A Novel Stream Cipher for Multimedia Security

P. Vidhya Saraswathi, M. Venkatesulu

Abstract: ***In the last decades the tremendous usage of multimedia data like audio, video and images through communication channels create a need on the security over networks. Since multimedia content utilize large amount of storage for storing images, audio and video, classical cryptographic algorithms such as DES, AES are not efficient in encrypting multimedia data. In future these data are represented as media stream, like real time audio and video. Therefore it is urgent need to protect the multimedia data from attackers in between communication channels. In this paper we propose a new algorithm that encrypt and decrypt compressed multimedia stream of image or audio or video. The compression results in less time in encrypting data because more compression results in less data volume. Our work ensures that multimedia data streams can be secured according to the requirements of the current scenario.***

Keywords : Encryption, Decryption, Stream cipher, Image, Audio,Video.

I. INTRODUCTION

Due to rapid growth in wired and wireless technologies, digital audio visual contents are easily made available on the network as a result it has raised many issues in multimedia security. Multimedia Security ensures confidentiality of the data during transmission over Wired and Wireless networks. Internet telephony, Internet conferencing, Internet security monitoring, Video conferencing, pay per view, Video on Demand are some of the applications that are to be protected .The design of efficient encryption algorithms for multimedia data has become more essential for public and private networks..

In early days traditional cryptographic algorithms are formulated to process the text based data as a bit stream and this stream does not have any complex internal data structure. But multimedia data such as, image, audio and video differ in their representation of generic data. Lossy and Lossless compression techniques are used to minimize the memory requirements and rapid transmission of the multimedia content.

Cryptography principles are used for transforming original data into another form[1]. Many algorithms are designed to provide confidentiality and secrecy of multimedia data. But these algorithms are not appropriate for protecting real time applications. When we wish to transmit large still images, audio or video through networks to process the encryption algorithms it require a large amount of hardware and software. This is because of the characteristics of multimedia data which make encryption process more difficult.

Encrypting color images and videos are nowadays following partial or selective encryption. Partial encryption enables the multimedia encryption at different stages of compression according to different users and their needs. Many specialized encryption methods have been developed to encrypt images and videos [3]. The most common algorithms to encrypt data are Data Encryption Standard (DES), RC4 and AES. But the implementation of these algorithms is highly time consuming to process the multimedia data

. Multimedia data generate large amounts of data so a number of techniques for encrypting multimedia data have been developed. The two common approaches of multimedia encryption are selective encryption [3]] and entropy coding encryption

The paper is organized in such a way that Section 2 presents related work in Multimedia encryption, Section

3 discuss about the proposed methodology along with stream cipher for multimedia encryption and decryption, Section 3 deals with experimental results, Section 4 presents the performance and security analysis and ends with conclusion section.

II. RELATED WORK

A. Multimedia Encryption and Decryption

The possible ways in which encrypting multimedia data, are represented in Fig. 1.

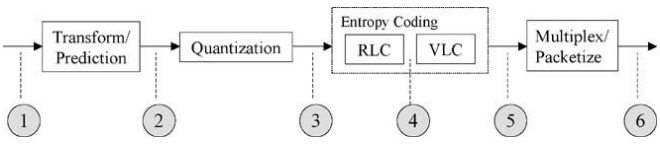

Fig. 1.Different Stages of Multimedia Encryption

Multimedia encryption can be applied in two stages either before compression or after compression as shown in Fig .1[4]. The encryption algorithm done before compression changes the characteristics of the multimedia data (Stage 1 to Stage 4). The second method [5] is to apply encryption after compression (Stages 5 and 6 in Fig. 1). This approach will create little overhead, but may tear down the structures of the multimedia data.

Revised Manuscript Received on December 16, 2019.
***** Correspondence Author
P.Vidhya Saraswathi*, Department of Computer Science & Information Technology, Kalasalingam Academy of Research and Education, Krishnankoil, India. Email: vidhyasaraswathi.p@gmail.com
M. Venkatesulu, Department of Information Technology, Kalasalingam Academy of Research and Education, Krishnankoil, India. Email: venkatesulum2000@gmail.com

Recently there has been raised a new idea to perform encryption in the intermediate stages illustrated in Fig. 1.The motion vectors [6] can be encrypted by DES algorithm. DC and AC coefficients in each block of an image or video frames can be scrambled within the block after Quantization, [8], encryption on entropy coding at stage 4 can be done within the compressed data [7]; the motion vectors and Huffman code words can be encrypted in a cryptographically [10]. At Stage 5,MPEG video I and P frames are encrypted using DES cipher [9].

B. Image Encryption

Many Image encryption algorithms are developed by cryptographic principles. Scrambling algorithms [12] are also used for image encryption by dividing the whole image into its binary form. Yicong Zhou, Karen Panetta and Sos Agaian [13] developed an image encryption algorithm by doing XOR operation with key image, by using scrambling method. Yongliang Xiao and Limin Xia[14] designed an image encryption algorithm in which the position of images are changed and chaotic maps are used to change the grey scale bits

C. Video Encryption

Secure MPEG is an after compression algorithm [2] in which important parts of video stream are selected and encrypt them using RSA or DES in CBC mode. SECMPEG encrypts important so that four levels of security may be achieved by selecting different parts of video for encryption. Maples and Spanos in [11] have proposed full encryption and highly applies for secured video transmission. They introduced a new method called AEGIS to securely encrypt the MPEG video stream based on selective scheme.

Video encryption algorithms require more time for encrypting the video data. These algorithms can be classified as naïve approach, selective approach and Zigzag method along with RC4 and AES [14]. In naïve approach, the idea is to encrypt video streams as byte by byte otherwise bit by bit and our proposed method follows the naïve approach.

III. METHODOLOGY

In general multimedia encryption is performed by getting input as block of bits or bytes as plaintext. But in the proposed cipher we process the plain text bit by bit with two keys K and M.

In our algorithm two keys M and K, may be chosen by pseudo random generator from the input file or any other file, which is converted into binary format. For encryption we use stream cipher in which the entire video stream converted into bit stream is involved with XOR operation with two keys K and M.

Though the algorithm describes the encryption and decryption process in terms of blocks, but the actual implementation is in terms of bits. Therefore it is a stream cipher in disguise which uses the basic operations of sum, product and XORing. The implementation style guarantees the efficiency in terms of speed and most applicable for multimedia encryption

Encryption Algorithm:

1. Choose a Key K of size n+1 bits.
   $K= (k_0,k_1 \ldots k_n), k_0=1$
2. Choose a Key M of size n+1 bits.
   $M=(m_0,m_1,\ldots m_n)$
3. Let P be a plain text of any size in the binary form
   $P=(P_0P_1 \ldots P_n,P_{n+1},\ldots\ldots P_{2n},P_{2n+1} \ldots..)$
4. Let '+' denote the arithmetic modulo operator and * denote the XORing operator between bits.
5. For (0<=j<=(size of P)
   Let
   $C=(K+2P_0K+2^2P_1K+\ldots\ldots..2^{j+1}P_j)*(M+2^{n+1}M+2^{2n+1}M+\ldots.2^{ln+1}M)$
   where l is size of P, say P size satisfies
   $l_n<=Psize<=l_{n+1}$

Decryption Algorithm:

For (j=0,1,2……till the end of Cipher text

1. $C*(M+2^{n+1}M+\ldots\ldots..2^{ln+1}M)$

   $=K+2P_0K+2^2P_1K+2^3P_2K+\ldots..2^{j+1}P_jK\ldots..$

2. $(K+2P_0K+2^2P_1K+\ldots\ldots\ldots2^{j+1}P_jK\ldots\ldots\ldots\ldots) - K$

   $= 2P_0K+2^2P_1K\ldots.2^{j+1}K\ldots\ldots\ldots$

From the RHS of the above equation we get the bit P_0

3. Subtract $2P_0K$ from RHS of step 2 ,we get

   $2^2P_1K+2^3P_2K+\ldots\ldots.2^{j+1}P_jK+\ldots\ldots$

   and thus we get next bit P_1.

IV. EXPERIMENTAL RESULTS

If you We have experimented this algorithm with Intel® Dual Core CPU 5 GHz, 2 GB of RAM. Java programming language using Net Beans has been used since it has many advantages with the network programming. In addition, we tested the algorithm for variable key size of K and M. We experimented our final code that handle the encryption operations with mathematical functions described in encryption and decryption algorithm. Multimedia files of all types either, image or audio or video are encrypted and decrypted by the above algorithm.

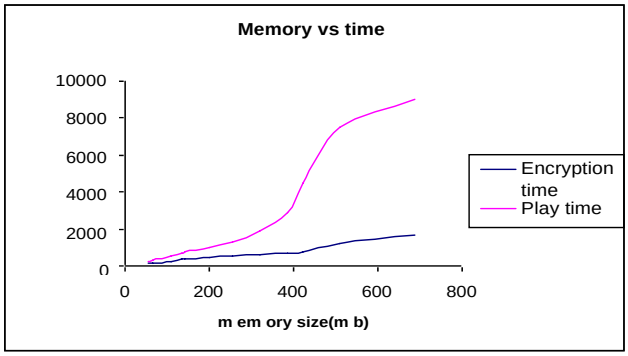

Fig. 2..Results for Encryption Vs Playtime

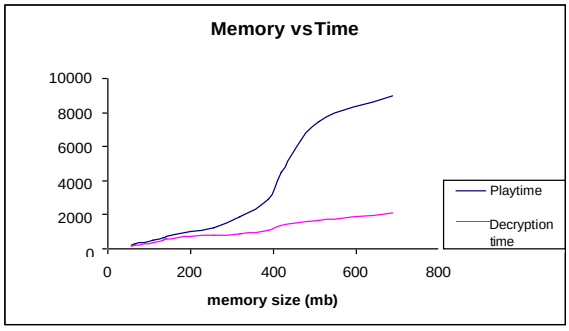

Fig. 3. Results for Decryption Vs Playtime

Many multimedia files of different sizes are encrypted and decrypted and their time for encryption and decryption are calculated and given in Table 1.

Table- I: Encrption and Decryption Time

Key size	Encryption	Decryption
8	7 minutes 11 secs 875 msecs	13 min 33 secs 590 msecs
16	3 minutes 33 secs 499 msecs	4 minutes 33 secs 590 msecs
32	2 minutes 50 secs 260 msecs	3 minutes 39 secs 449 msecs
64	2 minutes 50 secs 260 msecs	3 minutes 33 secs 590 msecs
128	2 minutes 50 secs 260 msecs	3 minutes 33 secs 590 msecs
256	2 minutes 50 secs 260 msecs	3 minutes 33 secs 590 msecs
512	2 minutes 50 secs 260 msecs	3 minutes 33 secs 590 msecs

V. SECURITY AND PERFORMANCE ANALYSIS

The security analysis can be done into three categories such that key setup function, algebraic analysis and correlation analysis of the binary functions and also we discussed the statistical properties of proposed stream cipher.

A. Key Setup Function

Since the key is generated randomly from the input text, we prevent key redundancy. The key K ensures that the plaintext

A conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

is expanded and it is ready for performing addition modulo This process yields pseudo cipher text and then XORing with M, we get the cipher text.

B. Algebric Analysis

We analyzed dependence of output byte's on its input bytes and it is found that the degree of dependence is very low.

C. Linear Correlation Analysis

The correlation analysis is to find the approximations bits in the input to the extracted output. It is found from the pseudo cipher generation that the correlation between the bits is very low.

D. Chosen Plain Text Attack

From the resulting cipher text the cryptanalyst tries to get the key. In our approach the key length is not fixed. The key pair and the encryption function are designed in such a way that one key is used for one type of operation and the other key is used for different operation. The algorithm is tested on randomly chosen plaintext and it is found that it is very difficult to find the key pair from the cipher text.

E. Brute Force Attack

A brute force attack is used to break the key used in encryption. It involves in finding all possible keys until the key used for encryption is found. The key size selection depends on the way of performing brute force attack. In the proposed algorithm the two keys are used and it is difficult to find key pair.

VI. CONCLUSION

Thus in this paper we presented a novel stream cipher for securing multimedia data. The algorithm is effectively implemented on any type of multimedia content using naïve approach and it is efficient than traditional algorithms like AES,DES,RC4 etc..

REFERENCES

1. Bruce Schenier,"Applied Cryptography", John Wiley and sons, New York,2nd edition,1996.
2. J. Meyer and F. Gadegast, "Security mechanisms for multimedia data with the example MPEG-1 video," in Project Description of SECMPEG. Berlin, Germany: Technical Univ. Berlin, 1995.
3. Min Wu, Yinian Mao, "A Joint Signal processing and Cryptographic Approach to Multimedia Encryption" IEEE Transactions on Image Processing , Vol. 15, No. 7, July 2006.
4. L.Qiao and K.Nahrstedt,"Comparison of MPEG encryption algorithms"Int..Comput.Graph,vol.22,no 3 1998.
5. J. Wen, M. Muttrell, and M. Severa, "Access control of standard video Bit streams," presented at the Int. Conf. Media Future, Florence, Italy, May 2001
6. L. Tang, "Methods for encrypting and decrypting MPEG video data efficiently,"in Proc. 4th ACM Int.

Conf. Multimedia, Boston, MA, Nov.1996, pp. 219– 229.
7. J.Wen, M. Severa,W. Zeng, M. H. Luttrell, and W. Jin, "A format-compliant configurable encryption framework for access control of video," IEEE Trans. Circuits Syst. Video Technol., vol. 12, no. 6, pp. 545– 557, Jun. 2002.
8. T.-L. Wu and S. F. Wu, "Selective encryption and watermarking of MPEG video," presented at the Conf. Image Science, Systems, Technology, as Vegas, NV, 1997.
9. C.-P. Wu and C.-C. Kuo, "Efficient multimedia encryption via entropy Codec design," Proc. SPIE, vol. 4314, Jan. 2001.
10. Design of Integrated Multimedia Compression and Encryption Systems Chung-Ping Wu, Member, IEEE, and C.-C. Jay Kuo, Fellow, IEEE.
11. T.B.Maples and G.A.Spanos. "Security for Real-time MPEG-1 Compressed Video in Distributed Multimedia Applications", Proceedings of the IEEE 15th Annual International Conference on Computers and Communications, 1996
12. Yicong zhou,Karen Panetta,Sos Agaian,"Image Encryption Using Binary key images", Proceedings of The IEEE International Conference on Systems,Man and Cybernetics,San Anbnio,USA,October,2009
13. T. Seidel, D. Socek, and M. Sramka, "Cryptanalysis of Video Encryption Algorithms", Proceedings of the 3rd Central European Conference on Cryptology ,TATRACRYPT 2003,

AUTHORS PROFILE

P.Vidhya Saraswathi is working as Assistant Professor in the Department of Computer Science and Information Technology, Kalasalingam Academy of Research and Education, ,Krishnankoil,Srivilputtur(Via),Tamilnadu ,India.She has completed B.Sc(ComputerScince),Master degree in Computer Applications,M.Phil(Computer Science) and Ph.D in Computer Applications.Her area of interests include Multimedia Security,Image Processing,Data Analytics,Cloud Computing etc

Dr.M. Venkatesulu received his post graduate degree in Mathematics from Sri Venkateswara University, Tirupati, India in 1975 and Ph.D. in Mathematics from Indian Institute Technology, Kanpur in 1979, He worked as a faculty at Shri Sathya Sai University, Prashanthinilayam, India between 1983 and 2002. He worked as a consultant for Satyam Computers, Hyderabad, India for a short period. He was visiting professor at the University of Missouri, Kansas City, USA between August 2006 and May 2007. Currently, he is a senior professor of the Department of Information Technology at Kalasalingam University, Krishnankoil, Srivilliputtur (via), Tamil Nadu, India. His areas of interests include differential equations, image processing, cryptography, bioinformatics and grid computing