Journal of Computer Science 8 (5): 731-736, 2012
ISSN 1549-3636

A Survey on Joint Compression and Encryption Techniques for Video Data

[1]K. John Singh and [2]R. Manimegalai
[1]School of Information Technology and Engineering,
VIT University, Vellore, Tamil Nadu, India
[2]Research Supervisor, Anna University of Technology Coimbatore,
Tamil Nadu, India

Abstract: Problem statement: When we send any video data over the network it consumes more time. This is due to the huge size of the video file when compared to text file. Therefore, video data should be compressed before sending to the destination. Another important factor during data transfer is security. Joint compression and encryption is employed to enable faster and secured transmission of video data. **Approach:** Compression and encryption algorithms can be classified into two main categories: Independent encryption technique and joint compression and encryption technique. Independent encryption techniques can further be classified as heavy weight and light weight encryption algorithms. There are many algorithms available in the joint compression and encryption technique. Comparative study of the above mentioned algorithms is done in this study. **Results:** Based on our study, found joint compression and encryption algorithms reduced 40% of the memory storage size and they increased execution speed up to 21%. **Conclusion:** Joint compression and encryption algorithms perform better in terms of speed and security when compared to independent encryption algorithms. This is because they employ compression before encryption.

Key words: Video Encryption Algorithm (VEA), Real Tome Video Encryption Algorithm (RVEA), Elliptic Curve Cryptography (ECC), Discrete Cosine Transform (DCT)

INTRODUCTION

The revolution of multimedia and hyper media has been a driving force behind fast and secured data transmission techniques. Nowadays, people are offering web based learning through an internet (Afolabi and Adagunodo, 2011). Mostly, these courses are offering through video conferencing mode only. In general, video data takes more time for encryption, because of its large size. Since the size of video data is huge in volume, it needs to be compressed and encrypted to avoid security threats and delay. There are two strategies for this, namely, independent encryption algorithms and joint compression and encryption algorithms. In independent encryption algorithms, both compression and encryption are done independently as two different steps by employing suitable algorithms. Steps involved in independent encryption are illustrated in Fig. 1. This strategy consumes more time and memory. When independent encryption algorithms are employed, overall system performance decreases due to the huge computation overhead involved.

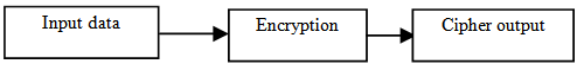

Fig. 1: Independent encryption process

But in joint compression and encryption algorithm, both the steps, namely, compression and encryption are integrated together as a single step. There are two approaches for joint compression and encryption algorithm: the first method employs encryption after compression and the second method does encryption before compression. Steps involved in both the approaches are illustrated in Fig. 2a and 2b. In the first strategy, as encryption is done after compression we get two-fold advantage, namely, reduced data size and time. The second strategy encrypts data without compression and is time consuming. In general, any joint compression and encryption algorithm will provide two levels of security and consumes less time when compared to independent compression and encryption algorithms.

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

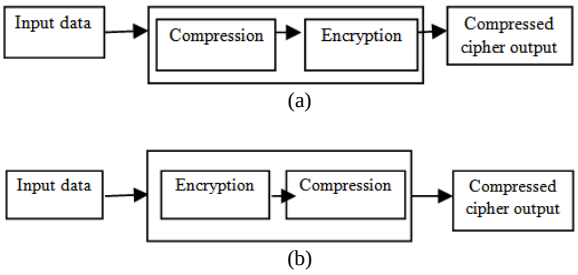

Fig. 2: Joint compression and encryption process (a) Compression before encryption (b) Compression after encryption

Elliptic Curve Cryptography (ECC) (Hitchcock, 2003), Pretty Good Privacy (PGP) (Li *et al*., 2002), Tiny Encryption Algorithm (TEA) (Wheeler and Needham, 1995), Advanced Encryption Standard (AES) are few examples for independent encryption algorithms. Secure Motion Picture Experts Group (SECMPEG) (Meyer and Gadegast, 1995), Video Encryption Algorithm (VEA) (Shi and Bhargava, 1998), Real-time Video Encryption Algorithm (RVEA) (Shi *et al*., 1999), are few examples for joint compression and encryption algorithms. Joint compression and encryption algorithms are faster in encrypting the video data due to selective encryption technique when compared to other video encryption algorithms.

The data is prone to be hacked when the digital video data is transmitted wired and wireless IP networks, it may be attacked by some attacker. Due to this the confidentiality in the data will be lost. The confidentiality is important for any transmitted video data. Video conferencing, video security monitoring and video databases are the few examples which need confidentiality. To maintain the confidentiality and speed better use joint compression and encryption algorithms.

MATERIALS AND METHODS

As already mentioned, video encryption algorithms are categorized into, namely, independent encryption algorithms and joint compression and encryption algorithms. Various algorithms in the above categories are discussed in this section.

Independent encryption algorithms: In independent encryption technique, both compression and encryption are carried out separately. Any standard algorithms can be used for compression; Heavyweight or lightweight algorithms are used for encryption. Heavyweight algorithms are more secured than lightweight algorithms. But the computing overhead is high in heavyweight encryption algorithms.

Adida *et al*. (2005) have presented a lightweight encryption technique for video sent through email. Adida *et al*. (2005), the user has to undergo the authentication process to access his/her email data. This method works well for email authentication. However this method did not address key generation and key management related issues. An encryption scheme based on wavelet packet transform method is proposed in Engel and Uhl (2006). The methodology proposed in Engel and Uhl (2006), encrypts only a portion of the data and thereby taking less time for generating the cipher text. As, the whole data is not encrypted, this solution is vulnerable to security threats. It has increased computational complexity when compared to other algorithms because the input video data should be converted into a wavelet form before encryption.

The polynomial interpolation based Elliptic Curve Cryptosystem (ECC) is proposed by Jie and Kamarulhaili (2011). ECC uses 160 bit key which is shorter than the key used in other heavyweight algorithms like RSA. As the key size is smaller, data is encrypted quickly. This is the advantage of the solution proposed in ECC. But, the key can be hacked easily because the size is small. Video streaming over wireless networks are vulnerable to privacy and malicious attacks.

TwoFish (Schneier *et al*., 1998) was not patented and is free to use. The key size in TwoFish algorithm is 256 bits and sixteen rounds of XOR operation is performed for encryption which leads to more computational steps. Wang and Xu (2007) have studied lightweight and scalable encryption algorithm for streaming video over wireless networks. Pretty Good Privacy (PGP) algorithm is mainly used for secured communication through an electronic environment (Li *et al*., 2002). This environment transfers text data easily. But it is very complex to transfer a video data over this environment because PGP takes more time for video data encryption.

The algorithm proposed in Wheeler and Needham (1995), known as Tiny Encryption Algorithm (TEA), is vulnerable to brute-force attack due to limited steps involved. Rivest Cipher 4 (RC4) was good for Secured Socket Layer (SSL) security (Yekkala *et al*., 2007). Rivest Cipher 6 (RC6) could be parameterized to support a wide variety of key sizes, word-lengths and number of rounds (Wheeler and Needham, 1995; Wang and Xu, 2007). RC6 has higher time consumption.

Joint compression and encryption algorithms: In joint compression and encryption algorithm, the

encryption is applied with certain steps of compression algorithm. If we combine both compression and encryption together, the system can do the encryption process quickly. And we will get the multilevel of security. So the data will be transmitted with high speed and security.

Zeng and Lei have proposed a frequency domain scrambling approach in Zeng and Lei (2003) which performs encryption after the Discrete Cosine Transform (DCT). Compression is done only on scrambled frames leading to low image quality. In addition, the proposed solution in Meyer and Gadegast (1995) tends to consume more memory due to uncompressed frames.

The proposed solution in Tang (1996) performs compression and encryption with minimum overhead using random permutation and probabilistic encryption. It provides different levels of secrecy for various multimedia applications. The proposed strategy in Tang (1996) employs Discrete Cosine Transformation (DCT) to map smaller blocks with size 8×8 to bigger blocks with size 1×64. The output from DCT is uniformly quantized and all quantized coefficients are arranged in zig-zag order. Finally entropy coding is done for compression.

The joint compression and encryption algorithm proposed in Meyer and Gadegast (1995), SECMPEG, does selective encryption using conventional encryption algorithms. The Video Encryption Algorithm (VEA) proposed in Shi and Bhargava (1998) encrypts all sign bits of DCT coefficients by using XOR–operation. VEA has the disadvantages of having known-plaintext attack and complex key management scheme. In known-plaintext-attack, if both the original and encrypted videos are available, the attacker can easily determine the secret key. To overcome known-plaintext attack, Shi *et al*. (1999) have proposed Real-time Video Encryption Algorithm (RVEA). The XOR operation in VEA (Shi and Bhargava, 1998) is replaced with a conventional encryption algorithm in RVEA (Shi *et al*., 1999). RVEA is a selective encryption algorithm which operates on the sign bits of both DCT coefficients and motion vectors of a MPEG compressed video. RVEA can use any secret key cryptography algorithms to encrypt selected sign bits. The proposed solution in Wu and Kuo (2005), Multiple Huffman Table (MHT) converts entropy coders into encryption ciphers. The computational cost of this algorithm is less but this is more vulnerable to chosen-plaintext attack.

Two approaches for integrating encryption with multimedia compression systems are studied in Wu and Kuo (2005), i.e., selective encryption and modified entropy coders with multiple statistical models. First, they examine the limitations of selective encryption using cryptanalysis and provide examples that use selective encryption successfully. Two rules to determine whether selective encryption is suitable for a compression system are concluded. Next, they propose another approach that turns entropy coders into encryption ciphers using multiple statistical models. Two specific encryption schemes are obtained by applying this approach to the Huffman coder and the QM coder. It is shown that security is achieved without sacrificing the compression performance and the computational speed. This modified entropy coding methodology can be applied to most modern compressed audio/video such as MPEG audio, MPEG video and JPEG/JPEG2000 images.

The partial encryption was implemented in FPGA (Reaz *et al*., 2011), in which a secure encryption algorithm is used to encrypt only part of the compressed data. Partial encryption is integrated in FPGA and applied to several image and video compression algorithms. The partial encryption schemes are fast, secure and do not reduce the compression performance of the underlying compression algorithm.

The chaotic Wong and Yuen (2008) map algorithm is used to perform compression and encryption simultaneously. This is can be applied for lossless data and lossy image compression.

RESULTS AND DISCUSSION

Performance of compression: When compared with independent encryption algorithms, joint compression and encryption algorithms give better compression ratio. In joint compression and encryption technique, selective encryption is employed in order to provide quick results. The results are shown that joint compression and encryption algorithms can increase the compression ratio up to 25%.

Performance of encryption: In general, joint compression and encryption algorithms are more efficient than independent encryption algorithms. Since the encryption is done after compression, these algorithms provide high encryption speed. The study has shown that joint compression and encryption algorithms can increase the encryption speed up to 21% than independent encryption algorithms. This is because the data size will be reduced during compression before encryption process.

Security: In joint compression and encryption technique, the compression process involves one or

more encryption steps. Additionally, a separate encryption process is applied after compression. Thus, joint compression and encryption technique gives two levels of security when compared to independent encryption technique.

Execution speed: In joint compression and encryption technique, compression and encryption are done as one process; whereas in independent encryption technique, they are done as two different processes. Thus, joint compression and encryption technique takes less execution time when compared to independent encryption technique.

Memory utilization: As discussed earlier, joint compression and encryption technique use the compressed video during encryption and hence require less memory space.

To analyze the performance of the joint compression and encryption algorithms and independent encryption algorithms, metrics such as execution time, CPU utilization and memory utilization are considered. Joint compression and encryption algorithm are more secured, faster and consume less memory when compared to independent encryption algorithms. Performance comparison based on execution time, CPU utilization and memory utilization are shown in Fig. 3-5 respectively.

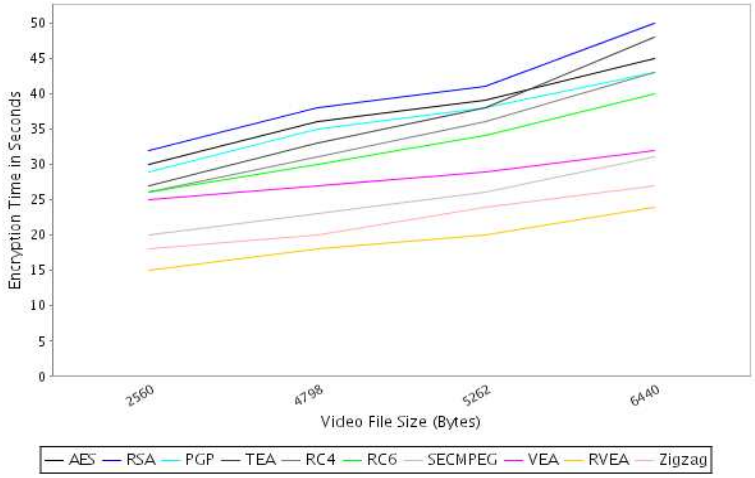

Fig. 3: Comparison of encryption algorithms based on execution time

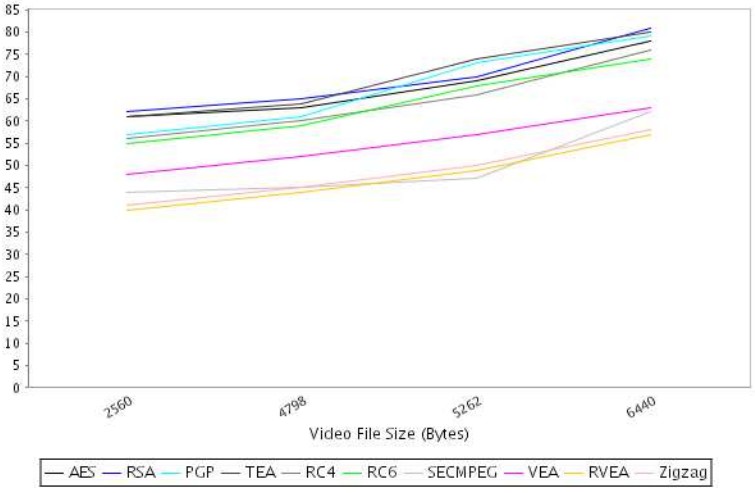

Fig. 4: Comparison of encryption algorithms based on CPU utilization ratio

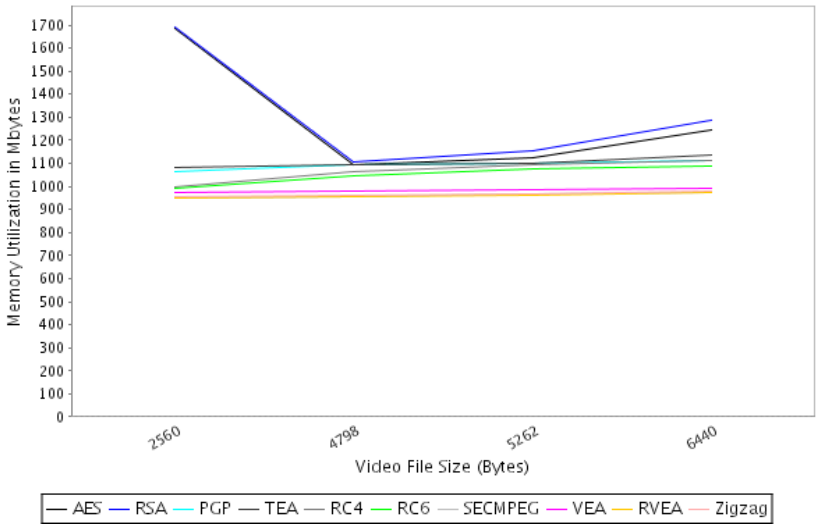

Fig. 5: Comparison of encryption algorithms based on memory utilization

CONCLUSION

The joint compression and encryption algorithms resolve two major issues such as speed and security when confidential video data is sent over the network. In this study, comparative study of two categories of encryption algorithms viz. independent encryption algorithms and joint compression and encryption algorithms. The study shows that the joint compression and encryption algorithms are more secured and faster than all existing independent encryption algorithms.

REFERENCES

Adida, B., S. Hohenberger and R.L. Rivest, 2005. Lightweight encryption for email. Proceedings of the Steps to Reducing Unwanted Traffic on the Internet on Steps to Reducing Unwanted Traffic on the Internet Workshop, (SRUTI' 05), ACM, USENIX Association Berkeley, CA, USA., pp: 93-99.

Afolabi, A.O. and R. Adagunodo, 2011. Implementation of an improved data encryption algorithm in a web based learning system. Phys. Int., 2: 31-35. DOI: 10.3844/pisp.2011.31.35

Engel, D. and A. Uhl, 2006. Secret wavelet packet decompositions for JPEG 2000 lightweight encryption. Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, May 14-19, IEEE Xplore Press, Toulouse, pp: 465-468. DOI: 10.1109/ICASSP.2006.1661313

Hitchcock, Y.R., 2003. Elliptic curve cryptography for lightweight applications. PhD Thesis, Queensland University of Technology.

Jie, L.K. and H. Kamarulhaili, 2011. Polynomial interpolation in the elliptic curve cryptosystem. J. Math. Stat., 7: 326-331. DOI: 10.3844/jmssp.2011.326.331

Li, Y., Z. Chen, S.M. Tan and R.H. Campbell, 2002. Security enhanced MPEG player. Proceedings of International Workshop on Multimedia Software Development, Mar. 25-26, IEEE Xplore Press, Berlin, Germany, pp: 169-175. DOI: 10.1109/MMSD.1996.557770

Meyer, J. and F. Gadegast, 1995. Securitymechanisms for multimedia-data with the example MPEG-I-Video. Project Description of SECMPEG, Technical University of Berlin.

Reaz, M.B.I., M.S. Amin, F.H. Hashim and K. Asaduzzaman, 2011. Single core hardware module to implement partial encryption of compressed image. Am. J. Applied Sci., 8: 566-573. DOI: 10.3844/ajassp.2011.566.573

Schneier, B., J. Kelsey, D. Whiting, D. Wagner and C. Hall *et al*., 1998. Twofish: A 128-Bit Block Cipher. The Pennsylvania State University.

Shi, C. and B. Bhargava, 1998. A fast MPEG video encryption algorithm. Proceedings of 6th ACM International Conference on Multimedia, Sept. 13-16, ACM, Bristol, United Kngdm, pp: 81-88. DOI: 10.1145/290747.290758

Shi, C., Wang, S.Y. and Bhargava, B., 1999. MPEG video encryption in real-time using secret key cryptography. Proceedings of International Conference on Parallel and Distributed Processing Techniques and Applications, (PDPTA' 99), The Pennsylvania State University, pp: 2822-2828.

Tang, L., 1996. Methods for encrypting and decrypting MPEG video data efficiently. Proceedings of the 4th ACM International Conference on Multimedia, Nov. 18-22, ACM, Boston, MA, USA., pp: 219-229. DOI: 10.1145/244130.244209

Wang, H. and C.W. Xu, 2007. A new lightweight and scalable encryption algorithm for streaming video over wireless networks. Kennesaw State University.

Wheeler, D.J. and R.M. Needham, 1995. TEA, a tiny encryption algorithm. Fast Software Encryption Lecture Notes Comput. Sci., 1008: 363-366. DOI: 10.1007/3-540-60590-8_29

Wong, K.W. and C.H. Yuen, 2008. Performing compression and encryption simultaneously using chaotic map. City University of Hong Kong, China.

Wu, C.P. and C.C.J. Kuo, 2005. Design of integrated multimedia compression and encryption systems. IEEE Trans. Multimedia, 7: 829-839. DOI: 10.1109/TMM.2005.854469

Yekkala, A.K., N. Udupa, N. Bussa and C.E.V. Madhavan, 2007. Lightweight encryption for images. Proceedings of IEEE International Conference on Consumer Electronics, Jan. 10-14, IEEE Xplore Press, Las Vegas, NV., pp: 1-2. DOI: 10.1109/ICCE.2007.341551

Zeng, W. and S. Lei, 2003. Efficient frequency domain selective scrambling of digital video. IEEE Trans. Multimedia, 5: 118-129. DOI: 10.1109/TMM.2003.808817