Proceedings of the 5th WSEAS Int. Conf. on MULTIMEDIA, INTERNET AND VIDEO TECHNOLOGIES, Corfu, Greece, August 17-19, 2005 (pp149-153)

Partial selection scheme of MPEG-1 stream for the purpose of encryption using Open SSL Libraries

ANURADHA JAGANNATH, DR. K.R.RAO
Department of Electrical Engineering
The University of Texas at Arlington
416, Yates street, Box 19016, Arlington, Texas 76019
UNITED STATES OF AMERICA

Abstract: - Modern day communications require that the information be transmitted in a secure manner with due importance given to bandwidth requirements. This gains more importance in lieu of the ever-increasing use of the internet in today’s world. The SEAL algorithm is a stream cipher that has some drawbacks when taking factors like licensing and standardization into consideration. This paper focuses on a widely used form of encryption, DES and RSA, using Open SSL libraries, implemented on a partially selected MPEG1 encoded stream, thus taking care of the bandwidth factor also. The new scheme evolved, is more efficient than the previously proposed scheme.

Key-Words: - Algorithms, DES, Encryption, MPEG1, Open SSL, RSA, Video

1 Introduction

Multimedia has come to play a major role in numerous applications and the increase in its popularity has given rise to a demand on the data storage and transmission techniques [1]. The easy interception of data in network communications, especially in the wireless environment, has led to the essentiality of the protection of communications. Encryption and decryption provide a solution to the problem but are not very efficient in terms of real time processing and communication of image and video. Also, the recent increases in the use of World Wide Web and video conferencing, which are in reality, image and video applications, has led to further emphasis of this problem. The limitations of communication bandwidth and storage have led to data compression. Encryption is combined with the compression, for protection of privacy of the users. Typically, a suitable compression algorithm is implemented on the multimedia data and its results are encrypted by an encryption scheme and this whole process is reversed at the other end by the decoder [2]. Also, as a result of the increasing demand of Internet based Electronic Commerce, the need for securing data and commercial transactions has increased [3].

2 MPEG1

2.1 Introduction

Communications is synonymous to standards, but is faced by the problem of existence of various approaches to standardization by the numerous industries [4]. MPEG (Moving Picture Experts Group) is a family of standards used for coding audio-visual information in a digital compressed format. The major advantage of this group of standards compared to other video and audio coding formats, is the smaller size of files for the same quality, attributed to the very sophisticated compression techniques used by them. It recognized the importance of bandwidth and number of pixels per second, over the number of lines or number of fields per second, in the digital domain for a television signal [5]. MPEG1 was the first standard to come out of the MPEG working group [6][7].

2.2 MPEG1

Its initial target was compressed video and audio signals at a bit rate of 1.5Mbps. This bit rate was chosen because it was the data rate for a CD running at normal speed. In 1988, work on MPEG1 began and in 1993, the international standard, IS 11172-2 was published [5]. The MPEG1 standard has five parts dealing with systems aspects, video compression, audio compression, compliance testing and software reference model. These together make up a standard, which defines an MPEG1 bit stream as well as the exact requirements for building an MPEG decoder.

MPEG1 has five parts: The first of these deals with the system aspects of MPEG1 that defines a system layer, which provides an envelope for the compression layers, for storing the compressed video data. The second part deals with video compression and compressed video data, defined in a bit stream. It can be used for compressing video sequences - both 625-lines and 525-lines - to bit rates around 1.1 Mbps. It defines how to decode the data to achieve a visual representation but not how the data is to be compressed. The third part deals with audio compression and compressed audio for both mono and stereo audio, defined in a bit stream. It deals with audio perception models of the human ear and techniques by which lossy audio compression has no perceivable differences in the resulting audio. The fourth part of the standard deals with compliance testing and specifies how bit streams and MPEG1 decoders can be tested to ensure that they comply with the standard. The fifth part of the standard is the software reference model and the software for both an encoder and an arithmetically correct decoder.

MPEG1 video compression is defined in part two of the MPEG1 standard. The syntax permits sampling dimensions as high as 4095 x 4095 x 60 frames per second and is considered as a kind of subset known as Constrained Parameters Bit stream (CPB), a limited set of sampling and bit rate parameters used to normalize computational complexity, buffer size, and memory bandwidth. MPEG1 audio compression based on the psycho-acoustic model and offers a compression ratio from 2.7 to 24. The encoder functions on the basis that the original audio stream passes through a bank of filters for conversion of audio data into multiple sub bands of frequency values and a psycho-acoustic model determining the ratio of signal energy to masking threshold for each sub band. The decoder unpacks the bit stream, reconstructs the frequency samples and converts them into a raw audio data stream. The system stream is a binary stream defining the MPEG-1 file, encapsulating the audio and video streams, and is passed to the decoder to be decoded and played, as a representation of the movie.

3 Encryption

3.1 Introduction

Encryption deals with the task of security, which is required so that the legitimate users have access when they need it and the unauthorized users are kept out. There are some security threats like information disclosure or leakage, integrity violation, masquerading, denial of service and illegitimacy. Security can be extended to channels of higher bandwidth or smaller delay, when a secure channel exists along which keys can be transmitted and encrypted messages can be sent [10]. The algorithms developed for securing text data may not be suitable for multimedia applications due to the large data sizes and real time limitations. Authentication control mechanisms can be used to secure multimedia data broadcast on wireless, satellite, or Mbone networks [11]. Cryptography [1] is the art or science of storing information for shorter or longer periods of time in a form that allows it to be revealed to those you wish to see it and yet hides it from all others. A cryptosystem is a method to accomplish this and cryptanalysis is the practice of defeating such attempts to hide information. Cryptology is the amalgamation of both cryptography and cryptanalysis.

3.2 Encryption schemes

Two classes of key-based encryption algorithms are symmetric (private key) and asymmetric (public key). The key forms the basis of encryption and hence its strength against attack is an important feature, which is determined by its length such that for a given encryption algorithm the longer the key, the stronger the key.

Private Key encryption also referred to, as conventional or symmetric or single-key encryption was the only available option prior to the advent of Public Key encryption. It is simpler of the two classes of key-based encryption algorithms and uses the same key to encrypt and decrypt the message. It requires all parties that are communicating to share a common key and is essential that the sender and receiver have a way to exchange secret keys in a secure manner [12]. Symmetric algorithms can be categorized into block ciphers and stream ciphers.

Block ciphers take a number of bits (typically 64 bits in modern ciphers), and encrypt them as a single unit. It transforms a fixed-length block of plaintext data into a block of cipher text data of the same length under the action of a user-provided secret key. *Stream ciphers* encrypt each bit of plaintext to a single bit of cipher text and the reverse operation is carried out at the destination. The stream cipher operates by XORing the plain text with the random number generated and hence the importance of the efficiency of the random number generator. [1-3, 12] DES is the popularly used secret cryptosystem and published as federal information processing standard (FIPS) [11]. This scheme is a block cipher with 64 blocks, 16 rounds, and a key length varying up to 56 bits. In the electronic code book (ECB) mode, it encrypts in blocks of 64 bits and is used in the cipher block-chaining mode to improve the crypto graphical strength.

Public key encryption is important because messages enciphered by it cannot be broken by randomly trying out all possible keys, even with powerful computers that try thousands of keys a second. Public key encryption is based on the premise of making the encryption and decryption keys different by which the knowledge of one key would not allow a person to find out the other key. Each sender and recipient have a private key, known only to him/her and a public key, which can be known by anyone, such that each encryption/decryption process requires at least one public key and a private key.

RSA is named after its three inventors, Rivest, Shamir and Adleman and is the most widely used public-key cryptosystem. It may be used to provide secrecy and digital signatures with its security, based on the intractability of the integer factorization, and hence the security depends on the largeness of the number to be factored. The speed of the RSA algorithm is about 100 times less than DES though RSA is a popular and reliable algorithm [10].

4 A NOVEL MPEG-1 PARTIAL ENCRYPTION SCHEME FOR THE PURPOSES OF STREAMING VIDEO

4.1 Introduction

A partial selection scheme for the purpose of encryption of MPEG-1 [7] [8] [13] bitstream uses only a part of the bitstream for encryption while the rest is left as plaintext. This algorithm is a fast algorithm, requiring minimal CPU resources to execute and is compatible with different types of MPEG decoder systems. The digital content offered by a streaming video service needs to be safe guarded for it to be commercially feasible and a solution must consider the method of its implementation along with its integration into the structure [14]. One such solution lies in the domain of copyright protection, which should be implemented using methods like encryption and watermarking [15]. This scheme has been developed and implemented in the doctoral thesis submitted by Jason But of Monash University [9]. The idea of in-place encryption of the data streams within the System stream is developed resulting in an encoded bitstream of the same length and allows the encoding of multiplexed streams without changing any part of the System stream.

4.2 SEAL (Software optimized Encryption Algorithm) Encryption scheme

The encryption scheme used is the SEAL algorithm [9], which is a very fast software based stream cipher and is different from most stream ciphers as it is a member of the pseudo-random function family. The issue of encryption of the MPEG-1 system stream can be ignored since the contents of the audio and video streams are encoded as the payload data within the packets of the system stream. The System stream is parsed to get the audio and video streams and then sent to the respective encryption modules. Moreover, the length of the audio and video streams remains unchanged after passing through the modules and can function with blocks that can be restarted. The system stream parser parses the stream, passes the Packet Payload data to the appropriate cipher module and reinstates the data into the stream without changing the Packet Headers. The SEAL encryption scheme is mainly used for video streaming applications as in low bit-rate streaming to mobile terminals, Internet streaming to a personal computer and entertainment quality video.

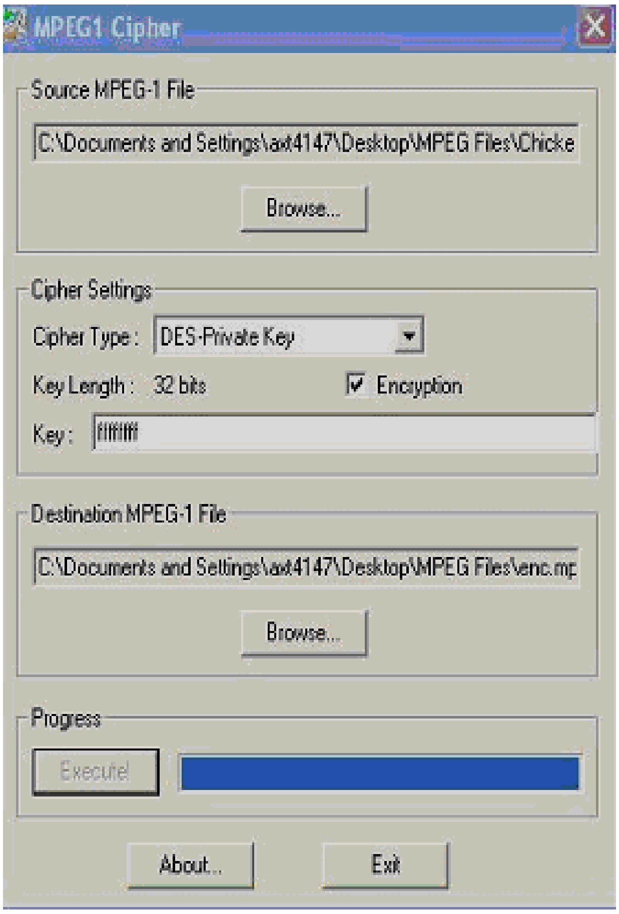
5 PARTIAL SELECTION SCHEME OF MPEG-1 STREAM FOR THE PURPOSE OF ENCRYPTION USING OPEN SSL LIBRARY

5.1 Introduction

The encryption (SEAL) scheme described in the previous section, is a stream cipher good for streaming purposes but not as safe as block ciphers. The cipher needs a license but is available for peer view. The strength of the cipher depends on the random bit generator with rekeying to be done for speed and security, which requires the restarting of the random number generator at each of the marker points which is cumbersome [9]. The SSL (Secure Socket Layer) Protocol provides privacy and reliability between two communicating applications. Open SSL is an Open Source toolkit implementing SSL/TLS (Transport Layer Security) and cryptography [1]. It is made up of SSL implementation, crypto library and bunch of applications, having a command-line interface and an application programming interface with lot of other tools using Open SSL's libraries to secure data or establish secure connections [16].

5.2 Encryption scheme

The audio and video streams are obtained from the MPEG1 encoded system stream and the video stream thus obtained is parsed twice, once to get the size of the stream buffer and the second time to collect the bytes for encryption. The status of the check box determines whether the bytes need to be collected or not for encryption. Accordingly, encryption or decryption is carried out and the resulting bytes are inserted back into the stream from where they had been initially collected. In case of encryption, the cipher text is ready for transmission and decryption whereas, for decryption the original stream is obtained. The results obtained on execution of the encryption scheme are shown in figures 1 and 2.



MPEG1 Cipher

Source MPEG-1 File

C:\Documents and Settings\axt4147\Desktop\MPEG Files\Chicke

Cipher Settings

Cipher Type : DES-Private Key

Key Length : 32 bits

☑ Encryption

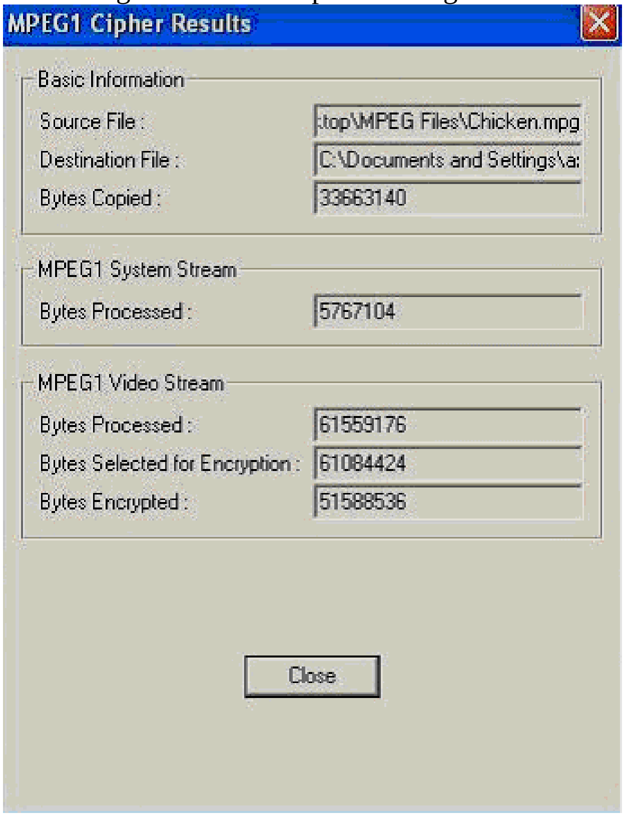
Key : ffffffff

Destination MPEG-1 File

C:\Documents and Settings\axt4147\Desktop\MPEG Files\enc.mp

Progress

Fig. 1 "MPEG1 Cipher" dialog box



MPEG1 Cipher Results

Basic Information

Source File : :top\MPEG Files\Chicken.mpg

Destination File : C:\Documents and Settings\a:

Bytes Copied : 33663140

MPEG1 System Stream

Bytes Processed : 5767104

MPEG1 Video Stream

Bytes Processed : 61559176

Bytes Selected for Encryption : 61084424

Bytes Encrypted : 51588536

Fig. 2 "MPEG1 Cipher Results" dialog box

6 CONCLUSIONS AND FUTURE WORK

6.1 Conclusions

The encryption done with private key and public key cryptography, using the open SSL libraries [16] is a more standardized method of performing encryption than the SEAL encryption scheme proposed by Jason But [9]. The SEAL is a proprietary scheme and is vulnerable to malicious attacks. Also, the SSL libraries are an open source and hence do not require licensing, as is the case for SEAL. The public key encryption done using RSA [17] is known to be a sturdy scheme and is widely used for commercial purposes. The private key encryption done using DES is also a well-accepted standard. The GUI (Graphic User Interface) [18] shown in Figure 1 is a representation of the menu of options provided to the user, obtained on the execution of the program. The code follows the options chosen by the user, for selection of the encryption scheme, whether encryption or decryption needs to be performed, the source file and destination file. The statistical representation of the bytes processed, selected for encryption and actually encrypted is shown in Figure 2. The video sequences are parsed using the state machine and the bytes are collected for encryption and the resulting cipher text obtained is suitable to be sent across the network. At the receiving end, the cipher text is converted back to plain text with decryption by running the same code again with decryption being selected. The corresponding keys that need to be used for the process are incorporated according to the encryption scheme used. The use of libraries has certain obvious advantages over the SEAL scheme as indicated above. Hence the usage of the Open SSL libraries is a more rational choice over the SEAL.

6.2 Future work

The encryption done using Open SSL libraries for the implementation of the private and public key cryptographic schemes can be extended to other MPEG standards like MPEG-2 [14] or MPEG-4 [14], especially MPEG-4 Part 10, also known as H.264 [19]. The high compression of the video stream, achieved using H.264, when combined with an encryption scheme, implemented using Open SSL libraries, can prove to be an efficient way to send data safely across the networks using lower bandwidth. Finally, the concept of encryption using Open SSL libraries can be further extended for encryption of audio streams also, for their secure transmission across the network.

References:

[1] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 2001.

[2] H.Cheng, and X. Li, Partial Encryption of compressed images and videos, *IEEE Trans. on Signal Processing*, Vol. 48, No.8, 2000, pp. 2439-2451.

[3] S.V. Wunnava, and E. Rassi, Data encryption performance and evaluation schemes, *Proc. IEEE SoutheastCon*, No.4, 2002, pp. 234-238.

[4] L.Chiariglione, MPEG and multimedia communications, *IEEE Trans. on Circuits Syst. Video Technol*., Vol. 7, No.1, 1997, pp. 5-18.

[5] L.Chiariglione, Impact of MPEG Standards on multimedia industry, *Proc. of the IEEE*, Vol. 86, No.6, 1998, pp. 1222-1227.

[6] http://www.mpeg.org/

[7] M. Ghanbari, *Standard Codecs: Image Compression to Advanced Video Coding*, Institution of Electrical Engineers, 2003.

[8] http://www.chiariglione.org/mpeg/standards/mpeg-1/mpeg-1.htm

[9] http://caia.swin.edu.au/cv/jbut

[10] M.Hellman, and W.Diffie, New Directions in cryptography, *IEEE Trans. on Information Theory*, Vol. 22, No.6, 1976, pp. 644-654.

[11] S.Changgui, and B.Bhargava, An efficient MPEG video encryption algorithm, *Proc. of Seventeenth IEEE Symposium on Reliable Distributed Systems*, 1998, pp. 381-386.

[12] http://www.mycrypto.net

[13] K.R.Rao and J.J.Hwang, *Techniques and Standards for Image, Video, and Audio coding*, Prentice Hall, 1996.

[14] J. But, Limitations of Existing MPEG-1 Ciphers for Streaming Video, *CAIA Technical Report 04029A*, Swinburne University, Australia, 2004.

[15] J. But, Requirements for a Generic MPEG-1 Cipher to Function in an Existing Streaming Server Environment, *CAIA Technical Report 040426A*, Swinburne University, Australia, 2004.

[16] http://www.openssl.org/

[17] http://www.linuxjournal.com/article/6695

[18] www.msdn.microsoft.com

[19] ftp://standards.polycom.com