World Applied Sciences Journal 33 (7): 1102-1108, 2015
ISSN 1818-4952
© IDOSI Publications, 2015
DOI: 10.5829/idosi.wasj.2015.33.07.200

Efficient Technique for Secure Transmission of Real-Time Video over Internet

Roopa Lakshmi S and K. John Singh

School of Information Technology and Engineering VIT University, Vellore, Tamil Nadu, India

Abstract: With the incessant increase of digital communications on internet, multimedia security is becoming more important. There are predominantly two featuresare there to pay attention while transferring real time videoover internet. Predominantly, time necessitate to transfer the data then the security providing to it without distressing the excellenceof the video. Vital issue tolook out in real time video transmission is the time span to transfer the data, because real time;the aforementioneddenotes to the spontaneous data transmission. Traditional encryption techniques used for video encryption is not appropriate for real time video. In this paper, we discussed various encryption mechanisms and evaluate their performance. This paper proposes a new technique called EnhancedReal Time Video Encryption using Lossless Compression (ERTVELC) for encrypting real time video with better quality of output video. According to the analysis and experimental results acquired, show that the proposed method has lossless compression with good security and fast transmission of data.

Key words: Videoencryption · Lossless Compression · ERTVELC

INTRODUCTION

Systems will make uninterrupted media stream, in the dawn of multimedia system. It is more vital to secure the continuous media from the potential threats like eavesdropper, hackers, etc. The streaming applications are endless and this streaming can be distributed as a subscription service, whole package of video of direct programming or by Pay-Per-View (PPV). A collaborative web siteor a tool or even a video preview can be formed using this. Applications of real time videos are in various fields like education, web based channels, broadcasting Video-On-Demand and content browsing. Their specific uses of each fields are corporate communications, distance learning, IP-TVs, radio in web, viewing lectures and asset management.These type of systems use various types of techniques for encryption to improve the security provisions for multimedia applications which used network [1, 2]. There should be a limited delay for sending the frames of the real time video streams over a network. Correspondingly, frames of the videos are to be delivered at an assured rate; hence, encryption packets which are receiving and sending need to be transferred in a particular extent of time to exploit the permissible delay. In case for VOD, whenever receiver needsvideo, video streams have to be played. Hence, there won't be any buffering or playback conceptions be used. Thus, many encounters for security of these data are to be maintained. Some of them are us under:

- The size of the video is generally huge even after compression, even though if we use best available techniques for compression. For example, 2 hour MPEG-1 video's size is of about 1GB.
- VOD type of application need to be run in real time multimedia applications.
- Concert of multimedia processing streams must bestandard (i.e. limited by definiterate of delay).
- In comparison of compression technique with encryption technique, system overhead should be less along with fast processing.

Some points are been taken for finding the efficient encryption technique of real time video, they are; applying AES for MPEG-4 in real timesheltered video transferring system, relating therecital of the AES with two main encryptiontechniques andestimating the variance between the system overhead with various multimedia data types such as audio, text and video with other encryption techniques as XOR, RC4, AES.

Corresponding Author: K. John Singh, School of Information Technology and Engineering, VITUniversity, Vellore, Tamil Nadu, India.

Related Work: There are two ways for encryption and decryption of a video or a real time video. The basic technique is to use the secret key, here secret key is used for the encryption of the video and fro decryption we need that secret key. This provide good security compared to other technique as we are using a key which is known to only the sender and the receiver. But at the same time system overhead is high in this case. Another way is using the public key encryption [3, 4]. This is not secure as the previous technique. As the key is known to all but this will reduce the system overhead.For real time video transferring we cannot use this technique, as it provide low security. Even this technique need time to encrypt and decrypt the video hence it is not suitable for real time video like video conferencing. There are basically seven building blocks of any video streams which are shown in Figure 1. From this figure, we can specify that with the help of audio compression and video compression algorithms, pre-compressionof raw audio and video data are done and those data are stored in storage devices. After user request,a streaming server recovers compressed audio/video data from media where it has been stored. Then the AL (Application Layer) segmentadjusts the audio/video bit-streams as per the network eminence and desires. After acceptance of data from AL it is been transferred to the next layer according to some transport protocols and these bit streams are sent to the Internet IP networks as a packets. Those packets may be delayed or destroyed during transmission in Internet because of congestion; due to bit erors in wireless medium these packets may be spoiled. Continuous distribution media services are used to increase the quality of audio/video transmission over network. In this, packets are first transferred to the transport layer and then application layer after processing it but before decoding it using audio/video decoder. Synchronization mechanisms are used to attain synchronization between audio and video [5].

There are numerous encryption algorithms for video. Some of such encryption techniques can be categorized as follows: naive algorithm, Zig-Zag algorithm, AES, RC4 and selective algorithm [6]. The impression of naive encryption is to pact with the video streams as text data [3]. The easiest technique to encrypt any video streams is to encode every byte. Naive algorithm, encrypt each byte in the entire video stream. It guarantees the supreme security level. Conversely, it is not relevant elucidation if the data size is bulky or outsized. Because of this encryption procedures, the delay in time increases and even the system overhead will not be adequate for the encryption of real time video.

In selective algorithm, there are four levels of selective algorithms [4] are advocated. Those levels all headers; encrypting every headers and I (Initial) frames; encrypting each I frames and all I segments in B and P frames and lastly according to Naive algorithm we need to encrypt all the frames to assure the premier security. The awareness about ZIG-ZAG algorithm is ultimately encrypting the streams of video then compressing them. Unequivocally, while representing (mapping) the 8x8 block to Ix64 vector every time in identical order. We can use a random permutation to map this transformation of the 8x8 block to the Ix64 vector. Consequently, the conception of the key (encryption key) does not occur in the ZIG-ZAG transformation algorithms. As soon as the transformation list is recognized, there won't be any security in that algorithm. A different Video Encryption Algorithm (VEA) that depends on separating the video streams into different frames. These frames are parted into two altered lists (even and odd lists). Subsequently, relating any encryption algorithm such as DES to that even lists and the last cipher is appending of output of XOR encryption algorithm with that odd list [5] [6].

In RC4 plain textwill be encrypted one byte per time and this is the structure of stream cipher. The maximum key length will be from 1 to 256 bytes (i.e. 8 to 2048 bits). We need same key to encrypt and decrypt it, hence it is called symmetric encryption. We are using the Random transformation in this algorithm. In stream cipher this type of algorithm is mostly used. Even in Secure Socket Layer/Transport layer Security (SSLITLS) is used. This standard is designed for communication between servers and web browsers. There are mainly two operations, Key setup operation and ciphering operation. In Key setup operation, pseudorandom bit streams are generated by RC4 (KeyStream) then some type of operations are applied to that key such as expansion and permutation; thus to maintain as more randomized [3]. Whereas in the next operation the data is XOR edwith that key. The rudimentary sequence and operations of RC4 is presented in Figure 2. Additional informationregarding this algorithm can be viewed in [6].

Basically the AES algorithm (Rijndael [7]) is symmetric key cryptosystem that practices 128-bit data blocks. It uses cipher keys with sizes of 128, 192, or 256 bits. Rijndael is more accessible and can hold various key sizes and data block sizes,still they are not encompassed in the standard.

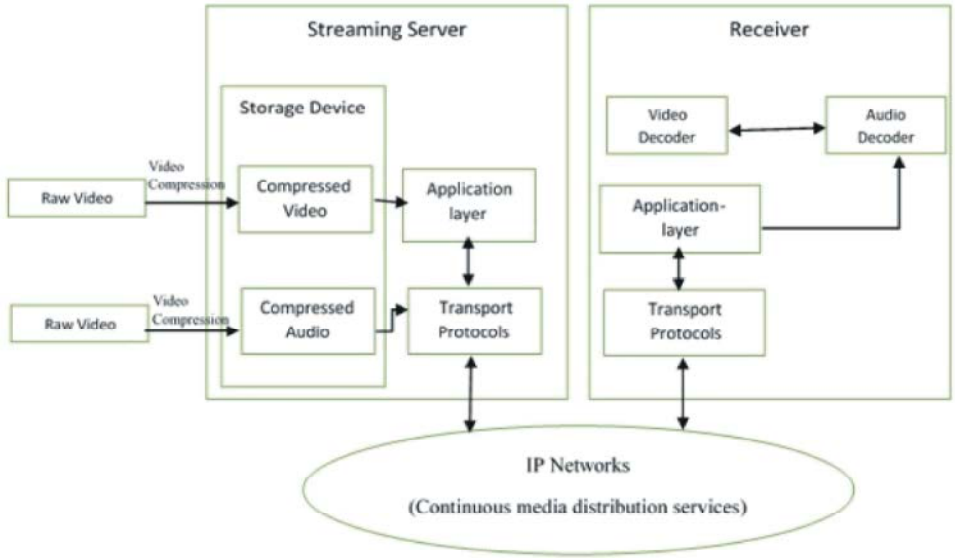

Fig. 1: 1-way data flow diagram of captured multimedia devices

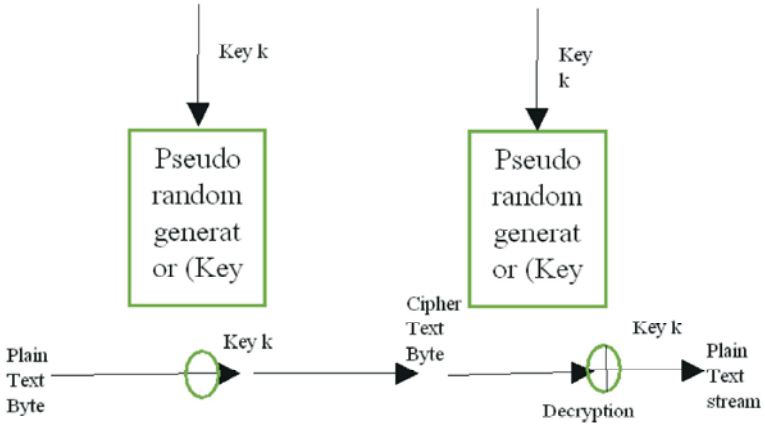

Fig. 2: Basic structure of RC4

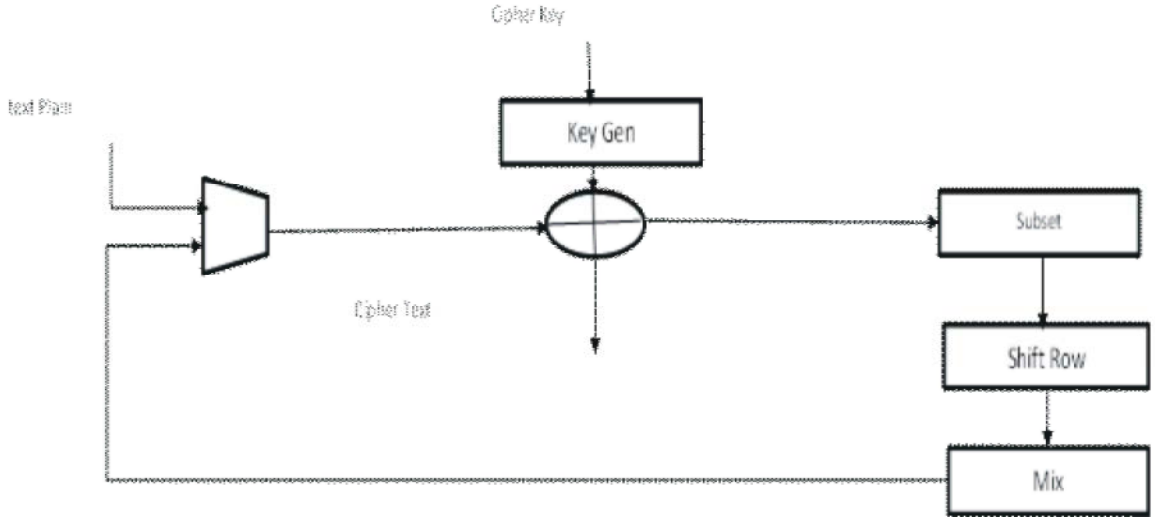

Fig. 3: Basic Architecture of AES

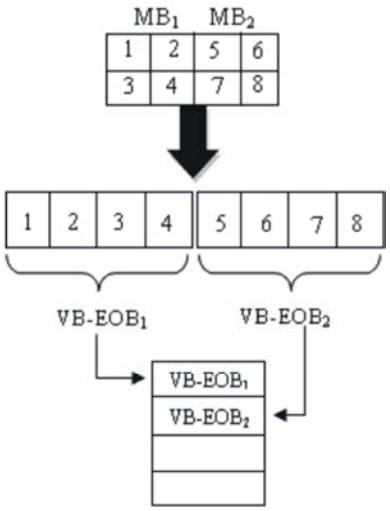

Fig. 4: Intra block shuffling

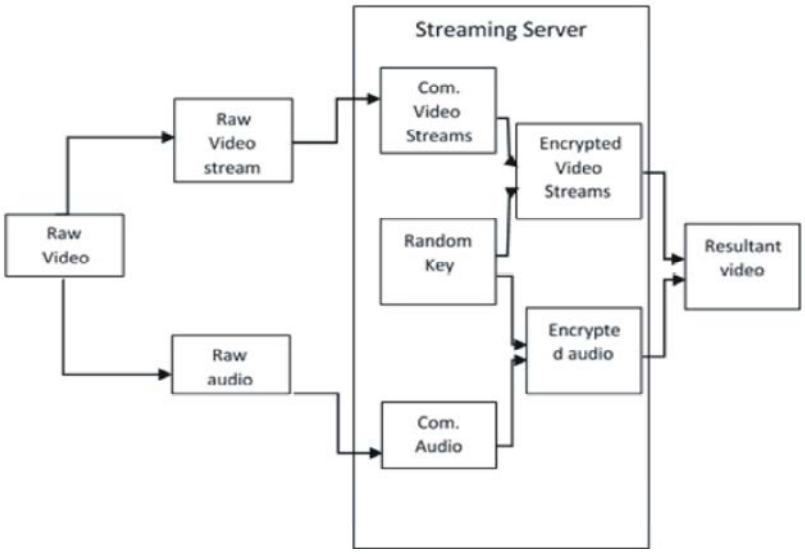

Fig. 5: ERTVELC Technique (Sender part: Encryption technique)

Similarly the fundamentalblocks of AES operation is exposed in Figure 3. For more information regarding this algorithm go to [8].

Certainprojectedefforts to secure video streams have been described. The most forthright procedure is to encrypt the whole video stream using ordinary encryption types. Evennaive algorithm is used [8]. Due to huge file size, processing speed get affects in this approach. Alternativemethod to secure video streams is the selective encryption algorithm. It encrypts only the I-frame of video streams [9] [10]. Meyer and Gadegasthave considered aninnovativevideo bit-stream SECMPEG that integrates selective encryption and supplementary header information and with highspeed software performance [11]. SECMPEG can use both RSA & DES and gives four stages of security: First and foremost level; all headers are encrypted.Second level; every header with DC and lower AC terms of I-blocks. Third level; From P and B frames all I-blocks and I-frames are encrypted. Fourth level; all data will be encrypted. This is not companionable with regular MPEG.A distinctive encoder/decoder would be mandatory to access the unencrypted SECMPEG streams. A suggestionpointing at combination of compression and encryption of MPEG streams into one step is presented in [12] using the "ZigZag-Permutation Algorithm". In this random permutation list are been replaced with the map which is of 8x8 block.

Some performance real time algorithm of decryption and encryption like AES done by Salah [13].With the video encoders and decoders like H261, JPEG, MPEG-112 and CellB algorithms like AES and XOR been adopted by them. He endeavored to chooseexplicit frames to encrypt.P and B frames are combined to form those encrypted streams of video. About four MPEG fast video encryption algorithm are presented in [14]. By changing randomly the bits of motion vectors and/or changing the sign bits of Discrete Cosine Transform (DCT) using those keys as secret keys in these algorithms which are based on DES [3]. The encryption is proficient by the counter DCT (IDCT) during the process of MPEG video compression.System overhead is there due to this algorithm to MPEG codec. The AES performance in encrypting MPEG-4 streaming video has been noticed by the previous authors. Furthermore, peer to peer stages are not used by most the studies due to this. Thus this gained more concernin modern era of video stream transferring to widespread application spectrum.

Ertvelc: Enhanced Real time Video encryption using Lossless compression technique proves less system overhead with the good security. The parameters used for this Algorithm setup time, Encryption time of video, Encryption time of audio, key generating time and decrypting time. In this technique we first separate the raw video into video streams and audio. These two streams are then passed to the network through server which is streaming server. In that server, random key will be generating with the help of Random Key Generator. To improve the efficiency of the transmission, compression technique is used.

Real time video must be in good quality, thus to improve the quality of the video we choose lossless compression technique. As the quality of the video is important with the efficiency of the transmission of the video. After compressing those streams, with the help of key encryption process takes place. Here AES and XOR technique is used to encrypt that compresses video streams and accordingly audio streams also encrypted with the key. Thus after encrypting it, combining audio and video into single packet and transmitting that packet to the network. At the same time, in receiving side video are been separated into audio and video and then performing the decryption process then combining it and then show it to the user.

Parameters are used in this paper to represent the quality encryption technique. Thus the comparison between other encryption techniques with ERTVELC technique. Time needed to setup the algorithm to process any data is evaluated in Algorithm Setup Time. Latency time to algorithm with path delay are measured in Video encrypting time parameter. The most important parameter in this is the Random key generating, which will consider the key generation time by the streaming server with the help of Key Generator. This parameter is totally depends on the key generator we used. We can accept that the delay timesignifies the summation of the preceding time delays.

$$T=Ts+ Te+ Td+Ts$$

RESULTS

With the above mentioned parameters, proved that the ERTVELC is better than the other existing encryption

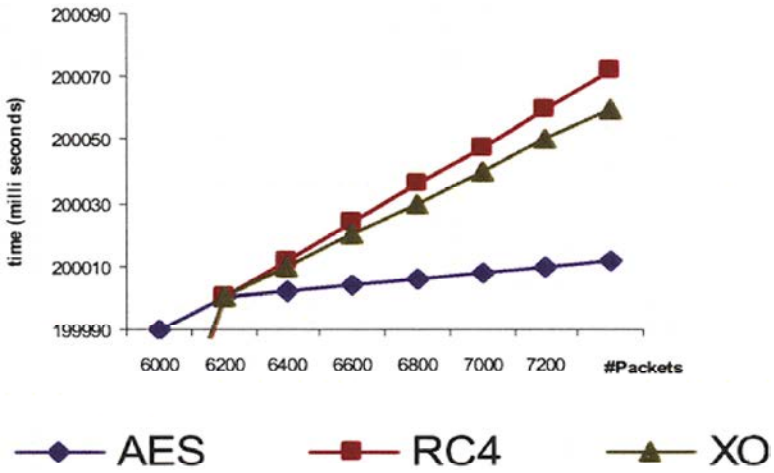

Fig. 6: Time delay *Te*for TEXT using XOR, RC4 and AES EncryptionAlgorithms

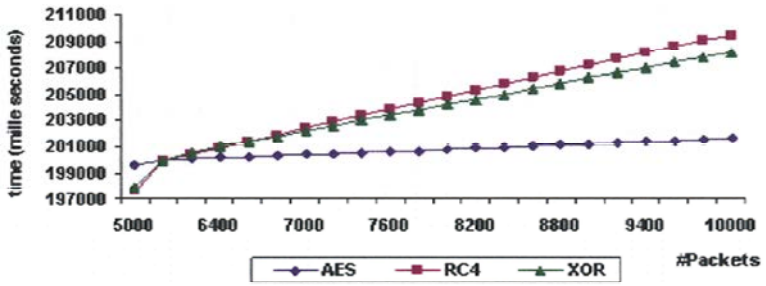

Fig. 7: Time delay *Te*for AUDIO using XOR, RC4 and AES Encryption Algorithms

technique. This technique is good for the real time video encryption, because we won't be storing streams in database. Hence it is efficient in real time video. And the encrypting time of video and audio is depends on the encryption technique used. In ERTVELC both the audio and video are encrypted, hence provide good security with less overhead. Lossless compression is used in this techniques to provide good quality video after the decryption of video.

Fig. 7 shows the result of the audio encryption with the other traditional technique. Fig. 6 explains the difference between the traditional techniques with the proposed technique.

CONCLUSION

Real time video should be sent to the receiver with the good quality. The transmission of these real time video must have security. Applications like Video on Demand, Video conferencing etc. are using real time video transferring. Hence these data may also carry important sensitive data. Thus security plays a vital role and also delays cannot be accepted in these application. Thus we cannot store those video in any storage device and also quality important characteristic. Hence proposed technique use lossless technique for compression.

REFERENCES

1. IEEE Transactions on Circuits and Systems for Video Technology: Special Issue on Authentication, Copyright Protection and Information Hiding, 13(8), August 2003.
2. Liu and A.M. Eskicioglu, 2003. "Selective Encryption of Multimedia Content in Distribution Networks: Challenges and New Directions", lASTED International Conference on Communications, Internet and Information Technology (CIIT 2003), Scottsdale, AZ, November 17-19, 2003.
3. Stinson, D.R., 2002. "Cryptography Theory and Practice," CRC Press, Inc.
4. William Stallings, 2005. "Cryptography and Network Security, Principles and Practice", Pearson education, Third Edition.
5. Chun-Shien, L., 2005. "Multimedia Security Steganography and Digital Watermarking Techniques for Protection of Intellectual Property", Idea Group Publishing.
6. Seidel, T., D. Socek and M. Sramka, 2003. "Cryptanalysis of Video Encryption Algorithms", Proceedings of The 3rd Central European Conference on Cryptology TATRACRYPT 2003.
7. Gladman, "A Specification for Rijndael, the AESAlgorithm,".
8. Agi, I. and L. Gong, 1996. Empirical Study of Mpeg Video Transmissions," In Proceedings of the Internet Society Symposium on Network and Distributed System Security, pp:137-144, San Diego, CA, February 1996.
9. Li, Y., Z. Chen, S. Tan and R. Campbell, 1996. "Security enhanced mpeg player", In Proceedings of IEEE First International Workshop on Multimedia Software Development (MMSD'96), Berlin, Germany, March 1996.
10. Maples, T.B. and G.A. Spanos, 1995. "Performance Study of a Selective Encryption Scheme for the Security of Networked Real-time Video", In Proceedings of lath International Conference on Computer Communications and Networks, Las Vegas, Nevada, September 1995.
11. Meyer, J. and F. Gadegast, "Security Mechanisms for Multimedia Data with the Example mpeg-I Video", Available on.
12. Tang, L., 1996. "Methods for Encrypting and Decrypting MPEG Video Data Efficiently", In Proceedings of The Fourth ACM International Multimedia Conference (ACM Multimedia'96), pages 219-230, Boston, MA, November 1996.

13. Salah Aly, 2004. "A Light-Weight Encrypting For Real Time Video Transmission", TR04-002, College of computing and digital media, Depaul University, August 2004.
14. Shi, W. Changgui and S. Wang, 2004. "MPEG Video Encryption Algorithms", Multimedia Tools and Applications, 24: 57-79, September 2004.