

Video Encryption using Bit Plane Decomposition and Multiple Chaotic Maps

Kiran

Assistant Professor
Dept. of Electronics and communication Engineering
GMIT, Mandya
Karnataka

Sandeep R.

Assistant Professor
Dept. of Electronics and communication Engineering
VVCE, Mysuru
Karnataka

Parameshachari B. D., PhD

Professor and Head
Dept. of Telecommunication Engineering
GSSIETW, Mysuru
Karnataka

Priyanka R.

PG student
Dept. of Electronics and communication Engineering
VVCE, Mysuru
Karnataka

ABSTRACT

Video encryption is an efficient technique for video content protection. In this work, proposed an video encryption using Henon map and chaotic map. Firstly read and convert the video into number of frames. The proposed algorithm decomposes four input frames into 32 bit-planes, randomly swaps bit-blocks among different bit-planes and conducts XOR operation between the scrambled images and secret matrix controlled by chaotic map. Cipher images are obtained and convert into cipher video. Many simulations are done to illustrate efficiency of our algorithm.

General Terms

Information security, Video encryption

Keywords

Henon map, Chaotic map, Bit planes

1. INTRODUCTION

In the present day lifestyle, achieving data security has grown up as one of the challenging tasks, especially in the applications related to military, medical and secure facsimile. Achieving confidentiality and preventing any illegal access into any network has become very important challenge today.

A novel bit-level video encryption technique was proposed which has the basis of creation of dynamic groups [1]. BLP method involves splitting up of a plain video into various random groups followed by implementation of bit level permutation and diffusion procedure. The logistic map generates key stream, complicates plain videos relationship with cipher video. Pseudo random sequences are created by chaotic systems, which exhibit excellent randomness, which are best fit for video encryption [2]. the proposed NPWLCM (Nested Piece Wise Linear Chaotic Map) involves shuffling of bit planes of grey/color levels in or-

der to make the encryption process more complicated. Conventional DCT/IDCT algorithms focus on reduction of mathematical complexities [3]. An architecture that can encrypt as well as compress the video was implemented, which is best suited for applications in real-time. Here DCT outputs with only some special points are computed and random numbers are generated by using LFSR which adds up with selected DCT outputs. The latest challenges include securing the information during data transfer. Variety of security models was discussed that involves different encryption standards so as to improve the security of data transfer [4]. Even the most complicated encryption algorithm that offered excellent security level became vulnerable as time proceeded. Majority of the proposed chaotic based encryption algorithms reduce the system performance and also give rise to key space problems [5]. Cyclic elliptical curve was combined with chaotic system to end up with a hybrid video encryption algorithm which overcame the mentioned limitations. Hill Cipher algorithm [6] has showed a number of merits among symmetric key algorithms used for plain text, with a drawback that not every time the inverse of key matrix exists, which obviously results in unsuccessful decryption

2. HENON MAP

Henon map is a dynamic system, which shows two-dimensional chaotic behaviors when it is subjected to iterations in discrete time. It is made up of closely packed periodic points and hence shows good sensitivity and dependency towards initial conditions. It appears while studying two-dimensional discrete dynamic systems as a strange attractor, a feature of chaos theory. The concept of strange attractor describes chaotic systems in a different way. A dynamic system is given with an attracting set, which is closed subset A of its phase space. The system evolves towards A for different values of initial point. Attractor defines that attracting set which holds good for certain supplementary conditions, such that it will be impossible to divide into smaller pieces. In iteration maps that follow discrete time steps, fixed points are attracted by attractors. Henon map displays simple 2-D iteration maps that have inverse, that possess

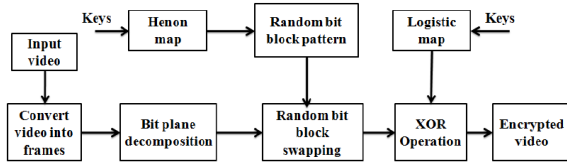


Fig. 1. Block diagram of proposed method

quadratic non linear behavior and chaotic solutions. It is called as strange attractor, which bridge chaos with fractals. Henons attractor is attractor with fractal (non integer) dimension, which is used to characterize strange attractors. Strange attractor obtains fractal structure from Henon map. Henon map is defined by

$$\begin{aligned} x(k+1) &= 1 - ax^2(k) + y(k) \\ y(k+1) &= bx(k) \end{aligned} \quad (1)$$

b measures rate of area contraction and hence Henon map is widely used 2-D quadratic map where contraction does not depend on x and y. Henon map becomes quadratic map if b=0, hence following period doubling route to chaos. In the range between a and b, bounded solution exists.

2.1 Chaotic Map

Chaotic maps show excellent results towards encryption of video files. Programmers who work on cryptography and cryptosystems relevant to video, are very much interested towards chaotic maps due to the interesting bondage between cryptography and chaos. Chaotic properties like sensitive to system parameters/initial conditions, ergodicity, etc are equivalent to diffusion, confusion of cryptography. Chaotic systems exhibit non linearity and behave randomly for few ranges of system parameters. Such systems are spontaneous and will be applicable to security procedures directly.

$$X(i+1) = \mu X(i)(1 - X(i)) \quad (2)$$

where μ is the control parameter and the logistic system is in chaos when $\mu \in [0, 4]$.

3. PROPOSED METHOD

Block diagram of Proposed method as shown in Figure 1. It involves the following basic steps:

1. Video is converted into frames, where four input frames are split into bit-planes.
2. With the help of Henon map, bit-blocks are obtained by dividing bit-planes randomly. Random swapping is done with bit-blocks among different bit planes.
3. The shuffled four videos are XOR-ed. Under the control of Logistic maps, Four chaotic images are obtained from secret matrix.

In random block partitioning, bit planes are divided into randomly overlapping bit-blocks and to carry out encryption effectively, they are swapped among different bit planes.

Encryption Algorithm Detailed steps of our video encryption are illustrated as follows. STEP 1: Read and convert the input video into number of frames. Convert the four input gray scale frames of video sized $M \times N$ into 32 bit-planes.

STEP 2: Use Henon map to calculate the arrays D and F for determining random bit-block pattern.

STEP 3: Let the key k_1 be the seed of pseudo-random generator. Generate 32 random numbers and record them in an array G. Suppose that $B_{i,j}$ is the j-th bit-block of the i-th bit-plane. Thus, random bit-block swapping can be done as follows.

for ($i = 1; i \leq 32; i++$)

Exploit $D[i]$ and $F[i]$ to calculate random bit-block pattern. Let K be the total number of bit-blocks and $G[i]$ be the seed of pseudo-random generator.

$P = \text{mod}(\text{rand}(1, K) \times 248, 32) + 1$;

$Q = \text{mod}(\text{rand}(1, K) \times 248, K) + 1$;

for ($j = 1; j \leq K; j++$)

$m = P[j]$;

if ($m == i$)

if ($m == 32$)

$m = 1$;

else $m++$;

$l = Q[j]$;

Swap $B_{i,j}$ and $B_{m,l}$.

STEP 4: Convert 1st ~ 8th bit-planes, 9th ~ 16th bit-planes, 17th ~ 24th bit-planes, and 25th ~ 32nd bit-planes to four scrambled gray scale videos, respectively. Let these scrambled videos be I_1, I_2, I_3 and I_4 , respectively. Use Logistic map to generate a secure matrix C by the defined Equation. Calculate $J_1 = I_1 \oplus C, J_2 = I_2 \oplus C, J_3 = I_3 \oplus C, \text{ and } J_4 = I_4 \oplus C$, where \oplus is the XOR operation between the corresponding elements of input matrices.

STEP 5: The chaotic videos J_1, J_2, J_3 , and J_4 are viewed as encrypted frames of video. Consequently, an encrypted video is obtained by assembling these encrypted frames.

4. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

4.0.1 Information entropy analysis. In information theory, entropy is the most significant feature of disorder, or more precisely unpredictability. To calculate the entropy $H(X)$ of a source x, we have:

$$H(X) = - \sum_{i=1}^n Pr(x_i) \log_2 \frac{1}{Pr(x_i)} \quad (3)$$

where X denotes the test image, x_i denotes the i^{th} possible value in X, and $Pr(x_i)$ is the probability of $X = x_i$, that is, the probability of pulling a random pixel in X and its value is x_i . For a truly random source emitting 2N symbols, the entropy is $H(X) = N$. therefore, for a ciphered image with 256 gray levels, the entropy should ideally be $H(X) = 8$. If the output of a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security. The entropies for plain image and ciphered images using various images are calculated in Table 2. Apparently, the proposed algorithm is much closer to the ideal situation. This means that information leakage in the encryption process is negligible and the cryptosystem is secure against entropy attack.

4.1 Mean Square Error (MSE)

Mean Square Error (MSE) is the cumulative squared error between two digital images and can be used to check the avalanche effect. Let C_1 and C_2 are input image and encrypted image respectively, then MSE can be calculated as in Eq. 4 [?].

$$MSE = \frac{1}{M * N} \sum_{i=1}^N \sum_{j=1}^M [c_1(i, j) - c_2(i, j)]^2 \quad (4)$$

where M, N is the width and height of digital images and C1(i,j) is input image and C2(i,j) is encrypted image.

4.2 Peak Signal to Noise Ratio (PSNR)

Peak signal-to noise ratio can be used to evaluate an encryption scheme. PSNR reflects the encryption quality. It is a measurement which indicates the changes in pixel values between the plaintext image and the ciphertext image. Mathematically as in [?].

$$PSNR = 20 * \log_{10} \left[\frac{255}{MSE} \right] \quad (5)$$

Where MSE is mean square error between input image and encrypted image and can be calculated by using Eq. 4

4.2.1 Analysis of differential attack. A well-designed encryption algorithm should be highly sensitive to plain-image and keys, so a slight change in plain-image or keys will make the cipher-image quite different. If an encryption scheme contains no confusion or diffusion stage, it would easily be destroyed by differential attacks. In order to confirm whether the proposed encryption algorithm is sensitive to plain image and keys, this paper brings out two tests: Number of pixels change rate (NPCR) and Unified average changing intensity (UACI) [8]. The equation to calculate UACI is Eq. 6

$$UACI = \frac{1}{M * N} \sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{255} \times 100\% \quad (6)$$

Where, M stands for images width, N stands for images height, c1(i,j) means the gray-scale value of cipher-image in position (i,j), and c2(i,j) means the gray-scale value of the new cipher-image which is the encryption result of modified plain image that has just one different pixel to the original plain-image. NPCR can be calculated by Eq. 7

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M * N} \times 100\% \quad (7)$$

Where, M stands for images width, N stands for images height and where D(i,j) defined as follows

$$D(i,j) = \begin{cases} 1 & \text{if } C1(i,j) \neq C2(i,j); \\ 0 & \text{if } C1(i,j) = C2(i,j). \end{cases}$$

When one bit of a pixels gray-scale value in the plain image is changed, then a new plain image is generated from the original one. Encrypt the two images with the same secret keys, then take cipher images into Eqs. 6 and 7 and results are shown in Table 2.

5. CONCLUSION

Proposed algorithm involving Henon map & Logistic map, to enhance the security of the cryptosystem and to reduce the computation redundancy in traditional architectures. Firstly read the input video used for encryption. Then convert video into number frames. Each frame represented as (x,y,t) so convert these frames into images. Next images undergo permutation and diffusion operation. In permutation, position of pixel values gets changes because image has always highly correlation with its adjacent pixels. In diffusion process, alter the pixel values. Proposed method can be implemented in FPGA for real time application.

Table 1. Input and Encrypted Video frames


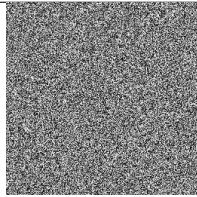

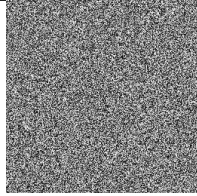

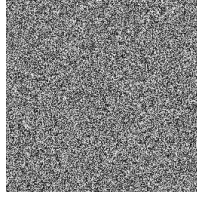

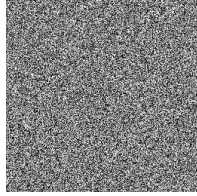
Input Video frames	Encrypted Video frames
	
	
	
	

Table 2. Performance analysis parameters

Parameters	Input Vedio			
	frame1	frame2	frame3	frame4
Entropy_in	7.5384	7.5387	7.5465	7.5350
Entropy_enc	7.9985	7.9984	7.9984	7.9984
MSE	34.7041	34.7041	34.7041	34.7041
PSNR	32.7270	32.7270	32.7270	32.7270
NPCR	99.6445	99.6345	99.6345	99.6345
UACI	32.7231	32.7231	32.7231	32.7231

6. REFERENCES

- [1] Zhou YC, Bao L, Chen CLP. *Image encryption using a new parametric switching chaotic system*. Signal Process 2013;93:303952.
- [2] Fu C, Meng WH, Zhan YF, Zhu ZL, Lau FCM, Tse CK, Ma HF. *An efficient and secure medical image protection scheme based on chaotic maps*. Comput. Biol Med 2013;43:100010.
- [3] Behnia S, Akhavan A, Akhshani A, Samsudin A. *Image encryption based on the Jacobian elliptic maps*. J Syst Softw 2013;86:242938.
- [4] Zhu HG, Zhao C, Zhang XD. *A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem*. Signal Process-Image Commun 2013;28:67080.
- [5] Sam IS, Devaraj P, Bhuvaneshwaran RS. *An intertwining chaotic maps based image encryption scheme*. Nonlinear Dyn 2012;69:19952007.

- [6] Ye GD, Wong KW. *An efficient chaotic image encryption algorithm based on generalized Arnold map*. *Nonlinear Dyn* 2012;69:207987.
- [7] Yue Wu, Joseph P. Noonan, *Shannon Entropy based Randomness Measurement and Test for Image Encryption* *Information Sciences* 00 (2011) 123
- [8] Yue Wu, Joseph P. Noonan, and Sos Aghaian, *NPCR and UACI Randomness Tests for Image Encryption* *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, April Edition, 2011.