An Efficient Chaotic Cryptosystem for Real-time MPEG Video Encryption Algorithm using Arnold's Cat Map and Henon Map

K.Bhuvaneswari[1] and K.Mahesh[2]

[1]Research Scholar, [2]Professor

Department of Computer Applications,

Alagappa University, Karaikudi-600 003, Tamilnadu, India.

kbb_bhuvana@yahoo.co.in[1], mahesh.alagappa@gmail.com[2]

Abstract

Rapid growth in network communication, there is need development inorder to provide the security for sensitive data from leakages. Many algorithms were designed for past years but they are not well proficient while concerning multimedia elements such as image and video due to high complexity of encoded /decoded, high correlation among all the pixels. Chaos based encryption algorithm has suggested to deal with these problems because it has desirable features of generate pseudo random number, sensitivity to initial conditions. A multimedia element video is bounded of audio and image so video encryption is to consider crucial part and critical task. The intent of proposed method is to secure the secret video clip by encryption using Arnold's Cat Map and Henon chaotic map. In this method, video is extracted into frames and equal size of chaotic sequences is generated. Original pixel values are shuffled using cat map and its result is XORed with the chaotic sequences of Henon Map. Further, security of the implemented algorithm is evaluated by experiments on different input video clips and result produced in less complexity with high security. Finally conclude that this system is efficacy and provides two layers of security for transmission of multimedia element video.

Keywords: Arnold Cat map, Henon Map, Security, Encryption, Video, Frame

1. Introduction

In present situation security of digital images draws more attention, especially when these digital images are stored in memory or send through the communication networks. Many different image encryption techniques have been proposed to save the security of images [1]. 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 [2]**.** Chaotic functions are blessed with important characteristics which makes it excellent for practical use against any statistical attack that is they are very sensitive to initial

condition or system parameter and it shows Pseudo-random behaviour which makes them desirable for encryption [3]**.** During image encryption, chaotic map followed by Arnold cat map has also been introduced for secure strong image cryptography. Unlike chaotic map, Arnold cat map has different significance towards image pixels positions. As a result of the initial sensitivity and the unpredictability of outcome of the chaotic map, it is very difficult to attack the secure system effectively [4]**.**

2. Related Work

The proposed method [8] select the I-frames of the video sequence as encryption objects. First, two coupling chaotic maps are used to scramble the DCT coefficients of every original I-frame, and receive the scrambled I-frame. Second, encrypt the DCT coefficients of the scrambled I-frame using another chaotic map.

In N.K.Pareek et al [5], an external secret key of 80-bit and two chaotic logistic maps are employed. The initial conditions for the both logistic maps are derived using the external secret key by providing different weightage to all its bits. Further, in the proposed encryption process, eight different types of operations are used to encrypt the pixels of an image and which one of them will be used for a particular pixel is decided by the outcome of the logistic map.

The proposed [9] a video encryption scheme based on the widely used substitution–diffusion architecture which utilizes the chaotic 2D standard map and 1D logistic map is proposed.

In the proposed scheme [10] used chaos theory to generate the necessary random matrix and used the same for Image encryption. For Decryption, used look-up table approach to find the element by element modular inverse of the random matrix and use it for decryption of an encrypted image.

3. Proposed Methodology

3.1 Arnold's Cat Map

Arnold map is also called cat map. It is a two-dimensional invertible chaotic map introduced by Arnold and Avez [5].

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod 1$$

Where " x mod 1 " means the fractional part of a real number x by adding or subtracting an appropriate integer. Good dynamical features in the generalized Arnold map, such as desirable auto-correlation and cross correlation features [6].

3.2 Henon Map

The Hénon map is two dimensional chaotic maps. It takes a point (xi, yi) and maps it to a new Point in the same plane. It can be describing as follows [7].

$$x_{i+1} = 1 - rx_i^2 + y_i$$
$$y_{i+1} = bx_i \qquad ,i = 0,1,2,.....$$

A simple 2D chaotic map with quadratic nonlinearity, depends on two parameters, r and b, which for the canonical Hénon map have values of r = 1.4 and b = 0.3. For the canonical values the Hénon map is chaotic. This map has chaotic behavior in range [1.07, 1.4], for other values it behave as periodic or convergence to constant value

3.3 Proposed Algorithmic Steps

In proposed method, two chaotic maps are used to encrypt the sensitive video. First, video is split into frames and original image pixels are shuffled with help of Arnold cat map. Again it is XORed with Henon map so video is well encrypted and send it to receiver. The entire process flow of proposed method is depicted as shown in figure 1.

The detailed steps of proposed algorithm are given below.

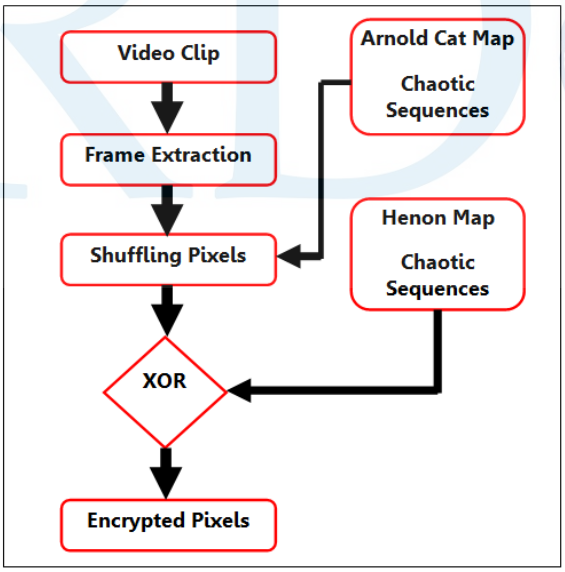


Figure 1. The process of Proposed System

3.3.1 Encryption Algorithm

Input: Secret Video Clip

Output: Encrypted Video Clip

1. Video is not directly processed because it takes high complexity so it is split in three different frames called Red, Green and Blue.
2. Again these frames are partition into 8x8 blocks.

3. Chaotic sequences are generated using Arnold Cat map to provide one layer of security.
4. Shuffle the original pixels of blocks according to the Arnold Cat Map Chaotic Sequences
5. Another chaotic sequences are generated using Henon Map to provide second layer of security.
6. Resultant values from the Step 2 are XORed with chaotic sequences of Henon Map.

3.3.2 Decryption Algorithm

Input: Encrypted Video Clip

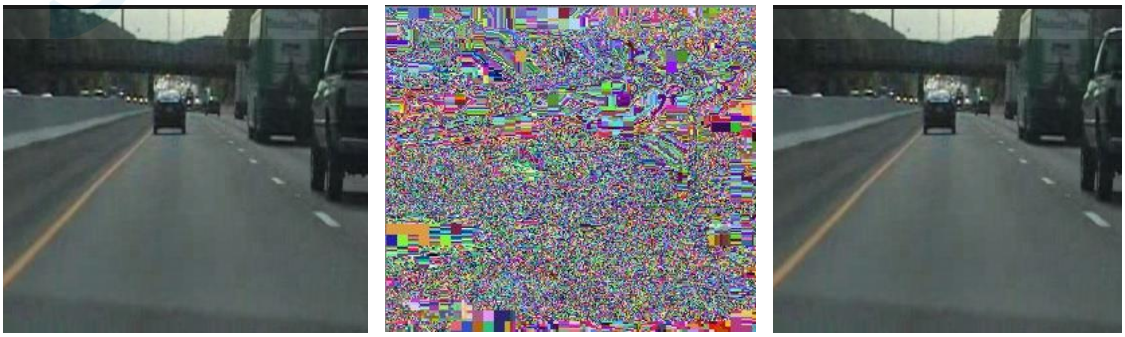
Output: Original Video Clip

1. Decryption on encrypted video clip is performed by the reverse process of encryption which means inverse equation of Arnold's Cat Map and Henon Map to decipher the frames.

2. To reshuffling the frames, inverse equations of two maps are applied. If once employed, receiver obtains the original video clip.

4. Experimental Results

The experiential results of the proposed method as show in table 1. The proposed encryption algorithm is simulated using different MPEG video formats such as MPEG-1and MPEG-2 videos. Figure 2, 3, 4 shows various kinds of sample videos such as Car, traffic and Professor Videos are used to evaluate the proposed algorithms. Figure 2, 3, 4. a shows the original videos and 2, 3, 4. b shows the corresponding encrypted videos frames and finally decrypted the original videos as shown in figure 2, 3, 4.c.



(a) Original Video (b) Encrypted Video (c) Decrypted Video

Figure 1 : Simulated Results of the Proposed Method in Car Video

(a) Original Video (b) Encrypted Video (c) Decrypted Video

Figure 2 : Simulated Results of the Proposed Method in Professor Video

(a) Original Video (b) Encrypted Video (c) Decrypted Video

Figure 3 : Simulated Results of the Proposed Method in Traffic Video

5. Conclusion

In this paper a Chaotic Cryptosystem is developed for Real-time MPEG Video security purpose with aid of Arnold's Cat Map and Henon Map is proposed. The proposed algorithm clearly explains about the step by step process of both encryption and decryption. The proposed video encryption algorithm more suitable, secure and robust for real time MPEG videos. The strength of the proposed algorithm is very difficult for any intruder to crack the original video by using our proposed algorithm. In future optimal key chaotic based methods are used to increase the execution speed for video encryption algorithms.

References

1. S Raghunath Reddy, K Srikanth and T Swathi, "**Secure Image Encryption and Decryption in Full Motion Video**", International Journal of Computer Science and Information Technologies, Vol. 5, Issue.3, pp: 3259 - 3261, 2014.
2. Gangadhar Tiwari, Debashis Nandi and Madhusudhan Mishra, "**Chaotic Cryptography and Multimedia Security: A Review**", International Journal of Engineering Research & Technology, Vol. 2 Issue 10, pp: 1520 -1525,2013.

3. Jyoti S. Bowade, Pawan khade and M. M. Raghuwansh, "**Technique of Video encryption/scrambling using chaotic functions and analysis**", Journal of Emerging Technologies and Innovative Research, Vol.2, Issue 6, pp: 1951-1958, 2015.
4. Sudhir Keshari and S. G. Modani, "**Image Encryption Algorithm based on Chaotic Map Lattice and Arnold cat map for Secure Transmission**", International Journal of Computer Science and Technology, Vol. 2, Issue 1, pp: 132-135, 2011.
5. N.K. Pareek,Vinod Patidara and K.K. Suda, "**Image encryption using chaotic logistic map**", Image and Vision Computing, Volume 24, Issue 9, pp: 926–934, 2006.
6. Junqin Zhao, Weichuang Guo and Ruisong Ye, "**A Chaos-based Image Encryption Scheme Using Permutation-Substitution Architecture**", International Journal of Computer Trends and Technology, Vol.15, Number.4, pp: 174-185, 2014.
7. Wei-Bin, Chen, and Zhang Xin. "**Image encryption algorithm based on Henon chaotic system.**" Image Analysis and Signal Processing, 2009. IASP 2009. International Conference on. IEEE, 2009.
8. Yang, Shuguo, and Shenghe Sun, "**A video encryption method based on chaotic maps in DCT domain**", Progress in natural science, Vol.18, Issue.10, pp: 1299–1304, 2008.
9. Varalakshmi, L. M., and G. Florence Sudha. "**Selective Encryption of Video Using Multiple Chaotic Maps**", Information Processing and Management, pp: 164-168, 2010.
10. Shyamsunder, S., and Ganesan Kaliyaperumal, "**Image encryption and decryption using chaotic maps and modular arithmetic**", American Journal of Signal Processing, Vol.1, Issue.1, pp: 24-33, 2011.