RESEARCH ARTICLE OPEN ACCESS

A Brief Study of Video Encryption Algorithms

Pranali Pasalkar, Nirmala Nadar, Neha Panchal, Prof. Mrunali Desai
Department of Computer Engineering,
K.J.Somaiya Institute of Engineering and Information technology, University of Mumbai
Sion, India

Abstract—
Video is a set of images .Video encryption is encrypting those set of images .Thus video encryption is simply hiding your video from prying eyes .Video monitoring has always been in concerned .Multimedia security is very important for multimedia commerce on Internet such as video on demand and Real time video multicast. There are various video encryption algorithm. All have some kind of weakness .In this paper classification of various existing algorithm, its advantages and disadvantages is discussed.

Keywords—Video frames, Video Compression, Video encryption, Video Sequence, Chaos.

I. Introduction

Cryptography is a method to process data into unintelligible form, reversibly and without data loss, mainly digitally. Cryptography can be used to protect multimedia contents. Data cryptography mainly is the scrambling of the content of data, such as text, image, audio, video and so forth to make the data unreadable, invisible or unintelligible during transmission or storage called Encryption. The main goal of cryptography is keeping data secure form unauthorized attackers. Decryption is the process of taking encrypted data and converting into a form easily understandable by computer.

There are various application of digital video encryption as security and privacy is now major issue. Encryption of data is the only option available. Till now, various encryption algorithms have been proposed and widely used most of which are used for text and binary data. It is difficult to use them directly in video encryption as video data are often of large volumes and require real time operations. some video encryption algorithms have been reported.

For a video encryption algorithm, security, time efficiency are really important. Security is the basic requirement, which means that the cost- of breaking the encryption should be larger than buying the authorized video. The time efficiency means encryption and decryption should not take much time as heavy delay is not acceptable in real time.

In this paper, classification of different video encryption algorithms is presented, parameters on which video is encrypted and algorithms that comes under those classification is presented.

In Cryptography, keys play an important role, when no key is used then that cryptography is based on hash functions. When one key is used then it is known as secret key cryptography. When two keys are used then it is known as public key cryptography.In this paper, classification of different video encryption algorithms and techniques are presented

II. classification and parameters of video encryption techniques

A. Classification of video encryption

We classify video encryption algorithms in four categories.

Fully layered Encryption: In this encryption method, the entire content of the video is first compressed to reduce its size and then encrypted using standard algorithms like AES, DES,RSA etc. The disadvantage in this method is it is not suitable for real-time video encryption because there are lots of computation and speed also slow.

Scrambling based Encryption: The video encryption algorithms in this class mainly use different permutation algorithms to scramble or encrypt the video contents. Scrambling means re-positioning pixels and not manipulating it's value.

Selective Encryption: The algorithms using selective encryption selects only the needed bytes within the video frames and then encrypts it. Each and every byte of video data is not encrypted so the computational capacity reduces to a great extent.

Perceptual Encryption: In this type, the quality of video is partially degraded. The low quality video seen in many pirated videos is due to perceptual encryption.

Chaotic Encryption: Chaos provides a promising approach for cryptography. Chaos describes the behavior of dynamic non-linear systems i.e. present determines future but the approximate present does not determines the approximate future. The properties of Chaotic systems are sensitive to initial conditions, topological mixing and dense periodic orbits.

B. Parameters to test video encryption

There are few parameters to test the quality video encryption technique. They are as follows:.

Speed: Total time required by algorithm to encrypt is its computational speed.

Security: Video encryption algorithm are evaluated mostly on its security parameter .It should withstand various attacks like brute force attack, plain text attack etc.

Size: Encrypting video can increase its size, which in turn can increase computation time for video.so size of video encryption should be as small as possible.so compression of video is performed .

Encryption ratio: Encryption of video is the ratio between the size of encrypted part and the whole data size. Encryption ratio has to be minimized to reduce computational cost.

III. video encryption algorithm based on classification

Video encryption techniques and its algorithms are explained in details.

a. Algorithms

1.Fully Layered Encryption:

It encrypts each and every byte of video. It is the simplest way to encrypt videos. It is also called Naive algorithm. The algorithm guarantees the most security level. The encryption here is done by Triple DES so the decryption takes huge amount of time. So, this encryption is not suitable for real-time digital video. From the figure below we can see that each and every pixel is encrypted in this.

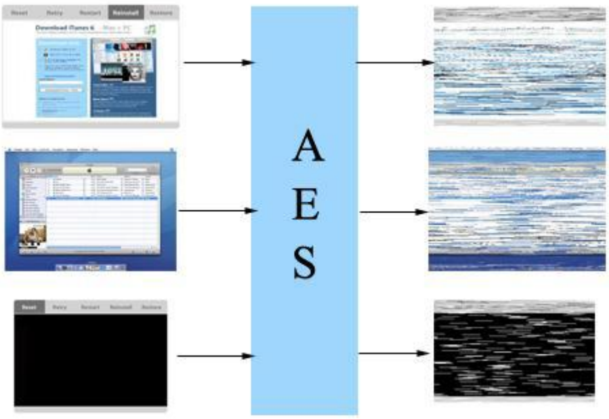

Figure 1: Fully layered encryption using AES encryption

2. Scrambling based Encryption

In this method, the frames or data within the video are scrambled. Scrambling is performed by permutation which means that the pixel value does not change but only its position changes. The disadvantage of this method is poor security and increased video file size.

.

2.1 A novel scrambling scheme for Digital video encryption

One of the novel method to encrypt data is to apply scrambling method to the compressed data after dividing the DCT coefficients of video data into 64 groups according to their positions in 8x8 size blocks and scrambled inside each group. Also motion vectors are grouped and permuted in term of their modes. The advantage of this method is less bit-stream overhead, no image quality degradation.[1]

2.2 A scalable frame scrambling algorithm for video encryption

This method treats video as a sequence of ordered frames and provide an algorithm to break this order of frames by first distributing frames into n frames-sequences and then by internally scrambling these frame sequences using proper keys. Thus the frames are ordered now in an incorrect order.

Advantages of this method is the content of the frames are not altered so it is extremely cost-efficient. It is also scalable.[2]

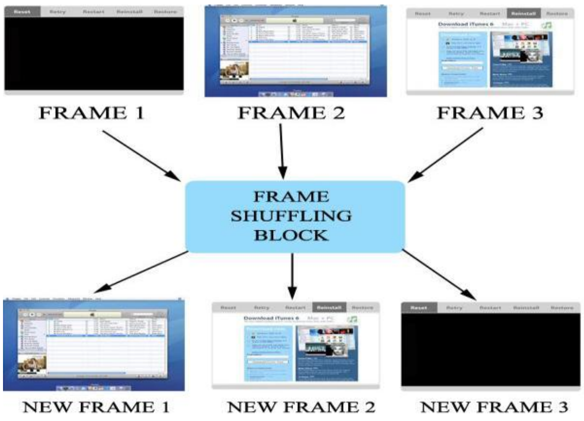

Figure 2: Scrambling of frames

3. Selective Encryption

To overcome the drawback of fully layered encryption, selective encryption is used. In fully layered encryption method, the whole content of video is encrypted but in selective encryption only the required partial video data is encrypted. It is also called partial encryption so in this method, there is reduced execution time and increased performance. One example of selective encryption in security field is the image acquired by a survey camera. For various reasons, this kind of images must be quickly transmitted and no full encryption is necessary. The security of selective encryption is always lower when compared to fully layered encryption. Below figure shows how normal selective encryption output looks like. only some part of video is encrypted and not entire one.

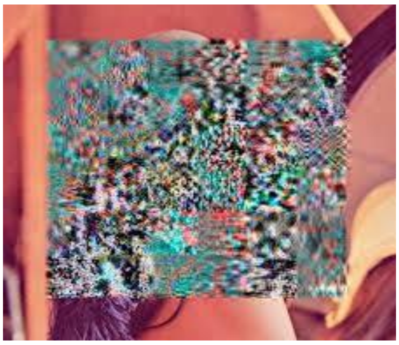

Figure 3: selective video encryption

3.1 Face Protection by Fast Selective Encryption in a Video

The purpose of this method is to selectively encrypt on the face of the human. It is based on AES stream ciphering using VLC(Variable Length Coding) of the Huffman’s vector. Thus it only encrypts a small part of the image [3]

3.2 A Real-time MPEG Video Encryption Algorithm using AES

In this method, only active video data are encrypted with Advanced Encryption Standard(AES) crypto algorithm and a self-synchronized cipher key mechanism based on the embedded video Timing Reference Signals(TRS) was designed to overcome the security leakage in Electronic Codebook(ECB) mode and to reduce the possibilities attacks which are used to recover the encryption key like brute force attacks. This saves upto90% time compared to other algorithm which encrypt whole video data. So this type of algorithm can be used for real-time video encryption type of system [4].

4 . Perceptual Encryption

In perceptual encryption, the quality of visual data is partially degraded by encryption. We can say that intentionally degrading the quality of the video by means of encryption, whereas the part of the data that remains untouched can be processed by the respective decoder without requiring access to the encryption key.

For example, we can use perceptual encryption to degrade the quality for a free online review of some movie and only if one pays for the content one obtains access to encryption key and thus to full quality content. from figure below we can see that quality of video is degraded.

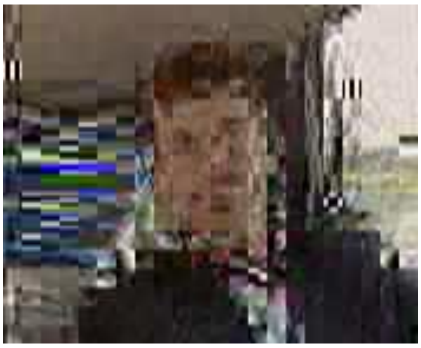

Figure 4:perpetual based encryption

4.1. On the Design of Perceptual MPEG-Video Encryption Algorithms

This algorithm selectively encrypts Fixed Length Codewords(FLC) in MPEG-video bit streams under the control of three perceptibility factors. It can be applied to both stream cipher and block cipher. When the block cipher is selected for perceptual encryption it is first concatenated together to form a longer bit stream the each block of the bitstream is encrypted. The encrypted FLC data element is placed back into its original position in the video stream. It has advantages such as size-preservation, support many applications because of multiple perceptibility[5].

4.2. A Prediction Reference Structure based Hierarchical Perceptual Encryption Algorithm for H.264 Bitstream

The idea about correspondence between the degree of video motion of macroblock(MB) should be known for this type of encryption. The frames to be encrypted are selected dynamically according to the degree of motion. At MB layer, MBs to be encrypted are selected based on their MRRs. And finally at bitstream layer, the most significant bits for reconstructed video quality are encrypted on the basis of the bit-sensitivity of H.264 bitstream [6].

5. Chaos Encryption

Chaos based cryptographic algorithms use dynamical algorithms defined on a set of real numbers. Thus chaos is mathematical study of non-linear dynamic systems. Chaos means present determines the future, but the approximate present does not approximately determine the future. The aim and objective of chaotic encryption system is to encrypt and decrypt real-time video using chaotic algorithm. To maintain security of the system without hampering the information within the video.

The properties of chaos are:

1. Sensitive to initial conditions.
2. Topology mixing.
3. Dense periodic orbits.

1. Sensitive to initial condition

As discussed earlier, deterministic is process whose resulting behavior is entirely determined by its initial state and inputs.

It is process having only one output and small change in initial behavior may give different future behavior .

For example: If we take the initial value of x1 = 0.1,x2 = x1* 3 which is 0.3,x3 = x2 * 3 =0.9

But, if we approximately consider the value of x1 as 0.12 ,then x2 will be 0.36 and x3 will be 1.08.

2.Topology mixing

No matter how close together two points are no matter how long their trajectories are close together, at any time, they can suddenly go in completely different directions.

3.Density of periodic orbits

It repeats itself after a certain period.

Example: Consider a equation x = 4x(1-x)

x1=0.34, x2=0.90, x3=0.34

i.e. it repeats itself after period=2

Figure shows chaos based encryption process.

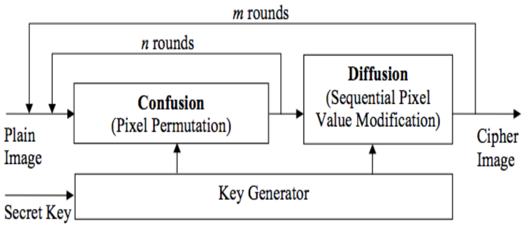

Figure 5 :chaos based encryption

5.1. Chaotic Video Encryption Scheme for Real-time Digital Video(CVES)

Chaotic Video Encryption Scheme is a novel video encryption scheme based on multiple digital chaotic systems. In CVES, **Error! Reference source not found.** chaotic maps are used to generate pseudo-random signal to mask the video, and to make pseudo-random permutation of masked video .Another chaotic map is emphasized to initialize and control the above **Error! Reference source not found.** chaotic map. This algorithm provides high security so it can be easily extended to other real-time application. It can be realized by both hardware and software [7].

5.2 A video encryption method based on chaotic maps in DCT domain

This method includes two key operations: scrambling I-frames and encrypting I-frames, and uses three chaotic maps (two coupling chaotic maps and one chaotic map).

The process is as follows:

1. Select I-frames of the video sequence for encryption.
2. Introduce 2 coupling chaotic maps to scramble the DCT coefficients of every original I-frame.
3. Encrypt DCT coefficients of the scrambled I-frame using another chaotic map.

It has five keys in the whole process which are found to be difficult, and the changes of the I-frames can bring much influence on the whole video. As verified by various test results, this frame encryption method is secure [8].

5.3 A Multiple chaotic video encryption based on DM642

In this paper, logistic mapping is used to design a kind of encrypted system applicable to DM642. At the same time, safety comes to a new step because it guarantees that each frame has a different encryption sequence and the processes of scrambling and diffusion get integrated. It can not only gain higher security but also achieve instant communication.[9]

IV. CONCLUSION:

In this paper, currently known video encryption algorithms for video streams were described. Fully layered encryption is not suitable for real-time video applications due to heavy computation and slow speed. . In scrambling/permutation based algorithm encryption security is low, speed is fast but it is vulnerable to known-plaintext attack. Selective encryption algorithm is fast but encryption ratio is low. Perceptual encryption is not secure against known-chosen plaintext attack Chaos based video encryption is best for real-time video encryption because of low computational complexity, invariance of compression ratio, format compliance, real-time, multiple levels of security, and strong transmission error tolerance and hence, it is superior over other conventional encryption methods. Chaos based video encryption can be implemented in hardware as well as software which we can see from paper [7] .

Reference

[1] Chen, Zhenyong Xiong, Zhang,Tang, Long., ”A Novel Scrambling Scheme for Digital Video Encryption”,Springer Berlin Heidelberg,2006-01-01, Book Section, 2006,978-3-540-68297-4,Advances in Image and Video Technology,Lecture Notes in Computer Science.

[2] Rajpurohit, J.; Khunteta, A., "A scalable frame scrambling algorithm for video encryption," *Information & Communication Technologies (ICT), 2013 IEEE Conference on* , vol., no., pp.981,985, 11-12 April 2013.

[3] Joslle Rodrigues, William Puech, Peter Meuel, Jean-Claude Bajard, Marc

Chaumont. Face Protection by Fast Selective Encryption in a Video. IET THE CRIME AND SECURITY Conference, Jun 2006, pp.420-425. <lirmm-00109723> .

[4] Jayshri Nehete, K. Bhagyalakshmi, M. B. Manjunath, Shashikant Chaudhari, T. R. Ramamohan "A Real-time MPEG Video Encryption Algorithm using AES ", unpublished.

[5] Shujun Li, Guanrong Chen, Albert Cheung, Bharat Bhargava,KwokTung Lo , " On the Design of Perceptual MPEG-Video Encryption Algorithms ",IEEE transaction on circuits and system for video technology, vol. 17, no. 2, pages 214-223, February 2007.

[6] Haojie Shen, Li Zhuo, and Yirui Li "A Prediction Reference Structure Based Hierarchical Perceptual Encryption Algorithm for H.264 Bitstream", Signal & Information Processing Lab, Beijing University of Technology, Beijing 100124,China .

[7] Shujun Lia, Xuan Zhengb, Xuanq in Moua and Yuanlong" Chaotic Video Encryption Scheme for Real -Time Digital Video", Year 2002

[8] Shuguo Yang , Shenghe Sun," A video encryption method based on chaotic maps in DCT domain" , School of Electrical Engineering and
Automation, Harbin Institute of Technology, Harbin 150001, China
Received 17 October 2007; received in revised Received 17 October
2007; received in revised.

[9] Xiangzhu Long, Jishen Li , Youjun Hu " A Multiple Chaotic Video Encryption System Based on DM642",2013 Ninth International Conference on Computational Intelligence and Security.