Australian Journal of Basic and Applied Sciences, 8(3) March 2014, Pages: 120-125

AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

Multimedia Security With Multi Agent System

[1]B.R. Shunmugapriya and [2]K.L. Shunmuganathan

[1]*Research Scholar, Information and communication engineering, Anna University, Chennai, Tamil Nadu, India.*
[2]*Professor, RMK Engineering College, information and communication engineering, Chennai, Tamil Nadu, India.*

ARTICLE INFO

Article history:
Received 20 November 2013
Received in revised form 20 March 2014
Accepted 25 March 2014
Available online 2 April 2014

Key words:
Multimedia Security, Multi Agent System, Encryption, MPEG.

ABSTRACT

The recent growth of networked multimedia systems has increased the need for the protection and security of digital multimedia. Security and privacy issues of the transmitted data have become an important concern in multimedia technology. The secured transmission of digital data is based on cryptography. In this paper, we propose a system Multimedia Security with Multi Agent System(MSMAS) with Multi-Agent System (MAS) concepts that facilitates the encryption process. We encrypt only the selected frames of MPEG video data. In these frames the DC components which are with high energy are encrypted. The encryption algorithm and the keys involved are dynamically selected by the agents according to the user, application and the threat on the channel. This system works autonomously with multi-applications and multi-clients more dynamically and efficiently.

To Cite This Article: B.R. Shunmugapriya and K.L. Shunmuganathan., Multimedia Security With Multi Agent System. ***Aust. J. Basic & Appl. Sci.,*** *8(3): 120-125, 2014*

INTRODUCTION

Multimedia (Durfee, E.H., *et al.*, 1989) is interacting with information that employs most or all of the media such as text, graphics, images, audio and video. The recent growth of networked multimedia systems has increased the need for the protection and security of digital multimedia. Generally multimedia security is different from text/binary data security since multimedia content is often of large volumes, with interactive operations, and requires real-time responses. Multimedia security in general provided by a method or a set of methods that are used to protect the multimedia content. These methods are based on cryptography.

We focus on secure multimedia transmission and distribution than on multimedia content protection. In particular we concentrate on secure real time video transmission. Few applications of secure real time video transmission are video conferencing, video on demand, video broadcasting, Pay-TV, etc…Multimedia security is in close relation with these applications. Different applications require different methods and different levels of security measures for content transmission or distribution. For secure video transmission encryption can be used, and for dynamic selection of encryption algorithms Multi-Agent System is used.

The naive approach for video encryption is to treat video data as text and encrypt it using standard encryption algorithms like AES (Advanced Encryption Standard) or DES (Data Encryption Standard) (Frederic Andre, 2001). The basic problem with these encryption algorithms is that they have high encryption time. They also result in vast increase in size of the video, making them unsuitable for real-time applications. Another one approach is selective encryption (Frederic Andre, 2001) where in only selected parts of the video data are encrypted based on the security requirements. This requires special encoder and decoder. And also various algorithms like ZIG-ZAG permutations (encrypting before compressing), Video Encryption Algorithm (VEA), Pure Permutation Algorithm (not secure if the permutation is figured out) are existing with their own limitations.

We would like to consider the MPEG video data which will be compressed using DCT. These DCT coefficients can be classified into two groups (Agi and L. Gong, 1996). DC and AC. DC is the mean value of a block. All the other coefficients describe the variation around this DC value and these are called AC coefficients. However, most of the energy is contained in the DC and a few AC coefficients. In our algorithm we will apply any one of the classical encryption algorithm like DES, AES or RC5 and encrypt the DCT coefficients whose energy level is high. The rest will be send as such. By which the computational efficiency can be improved and the video can be transmitted with high security.

This paper has been organized in the following manner. In the first section the working principles of MPEG has been discussed, which is followed by the Encryption and Decryption procedures. This section is followed by

Corresponding Author: B.R. Shunmugapriya, Research Scholar, Information and communication engineering, Anna University, Chennai,tamil nadu, india.

our study and analysis on various encryption algorithms available for video protection. The paper is concluded with our proposed system and its features.

Basic Concepts Of Video And Video Encryption:

Video:

Video is basically a three-dimensional array of color pixels. Two dimensions serve as spatial (horizontal and vertical) directions of the moving pictures, and one dimension represents the time domain. A data frame is a set of all pixels that correspond to a single time moment. Basically, a frame is the same as a still picture.

Video data contains spatial and temporal redundancy. Similarities can thus be encoded by merely registering differences within a frame (spatial), and/or between frames (temporal). Spatial encoding is performed by taking advantage of the fact that the human eye is unable to distinguish small differences in color as easily as it can perceive changes in brightness, so that very similar areas of color can be averaged out in a similar way to jpeg images. With temporal compression only the changes from one frame to the next are encoded as often a large number of the pixels will be the same on a series of frames.

MPEG Background:

MPEG (Moving Picture Expert Group) (Narsimha Raju, C., *et al.*, 2008) is an industrial standard for video processing and is widely used in multimedia applications in the Internet. But no security procedure is specified in this standard. A MPEG video is composed of a sequence of Group of Pictures (GOPs). Each GOP consists of three types of frames namely I, P and B. I frames are called intra-coded frames and are compressed without reference to any other frames. They are split into non-overlapping blocks (intracoded) of 8 × 8 pixels which are then compressed using Discrete Cosine Transform (DCT), Quantization (Q), Zigzag scan, followed by Run-length coding and entropy coding.

The P and B frames are forward predictive and bidirectional predictive coded frames, respectively. These are subjected to compensation by subtracting a motion compensation prediction. The residual prediction error signal frames are split into non-overlapping blocks (inter-coded) of 8 × 8 pixels which are compressed in the same way as the blocks of intra-frames. Sometimes, P and B frames also have some intra-coded blocks when better efficiency will be obtained using intra-coded compression. These intra-coded blocks are called I-blocks in P and B frames.

Encryption/Decryption:

The process of converting plaintext to ciphertext is called enciphering or encryption. Restoring plaintext from cipher text is deciphering or decryption. Both the encryption and decryption algorithms take a key (K) and plaintext/ciphertext as input. In the case of images, plaintext is a set of pixel values arranged in an orderly manner. Encrypting images/videos constitutes reordering these pixel values so that they convey no visual information about the original image.

An image/video can also be encrypted in the compressed domain. In this case, the DCT coefficients are encrypted in such a way that the content is made illegible for the unauthorized. Only an authorized user can get back the original content using the decryption algorithm. In cryptography, a block cipher is a symmetric key cipher which operates on fixed-length groups of bits, termed blocks, with an unvarying transformation. When encrypting, a block cipher might take an n-bit block of plaintext as input and output a corresponding n-bit block of cipher text. The exact transformation is controlled using a second input – the secret key. Decryption is similar, takes an n-bit block of cipher text together with the secret key and outputs the original n-bit block of plaintext. Examples of block ciphers are RC5, AES, DES, Blowfish, etc.

Survey on Video Encryption:

Communication security of digital images and textual digital media can be accomplished by means of standard symmetric key cryptography. Encrypting the entire multimedia stream using standard encryption methods is referred to as the naive algorithm. However, due to variety of constraints (such as near real-time speed,) communication security for streaming audio and video media is harder to accomplish. Communication encryption of video and audio multimedia content is not simply the application of established encryption algorithms, such as DES or AES, to its binary sequence. It involves careful analysis to determine and identify the optimal encryption method when dealing with audio and video media. This section analyses different types of algorithms available for video encryption.8 discussed below.

Naive Approach:

Classical encryption schemes are designed for encryption of textual or numeric data. Naïve approach uses this. In general, video data is huge (a frame can have 40, 000 bits and their would be 25-30 frames per second). The information value of video data is far less than that of an equal amount of text data. Even then, for better security, video data is encrypted by using classical algorithms (DES, AES, RC5 etc.). This causes delay in processing and is not suitable for real-time applications

Selective Video Encryption:

In order to meet real-time constraint for audio and video multimedia playback, selective encryption [8] is used. The basic idea of selective encryption is to encrypt only a portion of the compressed bit stream. For example, we can select only the most important coefficients from either final or intermediate steps of a compression process and encrypt those. Less important coefficients are left unencrypted or lightly scrambled. Typical examples of selective encryption for videos are Secure MPEG by Agi and Gong , zig-zag permutation by Tang, VEA by Qiao and Nahrstedt

Secure MPEG (SECMPEG):

Meyer and Gadegast (Frederic Andre, 2001) introduced a selective encryption method applicable to MPEG standard. SECMPEG is designed with four different levels of security. At the first level, SECMPEG encrypts the headers from the sequence layer to the slice layer, while the MVs and DCT blocks are unencrypted. At the second level, most relevant parts of the I-blocks are encrypted (upper left corner of the block) in addition. At the third level, SECMPEG encrypts all I-frames and all I-blocks. Finally, at the fourth level, SECMPEG encrypts the whole MPEG sequence (naive approach).

The selective encryption in SECMPEG (levels 1, 2, and 3) has some weaknesses. It is shown that even though single P- or B-frame on its own carries almost no information without the corresponding I-frame, a series of P- or B-frames can tell a lot if their base I-frames are correlated. The experiments in [AG96] by Agi and Gong show that encrypting I-frames only may leave visible I-blocks in other frames.

Zig-Zag Permutation:

Zig-zag permutation algorithm has encryption embedded into the MPEG compression process. As we saw in earlier discussion, JPEG and I-frames of MPEG undergo a zig-zag reordering of the 8x8 blocks. The zigzag pattern forms a sequence of 64 entries that are ready to enter entropy encoding stage (compression). The main idea of Tang's approach is to use a random permutation list to map the individual 8x8 blocks to a 1x64 vector. The Algorithm is consisted of three stages: In the first stage a list of 64 permutations is generated and in second stage Splitting procedure on an 8x8 block is performed as follows:

Denote DC coefficients by an 8 digit binary number with digits b7b6b5b4b3b2b1b0. This binary sequence is then split into two equal halfs: b7b6b5b4 and b3b2b1b0. Finally, place number b7b6b5b4 into DC coefficient and the number b3b2b1b0 as the AC63 (the last AC coefficient) which is the least important value in the block. This will result in no visible degradation of the quality. In stage 3 the random permutation is applied to the split block.

However, the Zig-Zag permutation algorithm is not particularly secure. There are two types of attacks possible on zigzag permutation (Agi and L. Gong, 1996). They are known-plaintext attack, and cipher text-only attack. Known-plaintext attack is particularly applicable to videos with known clips such as blank screens, the movie rating screens, MGM roaring lion, etc. If these known frames are used as a comparison, the adversary can easily generate the secret permutation list. Cipher text only attack is a model for cryptanalysis where the attacker is assumed to have access to a set of cipher texts and knows that encryption algorithm.

This is most difficult attack since the cryptanalyst has access only to the encrypted data.RC5 with four rounds of encryption and key size of 128 bits can be broken if 217 cipher texts are available.

3.2.3. Video encryption Algorithm (VEA):

The Video Encryption Algorithm by Qiao and Nahtstedt [6] is constructed with goal to exploit the statistical properties of the MPEG standard. The algorithm consists of several steps. They are

Step 1: Let the 2n byte sequence denoted a1a2: : : a2n represent the chunk of an I-frame.

Step 2: Create two lists, one with odd indexed bytes, and the other with even indexed bytes.

Step 3: Xor the two lists into an n byte sequence denoted with c1c2 : : : cn.

Step 4: Apply the chosen symmetric cryptosystem E (for example DES or AES) on odd list and create ciphertext c1c2 : : : cn .

The security of this method is very close to the security of the encryption scheme E that is internally used. The speed of this algorithm is roughly 1/2 of the speed of naive algorithm, but that is still large amount of computation for real-time high quality videos.

MPEG Encryption Scheme:

The most frequently used idea of MPEG encryption is to encrypt selective frames, macro blocks, DCT coefficients and/or motion vectors. The following is a list of selective data encryption in different schemes.

- All header information

- Selective AC coefficients of Y/V blocks in all I-frames.
- Selective leading DCT coefficients of each block
- Selective DCT coefficients of each block and motion vector
- All or selective motion vectors.
- All I-frames and header of MPEG video sequence.
- All I-frames and P-frames or all I frames and I-macro blocks of B and P frames
- All or selective I macro blocks and the headers of all predicted macro blocks.

Proposed System:

Surveys reveal that, selective encryption algorithm is better than naïve algorithm. So as a first step we would like to consider only a portion of the video data and encrypt that with any one the classical encryption algorithm. Here we have considered the MPEG video data which will be compressed using DCT. These DCT coefficients can be classified into two groups. DC and AC. DC is the mean value of a block. All the other coefficients describe the variation around this DC value and these are called AC coefficients. However, most of the energy is contained in the DC and a few AC coefficients.

In our algorithm we will apply any one of the classical encryption algorithm like DES, AES or RC5 and encrypt the DCT coefficients whose energy level is high. The rest will be send as such. By which the computational efficiency can be improved and the video can be transmitted with high security.

Since different applications require different methods and different levels of security measures for content transmission or distribution we have incorporated the Multi Agent System in our proposed system. The encryption algorithm, the keys used for encryption is selected dynamically according to the users, threats on the channel, and the application required.

In MSMAS we have five agents and each with its own responsibility. The agents are included because of their features. The agents are intelligent, Autonomous, Pro-active, Re-active, Communicative and Co-operative, Negotiable, and capable of Learning. In fact, the multi-agent system (MAS) is a technique in the artificial intelligence area focusing on the system where several agents communicate with each other. In [14], multi-agent system is defined as “a loosely coupled network of problem-solver entities that work together to find answers to problems that are beyond the individual capabilities or knowledge of each entity”.

The architecture of the proposed system is shown in Fig.1.

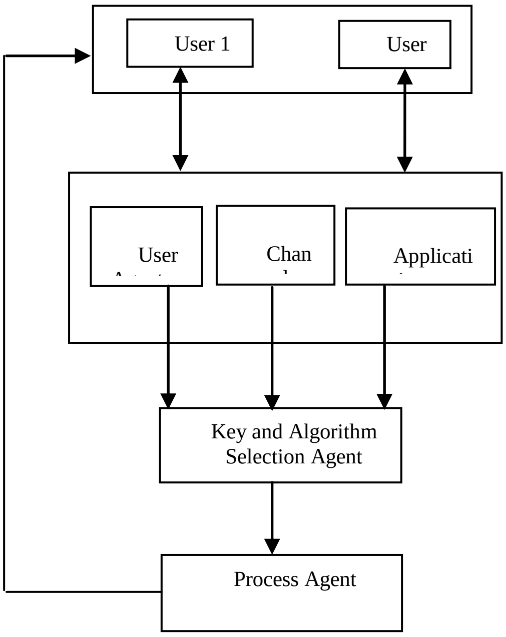

Fig. 1: Architecture of MSMAS

Functionalities of the Agents:

The responsibility of each agent in the system is given below.

User Agent:

Profile of the different users will be maintained by this agent. This keeps on learning the behavior of the users and determines the level of security required for a particular user.

Channel Agent:

The level of threats on the channel is calculated by this agent. This value will be produced after the thorough analysis of the channel.

Application Agent:

This agent checks for the applications requested by the users. Because, the cost of multimedia information to be protected shouldn't be less than the cost of protection itself. So the different applications like video on demand, Video conferencing, etc. require different levels of security, this agent produces a level of security value based on these applications.

Key and Algorithm Selection Agent:

The encryption algorithm and the keys involved are selected more dynamically by this agent. It considers the values produced by the above three agents to decide upon the algorithm and key. The agent will select any one of the classical encryption algorithm like DES, AES, RC5.

Process Agent:

The process of encryption is carried out by this agent. This agent takes only the I frames of the video. Figure 2. shows different types of frames in MPEG. I frames are the intra coded frames encoded as standard JPEG images without reference to other frames. And these are not predictable. But the P-frames are encoded with reference to the I frames, containing only the difference between the two consecutive frames. The B-frames are bidirectionally interpolated using the previous closes I/P frame and the following closest I/P frames.

Since the I frame plays a vital role they are considered for encryption.

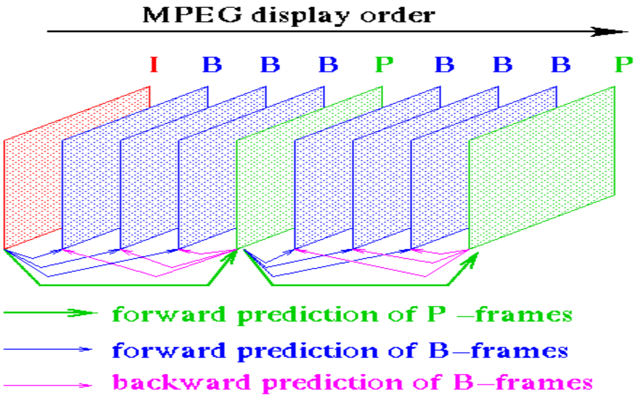
MPEG display order
I
B
B
B
P
B
B
B
P
forward prediction of P –frames
forward prediction of B–frames
backward prediction of B–frames

Fig. 2: MPEG video frames

MPEG as the video file format compressed using DCT. DCT coefficients may be DC or AC. Since most of the energy is contained in DC and few AC components we encrypt the DC components which are with high energy. The encryption algorithm and the key are produced by the key and algorithm selection agent. After encryption the data are transmitted. Since agents are involved, they can cooperate with each other and do the process more effectively and efficiently.

Conclusion:

Image and video encryption plays a more and more important role in today's multimedia world. Although many encryption schemes have been proposed to provide security for digital images and videos, some of them are too weak to resist various attacks designed by cryptanalysts. So ,to design a truly secure image/video encryption scheme, any one of the classical cryptography methods is employed based on the user, application required, and the threat on the channel and this is achieved by incorporating Multi Agent System. This makes the system to work more dynamically and efficiently. To fasten the encryption process only selected portions of the video frames are encrypted. So the proposed MSMAS system is more secure and efficient in terms of cost and time.

REFERENCES

Agi and L. Gong, 1996." An empirical study of secure MPEG video transmission", In Proc. of the Internet Society Symposium on Network and Distributed Systems Security, pp: 137-144.

Borko Furht, Daniel Socek, 2003. "A survey of Multimedia Security", Florida Atlandic University.

Chen, Z., Z. Xiong and L. Tang, 2006.“A novel scrambling scheme for digital video encryption”, In Proc. of Pacific-Rim Symposiumon Image and Video Technology.

Durfee, E.H., V.R. Lesser and D.D. Corkill, 1989. Trends in Cooperative Distributed Problem Solving. In: IEEE Transactions on Knowledge and Data Engineering,, KDE-1(1), pp: 63-83.

Frederic Andre, 2001. “Multimedia and Security”, IEEE.

Gang Liu, Takeshi Ikenaga, Satoshi Goto And Takaaki Baba, 2006. “A Selective Video Encryption Scheme For MPEG Compression Standard”, IEICE Transactions On Fundamentals Of Electronics, Communications and Computer Sciences, E89-A(1): 194-202.

Missouri, A., F. Lefebvre, C. De Vleeschouwer, B. Macq and J.-J. Quisquater, 2008. ”Overview on Selective Encryption of Image and Video: Challenges and Perspectives”,EURSIP Journal on Information Security, Article ID 179290, pp: 18.

Narsimha Raju, C., Ganugula Umadevi, Kannanan Srinathan, 2008. “Fast and Secure Real Time Video Encryption”, IEEE Computer Society, IEEE.

Palmer, W., Agnew, Ane S. Kellerman, “Fundamentals of Multimedia” , Chapter1.

Shiguo Lian, Dimitris Kanellopoulos, Giancarlo Ruffo, 2009. “Recent Advances in Multimedia Information System Security”, Informatica., 33: 3-24.

Shiguo Lian,Yan Zhang,Stefanous Gritzalis,Yu Chen, 28/1/09.”Multimedia Security in Communication”, Journal of Universal Computer Science, 15(2): 398-400.

Shujun Li, Guamrong Chen, Xuan Zheng, “Chaos-Based Encryption for Digital Images and Videos”,Chapter 4.

Wail, S., Elkilani, Hatem M. Abdul-Kader, 2009. “Performance of Encryption Techniques for Real Time Video Streaming”,978-1-4244-3778-8/0, IEEE Computer Society, IEEE.

William Stallings,”Cryptography and Network Security”, Third Edition.