Chaotic Cryptography and Multimedia Security: A Review

Gangadhar Tiwari
NIT, Durgapur

Debashis Nandi
NIT, Durgapur

Madhusudhan Mishra
NERIST, Itanagar

Abstract

With the rise in use of Multimedia Information over internet due to its ease and flexibility for communication, there arises the need of protecting it against unauthorized access. Protecting multimedia information during communication is the need of the hour. Cryptography seems to be a vital tool in achieving this. Although several Cryptographic techniques have been proposed so far each having their advantages and limitations, however none of them can ensure reliable protection for multimedia data. This review is an effort to discuss employing Chaos, an offshoot of Non-Linear Dynamics in Cryptography for securing multimedia data which have limitations like huge data sizes and real time constraints.

1. Introduction

Cryptography is a vital and efficient tool for ensuring information privacy. It does so by scrambling the messages using encryption algorithms thereby producing an unreadable cipher text which is to be decrypted to recover original message. If E denotes the encryption function and k is key, then

$$\boldsymbol{E_k\ (M) = C} \tag{1}$$

where M is the message to be encrypted and C is the cipher text and if D denotes the decryption function and k is key then

$$\boldsymbol{D_k\ (C) = M} \tag{2}$$

The conventional cryptographic techniques like DES, IDEA, AES etc based on number theoretic or algebraic concepts are most suitable for textual or binary data but are unfit for multimedia data due to their huge sizes, higher inter-pixel redundancy, interactive operations, and requirement of real-time responses. Hence employing chaotic cryptography can be an optimum solution in this regard. The foremost benefit is that a chaotic signal looks like noise for non-authorized users and that chaotic signals are very sensitive to initial conditions so the initial states and control parameters can be proficiently used as keys in the cryptographic process. Also cost of generation of chaotic signal is significantly low. The fundamental principle of chaotic encryption is the capacity of dynamic systems to generate number sequences with random nature which is used for encryption [1]. During decryption the sequence of random numbers are regenerated. The simplest and widely used chaotic equation (Logistic map) is represented as

$$\mathbf{x_{n+1}} = \square * \mathbf{x_n}(\mathbf{1} - \mathbf{x_n}) \tag{3}$$

where when $0 \le \mathbf{x_n} \le \mathbf{1}$ and $3.5699 < \mu \le 4$ the equation shows chaotic characteristics.

In this paper the section 2 discusses the requirements of multimedia encryption and their evaluation methods. Section 3 briefs about Chaotic image encryption schemes. Section 4 is devoted on chaotic encryption of Digital Audio. Section 5 discusses Digital Videos encryption using Chaos and Section 6 draws the conclusion and future scope in this field.

2 Multimedia Encryption Requirements

Multimedia data has special features like bulky data volumes, higher redundancy among neighbouring pixels, interactive operations etc. Therefore multimedia applications have their own requirements. This section discusses certain specific requirements of multimedia encryption.

High Security

Security is the principal condition for multimedia encryption, therefore employing chaotic maps must guarantee information security. Security of an encryption algorithm depends upon perceptual security, key sensitivity, key space, and its ability to retort possible attacks. Hence, a secure chaotic encryption algorithm must be secure in perception, have large key space, higher key sensitivity, and resistant to cryptanalytic attacks.

Reduced Computational complexity

Since the multimedia data is huge in size, encrypting all data bits will increase the computational complexity. As HVS/HAS is highly robust to signal distortions, only enciphering the data bits intelligibility tied will ensure data security with reduced computational complexity.

Compression ratio Invariant

The encryption algorithm employed for multimedia security should not change compression ratio or keep changes minimal.

Compliance in Format

Multimedia data is compressed before transmission, which produces the data streams with some format information. If the encrypting mechanism encrypts the multimedia data as normal data format information will be lost making format conversion impossible. Hence the encryption algorithm so employed must encrypt the data not the format information.

Real-time Performance

Real-time response is a vital requirement for multimedia applications. Therefore, the encryption and decryption process so employed must meet time requirement.

Multitier Security

In multimedia applications, multitier security is required to perform complex multimedia processing. Most available cryptographic systems are fully or partially scalable. A higher level of security is achieved with bigger key sizes or by increasing number of rounds.

Bit error tolerance

As multimedia data is transferred in noisy environments, the received data is prone to transmission errors. So, a perfect cryptographic system must be insensitive and robust to transmission errors

.

2.1 Evaluation methods of multimedia encryption

The evaluation of encryption algorithm is based on factors like analysis of security, analysis of time, compression ratio and fault tolerance.

Security analysis

Security of an encryption algorithm is evaluated by the perceptual strength, analysis of key space and key sensitivity and its robustness against cryptanalytic attacks. The perceptual effect is achieved through a set of comparison among the encrypted and the original multimedia data. Key space is determined using the number of key employed for the encryption process. Analysis of Key sensitivity for a chaotic cipher refers to its sensitivity with regard to initial states and control parameters sensitivity of chaotic map.

Time analysis

It is calculated in three following ways:-

Absolute encryption time- time assumed for encrypting a multimedia data and is measured in second.
Relative encryption time ratio- time ratio between compression and encryption of multimedia data.
Computation complexity-it depends on the chaotic cipher's cost and the volumes of multimedia data to be encrypted. A multimedia encryption scheme is deemed fit for real time applications provided computational cost or assumed time is negligible compared to the compression.

Test for Compression ratio

The compression ratio is measured by comparing compressed and encrypted data with respect to the original compressed data. The image and video quality is measured by calculating Peak Signal-to-Noise Ratio (PSNR) between the encrypted and original 2-D image using Equation (4) and (5).

$$PSNR = 10 * log_{10}\left(\frac{2^B - 1)^2}{MSE}\right) \qquad (4)$$

$$\mathrm{MSE} = \frac{1}{m*n}\sum_0^{m-1}\sum_{j=0}^{n-1}[I(i,j) - I']^2 \qquad (5)$$

where B is the sampling frequency, I and I' represent an original $m \times n$ image and the encrypted one.

While audio quality is measured by calculating Segmented Signal-to-Noise Ratio (segSNR) between original and encrypted audio using Equation (6).

$$\mathrm{segSNR} = \frac{10}{m} * \log_{10} * (\mathrm{sum}[s(i)]^2/\mathrm{sum}[sn(i) - s(i)]^2) \qquad (6)$$

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. A higher value of PSNR and segSNR signifies better security and good performance of the encryption scheme.

Test for Fault tolerance

An encryption algorithm is robust against transmission errors provided small change in a pixel does not affect neighbouring pixels and there is no change of file format. It is tested by analysing the correlation between the signal quality (PSNR, SegSNR*)* of the decrypted frames and the number of bit-error of the encrypted frames.

3. Chaos-based image encryption algorithms

The chaotic image encryption schemes are made by employing chaotic properties like non-linear transform, unpredictable behaviour and deterministic dynamics. It is broadly divided into full encryption and partial encryption depending upon the percentage of the data encrypted. On the basis of encryption ciphers, the algorithms are block ciphers and stream ciphers.

3.1 Full encryption algorithms

Here the whole image is encrypted without any compression process. It offers better security, can block unauthorized access, and is extensively used. Algorithms are proposed based on chaotic block ciphers as well as stream ciphers.

Chaotic block ciphers based Algorithms

A chaotic map based block cipher is a single key encryption scheme that transforms plain-text block into cipher text blocks of equal length, i.e. the image are encrypted block wise. Many block ciphers based algorithms are proposed including Mao et al., 2004;Lien et al, 2005;Cokal et al, 2009; and Wang et al., 2011 [5]. Mao et al proposed a 3-D chaotic baker map based algorithm having confusion and diffusion stage. Here three-dimensional baker map is generated by extending the standard two-dimensional baker map. It offers speed and security both compared to other 2-D baker map based schemes [3]. Lian et al model comprised 3 components: a chaotic skew tent map based key generator that generates the keys for confusion, random-scan and the diffusion process using equation (7), a chaotic map based corner-pixels confusion process which consists of the chaotic permutation and random-scan process, and a diffusion function realized by a logistic map based diffusion function that spreads changes among neighbouring pixels using equation (8).

$$\boldsymbol{x_{j+1} = \begin{cases} \dfrac{x_j}{h}, 0 < x_j \le h \\ \left(\dfrac{1 - x_j}{1 - h}\right), h < x_j \le 1 \end{cases}} \qquad (\mathbf{7})$$

$$\boldsymbol{x_{j+1} = 1 - \boxed{?} * x_j^2} \qquad (\mathbf{8})$$

It offers higher key-sensitivity and robustness against cryptanalytic attacks. However both the models requires chaotic confusion and pixel diffusion to be operated separately thereby resulting in situation where the algorithms require at least two image-scanning processes which increases time delay. To overcome this Wang et al model combined permutation and diffusion. Here the image is first divided into 8 × 8 pixels blocks. Then, the pseudorandom numbers are used to change the pixel values in the blocks. Meanwhile, the blocks are relocated according to lattice values of the nearest-neighbouring coupled map lattices using equation (9). It greatly increases the encryption speed besides being robust against attacks.

$$\boldsymbol{x_{n+1}(i) = (1 - \mathcal{E})f\big(x_n(i)\big) + \mathcal{E}f(x_n(i+1)} \qquad (\mathbf{9})$$

Chaotic stream ciphers based Algorithms

It is a pseudo random cipher key stream generated by a chaotic map that encrypts data bit by bit in a XOR operation. Some models includes Chen et al., 2004; Zhang et al, 2005, Gao et al, 2006 [8]. Chen et al, 2004 proposed a scheme based on 3D cat map which is fast and secure. Here 3D cat map is engaged to shuffle pixel positions in the image, and a logistic map based diffusion process among pixels is performed. The Chen model is represented using equation (10).

$$\boldsymbol{\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x - xz + cy \\ \dot{z} = xy - bz \end{cases}} \qquad (\mathbf{10})$$

Zhang et al, 2005 employed discrete exponential chaotic map where, 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 is chosen to generate key-stream to make it more secure against attacks. It is of high speed, high security, and can be applied in fast real time encryption applications. Gao et al, 2006 proposed an encryption scheme based on a new non linear chaotic algorithm (equation 11) which uses tangent and power functions [4]. Moreover it is a one-time-one password system. Thus it offers very high security.

$$\boldsymbol{x_{n+1} = \lambda.tg(\alpha * x_n)(1 - x_n)^{\beta}} \qquad (\mathbf{11})$$

However developing chaotic stream ciphers based algorithms is an open area and many other researchers like Wong (2009), Li (2009) are working on it.

Comparing Block and Stream Encryption Algos.

Stream ciphers are best suited where data size is either continuous or unknown [2]. Block ciphers are more suited when data size is known. The key reasons are:
When compared to stream encryption algorithms, the time and memory requirement of Block encryption algorithms is much higher as because block cipher, work on larger sized blocks whereas stream ciphers work on only a few bits at a time. Implementing Stream ciphers correctly based on usage is a tough task to perform and they are more susceptible to weaknesses. Stream ciphers are more immune to transmission errors as because bytes are individually encrypted without any relation to other ciphers, and possesses support for line interruptions. Whereas block ciphers are less tolerant since they encrypt a whole block at a time. Block ciphers provide validation and privacy; while stream ciphers do not.

3.2 Partial encryption

It only encrypts part of the data. Here an image is divided into insensitive data and sensitive data where only the latter is encrypted. The key issue while deploying partial encryption schemes is how to determine sensitive data of an image. Some key models based on chaotic stream ciphers include Lian et al, 2004; Xiang et al, 2007; El-Khamy et al, 2009 [6] . Lian et al (2004) proposed a partial image encryption algorithm by combining JPEG2000 codec and chaotic neural networks. Here the sensitive data is encrypted by a chaotic sequence in a chained encryption mode. The model is fast, compression ratio invariant and secure against common cryptanalytic attacks. Xiang et al (2007) proposed an image encryption scheme based ona one-way coupled map lattice (equation 12) that first splits image pixel into $n(n < 8)$ significant bits and $(8 - n)$ less significant bits, and encrypts the n bits by the key-stream based on a chaotic skew tent map.

$$\boldsymbol{x_{t+1}^{i}} = (\mathbf{1} - \mathcal{E})\boldsymbol{g}(\boldsymbol{x_{t}^{i}}) + \mathcal{E}\boldsymbol{g}(\boldsymbol{x_{t}^{i-1}}) \qquad (\mathbf{12})$$

However it is insecure for images with higher inter-pixel redundancy and cannot keep compression ratio and format compliance. El-Khamyl et al (2009) proposed a scheme based on ELKNZ chaotic stream cipher(El-Zen et al., 2008)and discrete wavelet transform (DWT) where the image first goes through a single-level 2D-DWT operation and lowest frequency sub-band is encrypted using the ELKNZ cipher, and the rest are scrambled. After that they undergo 2D inverse discrete wavelet transform (2D IDWT) to produce the encrypted image. It provided complete perceptual encryption and is secure.

4. Chaos-based audio encryption algorithms

Audio encryption algorithms are divided into partial and full encryption according to the percentage of data encrypted.

Full encryption of digital audio

In digital encryption, the bit stream is encrypted after the analog signal is digitized and compressed to generate a data signal. The key research models include Liu et al, 2008 and Sheu et al, 2011[10]. Liu et al model is a block encryption algorithm for digital speech codes that encrypts message with chaotic sequences using henon and logistic maps (using equation 13).

$$\begin{cases} \boldsymbol{x_{i+1}} = \mathbf{1} + \boldsymbol{by_i} - \boldsymbol{ax_i^2} \\ \boldsymbol{y_{i+1}} = \boldsymbol{x_i} \end{cases} \qquad (\mathbf{13})$$

Sheu (2011) proposed a model based on fractional Lorenz system. It can achieve high key sensitivity, has larger key space and secure.

Full encryption offers better security but is computationally expensive, and hence unsuited for real-time applications.

Partial encryption of digital audio

Partial encryption only encrypts the sensitive subset of an audio data. The key research models include Servetti et al (2003) and Su et al (2010). Servetti et al. presented a frequency-selective model for MP3 where only a part of the stop-band coefficients are encrypted. It is of low-complexity, more secure and format compliance. Su et al model presented a group of chaos-based hierarchical selective encryption schemes where speech bit streams are divided into two parts as per bit sensitivity and the sensitive bits are encrypted by a strong cipher whereas rest are encrypted by light weight cipher.

Partial encryption offers lower computational complexity than full encryption and is audio format compliance which makes it suitable for narrow bandwidth environments and power-constrained devices.

5. Video encryption using Chaos

There are three types of Video encryption algorithms: the raw video data encryption, encrypting the video data during compression process, and encrypting the compressed video data.

5.1 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. The former means encrypting video data frame by frame without considering semantic information. The key research models include Li et al., 2002; and Sudha et al, 2008[7]. Li et al proposed an encryption scheme based on multiple digital chaotic systems where each plain-block is first XORed by a chaotic signal, and then substituted by a pseudo-random S-box based on multiple chaotic maps. It has low computational complexity and is secure. Sudha et al used a high dimensional Lorenz chaotic system. The encryption scheme encrypts each video frame by confusing the pixel position and each frame is encrypted by a unique key. This model is secure and robust to transmission error.

In encrypting video data considering regions of interest the key models includes Tzouveli et al., 2004; and Kollias et al, 2005. Tzouveli et al model is based on logistic map where face regions are detected first followed by body regions. Then, extracted video object's pixels are encrypted based on logistic map. This model is efficient in computational resources and running time. In Kollias et al encryption system video objects are extracted first. After that for each video object, multi-resolution decomposition is performed and the pixels of the lowest resolution level are encrypted using two chaotic block ciphers and a complex product cipher combining a chaotic stream-cipher. Finally, the encrypted regions are propagated to the higher resolution levels and the encryption process is repeated until the highest level is reached. It is secure against attacks.

5.2 Encrypting video data in compression process

Here the Encryption of video data starts in the encoding process before entropy coding, such as Context-adaptive binary arithmetic coding (CABAC) and variable length coding (VLC), The key schemes includes Yang et al,2008; and Lian et al,2009. Yang et al, proposed a chaos-based video encryption method in DCT domain. Here I-frames are selected for encryption objects. First of all DCT coefficients of I-frames are scrambled using coupling logistic maps (equation 14), and then encrypted using another logistic map (equation 8).

$$\begin{cases} \boldsymbol{x_{n+1} = \boxed{?}_x x_n(1 - x_n)} \\ \boldsymbol{y_{n+1} = \boxed{?}_y y_n(1 - y_n)} \end{cases} \qquad \textbf{(14)}$$

This scheme consumes less time and has very large key space however it is not fully secure. In Lian et al scheme, the 2D coupled map lattice (2D CML) is employed for encrypting direct current coefficient (DC) and the signs of the alternating current coefficients (ACs). The encryption is operated after block partitioning, color space transformation, DCT quantization & transformation and before post-encode. It offers perceptual security, better PSNR and high key sensitivity. However the security depends upon randomness of chaotic sequences generated by 2D CML.

5.3 Encrypting the compressed video data

Here the video data is encrypted after entropy encoding and before packaging. The key encryption scheme includes. Lian et al (2007) and Wang et al, (2007)[9]. Lian et al scheme is based of chaotic stream cipher produced by Linear Chaotic Maps. Here both the motion vectors' signs and intra-macro blocks are encrypted. The encryption process is achieved after video length encoding and before packaging. It offers high key sensitivity, format compliance and bit error tolerance. In Wang et al scheme only the sub-bands, motion vectors and code blocks, are partially encrypted by a stream cipher based on a modified chaotic neural network. The Wang Model offer perceptual security, error robustness and is compression ratio invariant.

6. Conclusions

Protecting digital data is a key issue in the period of expansion of communication networks and multimedia technology. To tackle the menace, many encryption algorithms have been proposed each with their merits and demerits. However, as on date we are yet to achieve an encryption algorithm that can satisfy all information security requirements. From the above discussions in the review it is evident that chaotic encryption algorithms are far more superior to conventional encryption techniques and hence can form the basis for future research. However, chaos-based multimedia encryption is still in its infant stage and more efforts are required for its use in real-time applications with superior and multitier security, low computational complexity, better PSNR, and high fault tolerance capacity.

References

[1] Alligood, K. T., Sauer, T. &Yorke, J. A., Chaos: an introduction to dynamical systems, Springer-Verlag, New York, 1997.

[2] Jakimoski, G. and L. Kocarev, “Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps”, IEEE Transactions on Circuits and Systems—I, 2001, Vol. 48(2), pp. 163-169.

[3] Y.B. Mao, G. Chen, S.G. Lian, “A novel fast image Encryption scheme based on the 3D CB Map”, Int. J. Bifurcate Chaos, 2004, Vol. 14, pp. 3613–3624.

[4] H. Gao, Y. Zhang, S. Liang, and D. Li, “A new chaotic algorithm for image encryption”, Chaos, Solutions &Fractals, 2006, Vol. 29, pp. 393–399.

[5] Fengjian Wang, Yongping Zhang and Tianjie Cao “Research of chaotic block cipher algorithm based on Logistic map”, 2nd Int. Conference on Intelligent Computation Technology and Automation, 2009, pp. 678 – 681.

[6]. Cheng H, Li XB, “Partial encryption of compressed images and videos”, IEEE Trans Signal Processing 2000, Vol. 48(8), pp.2439 – 2451

[7] Dachselt F, Schwarz W, “Chaos and cryptography”, IEEE Trans Circuits and Systems-I, 2001, Vol. 48(12), pp.1498 – 1509

[8] Fridrich J, “Secure image ciphering based on chaos: Final report for AFRL”, 1997, Rome, New York

[9] Fridrich J, “Symmetric ciphers based on two-dimensional chaotic maps”, Int J Bifurcation and Chaos, 1998, Vol. 8(6), pp.1259 – 1284

[10] G. Jakimoski, L. Kocarev, “Analysis of some recently proposed chaos based encryption algorithms”, Physics Letters A, 2001, Vol. 291, pp. 381-384