexity, and thus it can be realized easily by both hardware and software.

Ganesan et al (Ganesan et al., 2008) described a public key encryption (PKVE) of videos based on chaotic maps. In PKVE, if the number of frames is too large, they first use phase scrambling (see Fig.9) (Nishchal et al., 2003) to scramble the video data, and then encrypt the data using chebyshev maps (Bergamo et al., 2005) (see Equation 17). Otherwise, they encrypt each frame by Arnold scrambling (Prasad, 2010). The PKVE is secure against known/chosen-plaintext attacks, and has high key sensitivity. In particular, it is very efficient in real-time applications for 64×64 and 128×128 pixel size videos.

$$\begin{cases} T_n(x) = 2 \cdot x \cdot T_{n-1}(x) - T_{n-2}(x), n \geq 2 \\ T_0(x) = 1 \\ T_1(x) = x \end{cases} \tag{17}$$

Kezia and Sudha (Kezia & Sudha, 2008) used a high dimensional Lorenz chaotic system to

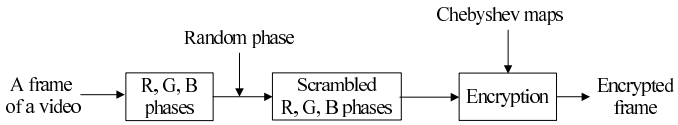


Fig. 9. The video encryption scheme in(Ganesan et al., 2008)

encrypt each frame of a video by confusing the position of the pixels (henceforth called LCVS).

In LCVS, each frame is encrypted by a unique key instead of changing the key for a particular number of frames. The LCVS can resist brute-force attack and differential attack, and it is robust to transmission error and much suitable for real-time transmission.

5.1.2 Encryption considering regions-of-interest

In many practical applications, it is not necessary or suitable to encrypt all video data, while just regions of interest. For the video data, a region of interest means human video objects or any other kind of regions of semantic information. In this issue, researchers have proposed some encryption algorithms according to the mode shown in Fig.10.

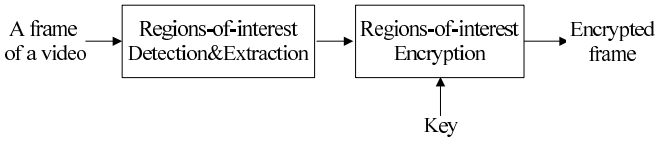


Fig. 10. The encryption mode considering regions-of-interest

Tzouveli et al (Tzouveli et al., 2004) proposed a human video object encryption system (henceforth called HVOE) based on logistic map. In HVOE, face regions are first efficiently detected, and afterwards body regions are extracted using geometric information of the location of face regions. Then, the pixels of extracted human video objects are encrypted based on logistic map. The HVOE can resist brute-force attack, different-key attack and differential attack, and it is efficient in computational resources and running time.

Ntalianis and Kollias (Ntalianis & Kollias, 2005) proposed a video object based chaotic encryption system (henceforth called VOCE). First, in VOCE video objects are automatically extracted based on the appropriate fusion of color information. Next, for each video object, multi-resolution decomposition is performed and the pixels of the lowest resolution level are encrypted using a complex product cipher combining a chaotic stream cipher and two chaotic block ciphers. Finally, the encrypted regions are propagated to the higher resolution levels and the encryption process is repeated until the highest level is reached. The VOCE presents robustness against brute-force attack and known cryptanalytic attack.

5.2 Encrypting the video data in compression process

Encrypting the video data in compression process means realizing encryption in the encoding process before entropy coding, such as Context-adaptive variable-length coding (CAVLC), Context-adaptive binary arithmetic coding (CABAC), variable length coding (VLC), run length coding (RLC), Golomb, Huffman, and so on. This section just discusses the most representative schemes for MPEG or H.26x.

Yang and Sun (Yang & Sun, 2008) proposed a chaos-based video encryption method in DCT domain (henceforth called CVED). In CVED, only I-frames are selected as encryption objects. First, they use a double coupling logistic maps (see Equation 18) to scramble the DCT coefficients of I-frames, and then encrypt the DCT coefficients of the scrambled I-frames by using another logistic map (see Equation 9). In CVED, five keys are introduced in the whole process, and thus the key space is large enough to resist brute-force attack. Besides,

only encrypting the DCT coefficients of I-frames consumes little time, and is feasible for real-time applications. However, considering that there are some macro blocks in B-frames or P-frames, which are encoded without referring to I-frames, these blocks will be left unprotected. Therefore, some video contents may be intelligible and the CVED is not secure enough.

$$\begin{cases} x_{n+1} = \mu_x x_n (1 - x_n) \\ y_{n+1} = \mu_y y_n (1 - y_n) \end{cases} \tag{18}$$

Lian (Lian, 2009) constructed an efficient chaos-based selective encryption scheme for image/video (henceforth called CSVE) shown in Fig.11. In CSVE, only the DC (direct current coefficient) and the ACs (signs of the alternating current coefficients) of each frame are encrypted using the 2D coupled map lattice (2D CML). The encryption is operated after pre-encoding (namely, color space transformation), block partitioning (each block is in 8×8 size), DCT transformation and quantization, and before post-encode (i.e., zig-zag scan and VLC). The CSVE has high key sensitivity and is secure in perception. Moreover, its encryption operation does not change the compression ratio a lot, and incurs little computational cost compared with video compression. The cryptographic security of CSVE depends on the randomness of the chaotic sequences generated by the 2D coupled map lattice.

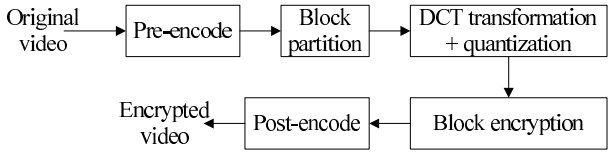


Fig. 11. The video encryption scheme in (Lian, 2009)

Chiaraluce et al (Chiaraluce et al., 2002) presented a selective encryption algorithm for the H.263 videos (henceforth called SEHV), in which the cipher operations have been seamlessly integrated into the H.263 encoding process, i.e., before RLC and packaging. In SEHV, only the most significant bit in the DC coefficients of DCT , the AC coefficients of I-MB (intra macro blocks), the sign bit of the AC coefficients of the PMB (predicted macro blocks), and the sign bit of the motion vectors are encrypted by using three suitably arranged different chaotic functions, namely, the skew tent map, saw-tooth likewise map, and logistic map. The key space (2^{512}) of SEHV is large enough to resist brute-force attack. The SEHV changes the key every 30 frames, and thus it is secure against known/chosen-plaintext attacks. Besides, it introduces a modest additional processing time and is suitable for "real time" or "almost real time" applications.

5.3 Encrypting the compressed video data

Encrypting the compressed video data means realizing encryption after entropy-encoding and before package (shown as Fig.12.). The representative works are done by Lian et al (Lian, Liu, Ren & Wang, 2007; Lian, Sun & Wang, 2007) and Qian et al (Qian et al., 2008).

Lian et al (Lian, Sun & Wang, 2007) proposed an efficient partial video encryption scheme based on a chaotic stream cipher generated by a discrete piecewise linear chaotic map (henceforth called VESC). In VESC, both the intra-macroblocks (all the macroblocks in I-frame and some intra-encoded macroblocks in P/B-frame) and the motion vectors' signs are

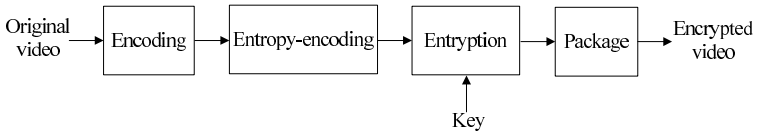


Fig. 12. The mode of encrypting the compressed video data

encrypted, and the encryption process is achieved after VLC and before packaging. The VECS has large key space, and high key sensitivity. Besides, it can keep invariance of compression ratio, format compliant and is robust to transmission error.

In (Lian, Liu, Ren & Wang, 2007), Lian et al proposed a fast video encryption scheme for MPEG-4 (henceforth called VEM4). In VEM4, the file format information, such as file header, packet header, and so on, are left unencrypted in order to support such operation as bit-rate control, and the motion vectors, subbands, code blocks or bit-planes are partially encrypted by a stream cipher based on a modified chaotic neural network (Lian et al., 2004). Moreover, for each encoding-pass, the chaotic binary sequence is generated from different initial-condition based on logistic map. Thus, if one encoding-pass cannot be synchronized because of transmission errors, the other ones can still be decrypted correctly. The VEM4 is of high security in perception, of low computation complexity, and secure against brute-force attack, statistic attack or differential attack. It keeps compression ratio and file format unchanged, supports direct bit-rate control, and keeps the error-robustness unchanged.

Qian et al (Qian et al., 2008) proposed a multiple chaotic encryption system (MCES) for MPEG-2. In MCES, three chaotic or hyperchaotic maps, namely logistics map, 2-D baker map and 4-D hyperchaotic map (Li et al., 2005), are introduced for stream partial encryptions, block permutation, confusion after block permutation, respectively. Moreover, stream ciphers encrypt only DC coefficients. The MCES is secure, efficient, of low computational complexity, and nearly brings no data expansion.

5.4 Performance comparison

In this section, we compare the performance of different encryption algorithms mentioned above. Here, various aspects listed in Section 2 are considered, and contrast results are shown in Table 3.

From Table 3, we get the following conclusions:

(1) The CVES, PKVE and LCVS encrypt the video data completely without considering interest regions. Their security depends on the proposed chaotic ciphers, and as long as the ciphers are well-designed, they are often of higher security and higher complexity than other types, and thus are more suitable for secure video storing.

(2) The HVOE and VOCE encrypt only the regions of interest, and leave the rest (such as background) unprotected. They are of lower computation complexity, and more suitable for real-time applications. Their cryptographic security depends on the adopted chaotic cipher and the region selection.

(3) The algorithms that encrypt the video data in compression process belong to partial or selective encryption, and are often of lower complexity than those encrypt the raw video data directly. However, some of them, such as CVED and SEHV, change the compression

	BFA	KPA	CPA	COA	DA	CC	ICR	FC	RT	MLS	TET
CVES (Li et al., 2002)	Y	Y	Y	Y	N	M	N	N	Y	N	N
PKVE (Ganesan et al., 2008)	Y	Y	Y	Y	N	H	N	N	Y	N	N
LCVS (Kezia & Sudha, 2008)	Y	N	N	Y	Y	M	N	N	Y	N	N
HVOE (Tzouveli et al., 2004)	Y	N	N	Y	Y	L	N	N	Y	N	N
VOCE (Ntalianis & Kollias, 2005)	Y	N	N	Y	N	L	N	N	Y	Y	Y
CVED (Yang & Sun, 2008)	Y	N	N	N	N	L	N	Y	Y	N	N
CSVE (Lian, 2009)	Y	N	N	Y	N	L	Y	Y	Y	N	N
SEHV (Chiaraluce et al., 2002)	Y	Y	Y	Y	N	L	N	Y	Y	N	N
VESC (Lian, Sun & Wang, 2007)	Y	N	N	Y	N	L	Y	Y	Y	N	Y
VEM4 (Lian, Liu, Ren & Wang, 2007)	Y	N	N	Y	Y	L	Y	Y	Y	N	Y
MCES (Qian et al., 2008)	Y	N	N	Y	N	L	Y	Y	Y	N	N

Table 3. Comparison of chaos-based video encryption algorithms

ratio because they change the statistical characteristics of DCT coefficients. Interestingly, some of them can keep file format unchanged, and thus support direct bit rate control, that is, they permit to re-compress the encoded and encrypted video before decrypting it firstly, and save much time for secure transcoding. Therefore, they are more suitable for real-time applications, such as wireless multimedia network or multimedia transmission over narrow bands.

(4) The algorithms that encrypt the compressed video data can not only preserve invariance of compression ratio and format compliance, but also be of low overhead. Additionally, they are of low-cost and easy to be realized, and thus are suitable for real-time required applications, such as video transmission or video access. However, as the video stream after entropy encoding may have a certain structure or syntax, they may destroy the structure of the video stream, furthermore, they may bring error spreading when the transmission error happens because they do not consider the rules of package before transmission.

6. Chaos-based audio encryption algorithms

Comparing to image and video, the work for audio or speech encryption is sadly lacking at present. Therefore, this section will deal with not only the chaos-based methods, but also other audio encryption technologies. In general, according to the percentage of the audio data encrypted, the existing audio encryption algorithms are mostly divided into full encryption and partial encryption.

6.1 Full encryption

For full encryption, there are two fundamentally distinct approaches to achieve audio security: analogue audio encryption and digital audio encryption.

6.1.1 Analogue audio encryption

Analogue audio encryption contains four main categories, namely, frequency domain scrambling, time domain scrambling, two-dimensional scrambling which combines the frequency domain scrambling with the time domain scrambling, and amplitude scrambling.

Sridharan et al (Sridharan et al., 1990; 1991) and Borujeni (Borujeni, 2000) proposed scrambling approach using orthogonal transformation like discrete fourier transform (DFT), fast fourier transform (FFT), DCT, respectively. Lin et al (Lin et al., 2005) proposed a modified time domain scrambling scheme with an amplitude scrambling method, which masks the speech signal with a random noise by specific mixing. Andrade et al (Andrade et al., 2008) presented a two-dimensional scrambling method combining the frequency domain scrambling with the time domain scrambling for AMR (adaptive multi-rate) speech. Sadkhan et al (Sadkhan et al., 2007) proposed analog speech scrambler based on parallel structure of wavelet transforms.

Mosa et al (Mosa et al., 2009) proposed a chaos based speech encryption system in transform domains (henceforth called SETD). The SETD consists of two stages: substitution and permutation. First, the stream of speech segments is divided and reshaped into two fixed size blocks and the elements are permutated by chaotic map technique, then substituted to different values by DCT and then permutated another time. The SETD is of low-complexity, and secure against brute-force attack, statistical attack and noise attack.

These analogue audio encryption techniques are simple and have following advantages (Sridharan et al., 1990):

- they provide excellent voice recognition or voice recovery.
- The quality of the recovered speech is independent of the language and speaker.
- It is possible to acoustically couple the encryption device to the handset which enables the device to be used with any handset.
- The system does not require speech compression or modems.
- The system is less sensitive to errors in synchronization.
- The system generates scrambled speech without any residual intelligibility.

However, these techniques do not change the redundancy of speech greatly, which leads to the intelligibility of the encrypted analog signal, and thus analogue audio encryption has poor security.

6.1.2 Digital audio encryption

In digital encryption, the analogue signal is first digitised and compressed to generate a data signal at a suitable bit rate. The bit stream is then encrypted.

Gnanajeyaraman et al (Gnanajeyaraman et al., 2009) proposed an audio encryption scheme (shown in Fig.13) based on a look-up table which is generated by using higher dimensional cat map (henceforth called AELT). The AELT has the characteristic of sensitive to initial condition, and resists brute-force attack and chosen/known-plaintext attacks.

Liu et al (Liu et al., 2008) proposed a block encryption algorithm for digital speech codes (henceforth called BEDS). The BEDS encrypts message with chaotic sequences which randomly come from chaotic model database using logistic map (see Equation 9) and henon map (see Equation 19). The BEDS has large key space, and partially solves the problem of decryption for receiver when some data packages are lost during real-time transportation.

$$\begin{cases} x_{i+1} = 1 + by_i - ax_i^2 \\ y_{i+1} = x_i \end{cases} \tag{19}$$

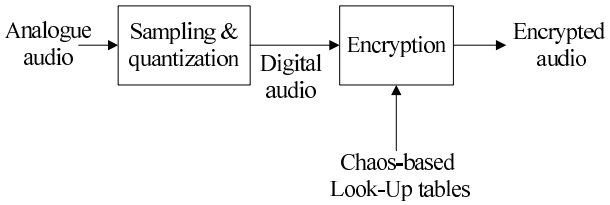


Fig. 13. The audio encryption scheme in (Gnanajeyaraman et al., 2009)

Sheu (Sheu, 2011) presented a two-channel chaos-based speech encryption using fractional Lorenz system for speech communication (henceforth called TCSE). The TCSE can achieve large key space, high key sensitivity, and the ability to resist chosen plaintext/ciphertext attack.

Full encryption can offer a high level of security and effectively prevent unauthorized access, however, is computationally demanding, and not effectively applied to power-constrained, real-time multimedia applications.

6.2 Partial encryption

Partial encryption, which is often operated on a certain audio coding standard, such as G.723, G.729 and MP3, only encrypts the sensitive subset of an audio data.

Wu and Kuo (Wu & Kuo, 2001) presented a fast selective encryption method for G.723 (henceforth called FSEM), where the most significant 37 bits of all important coefficients are encrypted. As the FSEM does not select any of the pulse position coefficients, it can be applied directly to bit rate modes. Moreover, it distorts speech totally, and is secure against ciphertext-only attack, brute-force attack, known/chosen-plaintext attacks.

Servetti and Martin (Servetti & Martin, 2002) proposed a perception based partial encryption scheme for G.729 (henceforth called LPPE). In LPPE, speech signals are first partitioned into two classes based on perception, where the mostly perceptually relevant bits are encrypted and the others are left unprotected. The LPPE can achieve content protection which is equivalent to full encryption. However, there are still remaining some comprehensible bit steams structures which might leak some information for attackers and reduce security to an extent.

Servetti et al (Servetti et al., 2003) presented a frequency-selective partial encryption for MP3 (henceforth called FPEM). In FPEM, only a part of the stop-band coefficients are encrypted. The FPEM is combined with low-pass filtering in the compressed domain, which makes the FPEM against statistical attack and offers good content protection. Moreover, the FPEM is of low-complexity and format compliance.

Su et al (Su et al., 2010) improved the LPPE and presented a group of chaos-based hierarchical selective encryption schemes (henceforth called CHSE) which can obtain a good tradeoff between high security and low computational cost. In CHSE, speech bit streams are partitioned into two parts according to the bit sensitivity where the sensitive bits are encrypted by a strong cipher and the remaining are encrypted by a lightweight cipher.

6.3 Performance comparison

In this section, we just compare the performance of SETD, AELT, BEDS, TCSE, LPPE, CHSE, FPEM and FSEM. Here, various aspects listed in Section 2 are considered, and contrast results are shown in Table 4.

	BFA	KPA	CPA	COA	DA	CC	ICR	FC	RT	MLS	TET
SETD (Mosa et al., 2009)	Y	N	N	Y	N	M	N	N	N	N	N
AELT (Gnanajeyaraman et al., 2009)	Y	Y	Y	Y	N	H	N	N	N	N	N
BEDS (Liu et al., 2008)	Y	N	N	Y	N	H	N	N	Y	N	Y
TCSE (Sheu, 2011)	Y	N	Y	Y	N	H	N	N	N	N	N
FSEM (Wu & Kuo, 2001)	Y	Y	Y	Y	N	L	Y	Y	Y	N	N
LPPE (Servetti & Martin, 2002)	Y	N	N	Y	N	L	N	Y	Y	N	N
FPEM (Servetti et al., 2003)	Y	N	N	Y	N	L	N	Y	Y	N	N
CHSE (Su et al., 2010)	Y	Y	Y	Y	Y	L	Y	Y	Y	Y	N

Table 4. Comparison of audio encryption algorithms

From Table 4, we can we get the following conclusions:

(1) As partial encryption only encrypts a subset of audio data, it has lower computational complexity than full encryption. Thus, audio encryption algorithms of this category can be used to meet the real-time demand for power-constrained devices and narrow bandwidth environments.

(2) As partial encryption is generally used for compressed audio data, it can keep the audio format compliance.

(3) Compared with analogue encryption, digital encryption can give lower residual intelligibility and higher cryptanalytic strength, and thus it is the main technique for audio encryption at present. However, analogue encryption also has its advantage in analogue telephone, satellite and mobile communication systems without the use of a modem.

7. Conclusions

Multimedia encryption becomes more and more important with the development of network and multimedia technology in today's world. To tackle the problem, many encryption algorithms have been proposed. Although there does not seem to be any multimedia encryption algorithm that can fulfill all aforementioned requirements in Section 2, chaos-based multimedia encryptions provide a class of very promising methods which can demonstrate superiority over the conventional encryption methods and can be used as the foundation of future research. However, chaos-based multimedia encryption is not yet mature and more efforts are needed for its further development toward practical applications with high security, low computational complexity, invariance of compression ratio, format compliance, real-time, multiple levels of security, and strong transmission error tolerance.

8. References

Alligood, K. T., Sauer, T. & Yorke, J. A. (1997). *Chaos: an introduction to dynamical systems*, Springer-Verlag, New York.

Alvarez, G. & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems, *International Journal of Bifurcation and Chaos* Vol.16(No.7): 2129–2151.

Alvarez, G., Montoya, F., Romera, M. & Pastor, G. (2004). Breaking two secure communication systems based on chaotic masking, *IEEE Transaction on Circuit and Systems II: Express Briefs* Vol.51(No.10): 505–506.

Andrade, J., Campos, M. & Apolinario, J. (2008). Speech privacy for modern mobile communication systems, *Proceedings of IEEE Int. Conf. on Acoustics, Speech, and Signal Processing*, IEEE Press, Nevada, U.S.A., pp. 1777 – 1780.

Arroyo, D. & C. Li, S. Li, G. A. W. A. H. (2009). Cryptanalysis of an image encryption based on a new total shuffling algorithm, *Chaos, Solitons & Fractals* Vol.41(No.5): 2613–2616.

Ballesté, A. M. (2004). *Real-time pay-per-view of protected multimedia content v:2.0*, Ph.D. Dissertation, Universitat Polit'ecnica de Catalunya, Barcelona.

Bergamo, P., D'Arco, P. & Santis, A.and Kocarev, L. (2005). Security of public key cryptosystems based on chebyshev polynomials, *IEEE Transactions on Circuits and Systems-I* Vol.52: 1382–1393.

Borujeni, S. (2000). Speech encryption based on fast fourier transform permutation, *Proceedings of ICECS 2000*, IEEE Press, Jounieh , Lebanon, pp. 290 – 293.

Brock, W. A. (1986). Distinguishing random and deterministic systems: Abridged version, *Journal of Economic Theory* Vol.1986(No.40): 168–195.

Chen, G., Mao, Y. & Chui, C. K. (2004). A symmetric image encryption scheme based on 3d chaotic cat maps, *Chaos, Solitons & Fractals* Vol.21(No.3): 749–761.

Chen, G. & Ueta, T. (1999). Yet another chaotic attractor, *Int J Bifurcat Chaos* Vol.9(No.7): 1465–1466.

Cheng, H. & Li, X. (2000). Partial encryption of compressed images and videos, *IEEE Transactions on Signal Processing* Vol.48(No.8): 2439–2451.

Chiaraluce, F., Ciccarelli, L., Gambi, E., Pierleoni, P. & Reginelli, M. (2002). A new chaotic algorithm for video encryption, *IEEE Transactions on Consumer Electronics* Vol.48(No.4): 833–844.

Cokal, C. & Solak, E. (2009). Cryptanalysis of a chaos-based image encryption algorithm, *Phys. Lett. A* Vol.373(No.15): 1357–1360.

Cormen, T. H., Leiserson, C. E., Rivest, R. L. & Stein, C. (2001). *Introduction to algorithms (2nd edition)*, MIT Press, McGraw-Hill Cambridge.

Dang, P. P. & Chau, P. M. (2000). Implementation idea algorithm for image encryption, *Proceedings of SPIE*, SPIE Press, San Diego, CA, pp. 1–9.

Devaney, R. L. (2003). *An introduction to chaotic dynamical systems(2nd edition)*, Westview Press, San Francisco.

Droogenbroeck, M. & Benedett, R. (2002). Techniques for a selective encryption of uncompressed and compressed images, *Proceedings of ACIVS 2002*, IEEE Press, Ghent, Belgium, pp. 90–97.

El-Khamy, S., El-Nasr, M. & El-Zein, A. (2009). A partial image encryption scheme based on the dwt and elknz chaotic stream cipher, *MASAUM Journal of Basic and Applied Sciences* Vol.1(No.3): 389–394.

El-Zein, A., El-Khamy, S. & El-Nasr, M. (2008). The chaotic stream cipher "elknz" for high security data encryption, *Proceedings of URSIGA'2008*, URSI Press, Chicago, USA, pp. 1105–1110.

Fridrich, J. (1997). Image encryption based on chaotic maps, *Proceedings of IEEE Conf. on Systems, Man, and Cybernetics*, IEEE Press, Florida, USA, pp. 1105–1110.

Furht, B., Muharemagic, E. & Socek, D. (2005). *Multimedia encryption and watermarking*, Springer-Verlag, New York.

Ganesan, K., Singh, I. & Narain, M. (2008). Public key encryption of images and videos in real time using chebyshev maps, *Proceedings of the 2008 Fifth International Conference on Computer Graphics, Imaging and Visualisation*, IEEE Computer Society, Washington DC, USA, pp. 211–216.

Gao, H., Zhang, Y., Liang, S. & Li, D. (2006). A new chaotic algorithm for image encryption, *Chaos, Solitons & Fractals* Vol.29(No.2): 393–399.

Gao, T. & Chen, Z. (2008a). Image encryption based on a new total shuffing algorithm, *Chaos, Solitons and Fractals* Vol.1(No.38): 213–220.

Gao, T. & Chen, Z. (2008b). A new image encryption algorithm based on hyper-chaos, *Physics Letters A* Vol.372: 394–400.

Gnanajeyaraman, R., Prasadh, K. & Ramar, D. (2009). Audio encryption using higher dimensional chaotic map, *International Journal of Recent Trends in Engineering* Vol.1(No.2): 103–107.

Gschwandtner, M., Uhl, A. & Wild, P. (2007). Transmission error and compression robustness of 2d chaotic map image encryption schemes, *EURASIP Journal on Information Security* Vol.2007(No.1): 1–16.

Guan, Z., Huang, F. & Guan, W. (2005). Chaos-based image encryption algorithm, *Physics. Letters A* Vol.346(No.1-3): 153–157.

He, J., Qian, H., Zhou, Y. & Li, Z. (2010). Cryptanalysis and improvement of a block cipher based on multiple chaotic systems, *Mathematical Problems in Engineering* Vol.2010: 14 Pages.

Kaneko, K. (1989). Pattern dynamics in spatiotemporal chaos: pattern selection, diffusion of defect and pattern competition intermittency, *Physica D* Vol.34(No.1-2): 1ÍC41.

Kezia, H. & Sudha, G. F. (2008). Encryption of digital video based on lorenz chaotic system, *Proceedings of the 16th International Conference on Advanced Computing and Communications*, IEEE Computer Society, Tamilnadu India, pp. 40–45.

Kwok, H. & Tang, W. (2007). A fast image encryption system based on chaotic maps with finite precision represention, *Chaos, Solitons & Fractals* Vol.32(No.4): 1518–1529.

Li, C., Li, S., Chen, G. & Halang, W. A. (2009). Cryptanalysis of an image encryption scheme based on a compound chaotic sequence, *Image and Vision Computing* Vol.27(No.8): 1035–1039.

Li, S., Zheng, X., Mou, X. & Cai, Y. (2002). Chaotic encryption scheme for real-time digital video, *Proceedings of SPIE*, SPIE Press, San Jose, CA, pp. 149–160.

Li, Y. X., Tang, W. K. S. & Chen, G. R. (2005). Generating hyperchaos via state feedback control, *Int. J. of Bifurcation and Chaos* Vol.15(No.10): 3367–3375.

Lian, S. (2009). Efficient image or video encryption based on spatiotemporal chaos system, *Chaos, Solitons & Fractals* Vol.40(No.5): 2509–2519.

Lian, S., Chen, G., Cheung, A. & Wang, Z. (2004). chaotic-neural-network-based encryption algorithm for jpeg2000 encoded images, *Proceedings of ISNN 2004-II*, Springer-Verlag, Praha, Czech Republic, pp. 627–632.

Lian, S., Liu, Z., Ren, Z. & Wang, H. (2007). Secure media distribution scheme based on chaotic neural network, *Proceedings of ISNN 2007*, IEEE Computational Intelligence Society, Nanjing, China, pp. 79–87.

Lian, S., Sun, J., Liu, G. & Wang, Z. (2008). Efficient video encryption scheme based on advanced video coding, *Multimed Tools Appl* Vol.38(No.1): 75–89.

Lian, S., Sun, J. & Wang, Z. (2005a). A block cipher based on a suitable use of chaotic standard map, *Chaos, Solitons & Fractals* Vol.26(No.1): 117–129.

Lian, S., Sun, J. & Wang, Z. (2005b). Security analysis of a chaos-based image encryption algorithm, *Phys Lett A* Vol.351(No.2-4): 645–661.

Lian, S., Sun, J. & Wang, Z. (2007). A chaotic stream cipher and the usage in video protection, *Chaos, Solitons & Fractals* Vol.34(No.1): 851–859.

Lin, C., Chung, C. & Chen, Z. (2008). A chaos-based unequal encryption mechanism in wireless telemedicine with error decryption, *Wseas Transactions On Systems* Vol.7(No.2): 75–89.

Lin, Q., Yin, F. & Liang, H. (2005). Blind source separation-based encryption of images and speeches, *Lecture Notes in Computer Science-Advances in Neural Networks* Vol.3497: 544–549.

Lin, R., Mao, Y. & Wang, Z. (2008). Chaotic secure image coding based on spiht, *Proceedings of ChinaCom 2008*, IEEE press, Hangzhou, China, pp. 149–160.

Liu, J., Gao, F. & Ma, H. (2008). A speech chaotic encryption algorithm based on network, *Proceedings of IIHMSP '08*, IEEE press, Harbin, China, pp. 283–286.

Mao, Y., Chen, G. & Lian, S. (2004). A novel fast image encryption scheme based on the 3d chaotic baker map, *Int J Bifurcat Chaos* Vol.14(No.10): 3613–3624.

Mosa, E., Messiha, N. & Zahran, O. (2009). Chaotic encryption of speech signals in transform domains, *Proceedings of ICCES 2009*, IEEE Press, Cairo, pp. 300–305.

Nishchal, N. K., Joseph, J. & Singh, K. (2003). Fully phase based encryption using fractional fourier transform, *Opt.Eng* Vol.42: 1583–1588.

Ntalianis, K. S. & Kollias, S. D. (2005). Chaotic video objects encryption based on mixed feedback, multiresolution decomposition and time-variant s-boxes, *Proceedings of ICIP (2) 2005*, IEEE press, Genoa, Italy, pp. 1110–1113.

Pommer, A. & Uhl, A. (2003). Selective encryption of wavelet-packet encoded image data: efficiency and security, *Multimedia Systems* Vol.9(No.3): 279–287.

Prasad, V. V. R.and Kurupati, R. (2010). Secure image watermarking in frequency domain using arnold scrambling and filtering, *Advances in Computational Sciences and Technology* Vol.3(No.2): 236–244.

Qian, Q., Chen, Z. & Yuan, Z. (2008). Video compression and encryption based-on multiple chaotic system., *the 3rd International Conference on Innovative Computing Information and Control*, IEEE computer society, Washington, DC, USA, pp. 561–564.

Qiu, Y. & He, C. (2002). Construction and analysis of one class chaotic running key generator, *J Shanghai Jiaotong Univ* Vol.136(No.3): 344–347.

Rhouma, R. & Belghith, S. (2008). Cryptanalysis of a new image encryption algorithm based on hyper-chaos, *Phys. Lett. A* Vol.372(No.38): 5973–5978.

Rueppel, R. A. (1986). *Analysis and design of stream ciphers*, Springer-Verlag, New York.

Sadkhan, S., Abdulmuhsen, N. & Al-Tahan, N. (2007). A proposed analog speech scrambler based on parallel structure of wavelet transforms, *Proceedings of NRSC 2007*, IEEE Press, Cairo, pp. 1–12.

Salleh, M., Ibrahim, S. & Isnin, I. F. (2003). Image encryption algorithm based on chaotic mapping, *Jurnal Teknologi* Vol.39(No.D): 1–12.

Servetti, A. & Martin, J. (2002). Perception-based partial encryption of compressed speech, *IEEE Transactions on Speech and Audio Processing* Vol.10(No.1): 637–643.

Servetti, A., Testa, C. & Martin, J. (2003). Frequency-selective partial encryption of compressed audio, *Proceedings of ICASSP '03*, IEEE Press, Hongkang, China, pp. 668–671.

Sheu, L. (2011). A speech encryption using fractional chaotic systems, *Nonlinear Dyn* Vol.65(No.1-2): 103–108.

Socek, D., Li, S., Magliveras, S. & Furht, B. (2005). Enhanced 1-d chaotic key-based algorithm for image encryption, *Proceedings of SecureComm 2005*, IEEE Press, Athens, Greece, pp. 406–408.

Solak, E. (2005). Cryptanalysis of observer based discrete-time chaotic encryption schemes, *International Journal of Bifurcation and Chaos* Vol.2(No.15): 653–658.

Sridharan, S., Dawson, E. & Goldburg, B. (1990). Speech encryption in the transform domain, *Electronics Letters* Vol.26(No.10): 655–657.

Sridharan, S., Dawson, E. & Goldburg, B. (1991). Fast fourier transform based speech encryption system, *Proceedings of the Int. Conf. on Communications, Speech and Vision*, IEEE Press, Anchorage, AK, pp. 215–223.

Su, Z., Jiang, J. & Lian, S. (2009). Selective encryption for g.729 speech using chaotic maps., *Proceedings of International Conference on Multimedia Information Networking and Security*, IEEE computer society, Wuhan , China, pp. 488–492.

Su, Z., Jiang, J. & Lian, S. (2010). Hierarchical selective encryption for g.729 speech based on bit sensitivity, *Journal of Internet Technology* Vol.5(No.11): 599–607.

Su, Z., S., L., Zhang, G. & Jiang, J. (2011). *Chaos-based video encryption algorithms*, Springer-Verlag, New York.

Tong, X. & Cui, M. (2008). Image encryption with compound chaotic sequence cipher shifting dynamically, *Image and Vision Computing* Vol.26(No.6): 843–850.

Tuchman, W. (1997). *A brief history of the data encryption standard*, ddison-Wesley Publishing, New York.

Tzouveli, P., Ntalianis, K. & Kollias, S. (2004). Security of human video objects by incorporating a chaos-based feedback cryptographic scheme, *Proceedings of MULTIMEDIA '04*, ACM Press, New York, USA, pp. 10–16.

Wang, Y., Wong, K. W., Liao, X. & Chen, G. (2011). A new chaos-based fast image encryption algorithm, *Applied Soft Computing* Vol.11(No.1): 514–522.

Wong, K., Kwok, B. & Yuen, C. H. (2009). An efficient diffusion approach for chaos-based image encryption, *Chaos, Solitons & Fractals* Vol.41(No.5): 2652–2663.

Wu, C. & Kuo, C. J. (2001). Fast encryption methods for audiovisual data confidentiality, *Proceedings of SPIE4209*, SPIE Press, Boston, MA, USA, pp. 284–295.

Xiang, T., Wong, K. & Liao, X. (2007). Selective image encryption using a spatiotemporal chaotic system, *Chaos* Vol.17(No.2): 2191–2199.

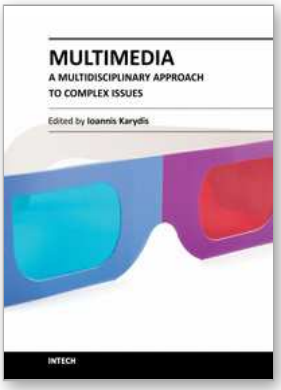
Xiao, D., Liao, X. & Wei, P. (2009). Analysis and improvement of a chaos-based image encryption algorithm, *Chaos Solitons & Fractals* Vol.2009(No.40): 2191–2199.

Yang, S. & Sun, S. (2008). A video encryption method based on chaotic maps in dct domain, *Progress in natural science* Vol.18(No.10): 1299–1304.

Yang, T., Wu, C. W. & Chua, L. O. (1997). Cryptography based on chaotic systems, *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* Vol.5(No.44): 469–472.

Zeghid, M., Machhout, M. & Khriji, L. (1996). A modified aes based algorithm for image encryption, *International Journal of Computer Science and Engineering* Vol.1(No.11): 70–75.

Zhang, L., X, L. & X., W. (2005). An image encryption approach based on chaotic maps, *Chaos Soliton Fract* Vol.24(No.11): 759–765.



Multimedia - A Multidisciplinary Approach to Complex Issues
Edited by Dr. Ioannis Karydis

ISBN 978-953-51-0216-8
Hard cover, 276 pages
Publisher InTech
Published online 07, March, 2012
Published in print edition March, 2012

The nowadays ubiquitous and effortless digital data capture and processing capabilities offered by the majority of devices, lead to an unprecedented penetration of multimedia content in our everyday life. To make the most of this phenomenon, the rapidly increasing volume and usage of digitised content requires constant re-evaluation and adaptation of multimedia methodologies, in order to meet the relentless change of requirements from both the user and system perspectives. Advances in Multimedia provides readers with an overview of the ever-growing field of multimedia by bringing together various research studies and surveys from different subfields that point out such important aspects. Some of the main topics that this book deals with include: multimedia management in peer-to-peer structures & wireless networks, security characteristics in multimedia, semantic gap bridging for multimedia content and novel multimedia applications.

How to reference
In order to correctly reference this scholarly work, feel free to copy and paste the following:

Zhaopin Su, Guofu Zhang and Jianguo Jiang (2012). Multimedia Security: A Survey of Chaos-Based Encryption Technology, Multimedia - A Multidisciplinary Approach to Complex Issues, Dr. Ioannis Karydis (Ed.), ISBN: 978-953-51-0216-8, InTech, Available from: http://www.intechopen.com/books/multimedia-a-multidisciplinary-approach-to-complex-issues/multimedia-security-a-survey-of-chaos-based-encryption-technology

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821