ISSN 2320-9984

Volume 6 Issue 2 | June 2018 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

A New Method of MPEG Video Encryption Using Frame Shuffling

Pratiksha Agrawal
M.Tech. Research Scholar
Shri Ram Group of Institutions
Jabalpur, (M.P.) [INDIA]
Email: heritage.etihadyui@gmail.com

Santosh Sahu
Assistant Professor
Department of Civil Engineering
Shri Ram Group of Institutions
Jabalpur, (M.P.) [INDIA]
Email: sant303@rediffmail.com

Anupam Choudhary
Lecturer
Kalaniketan Polytechnic College
Jabalpur, (M.P.) [INDIA]
Email: choudharyanupam7@yahoo.com

Abstract**—***In this era of digital communication, using and sharing of multimedia content is on peak. Data transmitted over the internet may include sensitive information which should not be intelligible to unauthorized access. Therefore, security and privacy are the topmost concern. Video security can be achieved using encryption. Also, design of an encryption method depends on the requirements of a particular application in terms of security level, cost and time. In this paper, we have proposed a new approach to encrypt a video by using combination of zigzag rule, swapping rule, selective method and AES which together contribute to achieve a great security level and moderate computational complexity.*

Keywords:**—***Video Encryption, MPEG, Frame Extraction, Zig-zag, Swap, Selective Scheme, AES.*

I. INTRODUCTION

Due to rapid increase in the multimedia usage, the need to secure and protect data shared over the network has become topmost priority. Now-a-days use of multimedia applications like video chat, video on demand, video broadcast, conferencing etc. has become the most popular and convenient ways of communication. So, large data is generated and stored which must be protected by encryption [1]. Video encryption is different from conventional encryption model. Basically, there are two models of video encryption, the first model is to encrypt full video data and second is selective scheme which aims at reducing the computational cost by encrypting only selected portions. MPEG (Moving Picture Experts Group) is a video compression format which consist of three types of frames namely I -frames, P-frames and B-frames. In recent years, video encryption has become a promising field of research in the world of information security.

This paper is organized into 5 sections: Section 1 presents a brief introduction. In section 2, we explore the literature for related and significant work done in this field. Section 3 provides detailed description of the proposed method and the steps involved. Section 4 presents the experimental results and a brief analysis of the outcomes. Finally conclusion and scope of future research is given in section 5.

II. RELATED WORK

Maples and Spanos in [2] proposed a method based on selective scheme AEGIS, which securely encrypts an MPEG video. Their work focuses on encrypting only I-frames, while P and B-frames are left unencrypted. Meyer and Gadegast in [3] proposed a method SECure MPEG, also based on selective scheme. Their work focuses on first selecting the important parts of a video stream and then encrypting them using DES or RSA. This method allows selecting one or more parts of video including headers, DC coefficients, lower AC coefficients, I-frames, I -blocks in P-, B-frames or entire bit stream. Qiao and Nahrstedt in [4] proposed a method based on scrambling of video bytes. All even numbered and odd numbered bytes are XORed to construct half of the cipher text; the other half is formed by applying DES over even numbered bytes. Tang in [5] proposed Zigzag permutation based method which permutes the DC coefficients of I-frames in a zigzag order. Shi, Wang and Bhargava [6] [7] [8] [9] proposed four different algorithms, all based on selective scheme. First algorithm VEA (Video Encryption algorithm) focuses on encrypting only the Huffman codewords in I-frames. Second algorithm VEA-II focuses on encrypting only the sign bits of DC coefficients. The third algorithm was MVEA (Moving VEA) which focuses on encrypting the differential values of DC coefficients along with motion vectors contained in P-, B-frames. Fourth algorithm was designed for real time application, called RVEA (Real Time VEA). This algorithm focuses on encrypting the sign bits of DCT coefficients and motion vectors.

III. PROPOSED METHOD

We propose a new method to encrypt MPEG videos to secure video sharing over the network. The proposed method combines the concepts of zig-zag permutation and selective approach to get the encryption done reducing the computational complexity. When a video is tested on this method the video is split into a number of frames depending upon the size of the video. Next a Zig-zag function is used to rearrange the extracted frames in a zig-zag fashion. Again, some of the frames are swapped to increase the level of induced randomness. To implement the selective scheme, only some of the frames are selected and encrypted. These are called as "key frames". The encrypted and non-encrypted frames are then stitched together to recreate the video. The steps are following below:

A. Frame Extraction Block: Our method inputs an MPEG video "indi008.mpg" which is of 00.23 seconds in length and extract a total of 706 frames from it. This sequence of extracted frames when navigated horizontally, each frame in the row replaces previous frame on the display screen and hence give a sense of motion. These frames are saved in movie frame format.

B. Zig-zag Rule: A video is worth watching when its individual frames are in proper sequence. Let the frame sequence be M1 M2 M3 M4 M5… A line having sharp turns in alternating directions is known as zigzag rule. Using zig-zag rule the first frame will be placed in right position. Again second frame will be placed in left, third frame will be placed in right position and so on. After zigzag, the sequence will become M5, M3, M1, M2, M4… Therefore, the correlation between the consecutive frames is reduced. This causes the video even harder to be intelligible.

C. Swapping: Again some of the frames from resulted sequence M5, M3, M1, M2, M4… are swapped. For example M3 is swapped with M2 and M4 is swapped with M3. The resulting sequence would become M5 M2 M1 M4 M3… Swapping further reduces the correlation between frames.

D. Selective Scheme: A selective scheme selects only the important part(s) from a video that may contain sensitive information and encrypts them using a conventional cipher. There are numerous ways to select sensitive information from a video. Our method utilizes the concept of shot transition in a video. The frame at which a video shot transits can tell us

about the video content and is termed as "key frame".

E. Encryption: The selected key-frames undergo AES encryption. AES is designed on basic techniques of transposition & substitution. AES have simple and efficient working syntax; it is more secure than other algorithms and gives flexibility to choose length of the key.

F. Decryption: The final step in the method is decrypting the video. When an encrypted video is received, it is decrypted using the reverse algorithm in AES. After decrypting the video, the receiver desire to understand the actual content of video. Thus post-decryption re-arrangement of frame sequence and recreation of original video using video editing software is necessary.

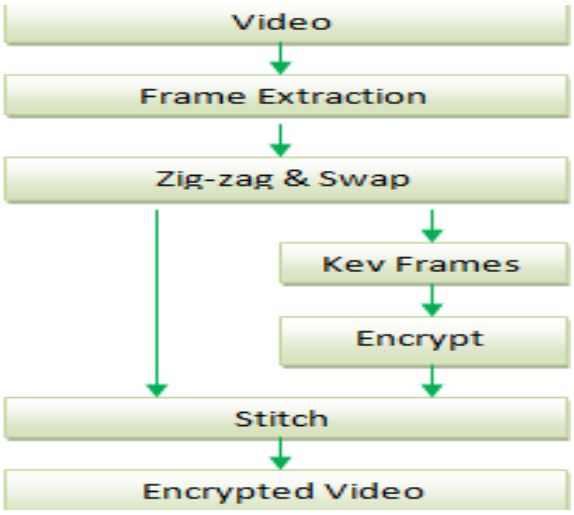

Figure1. Encryption

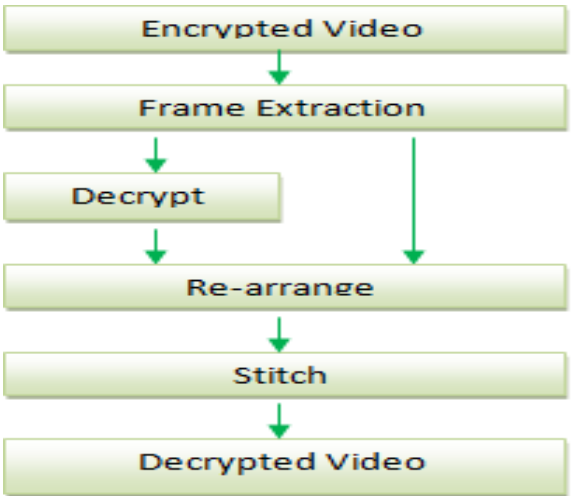

Figure 2. Decryption

4. SIMULATION RESULTS

This section of the paper contains the experimental result analysis of the proposed video encryption method. By seeing fig.3 it is clear that the encrypted frame gives no idea about the original frame content. Thus, our proposed method is immune to perceptual attacks. The histogram of a frame shows graphical distribution of the pixel intensities. We plot the histograms of original frame as well as of the encrypted frame. It is clear that the histogram of the encrypted frame is different from the respective histograms of the original frame. Also, histogram of encrypted frame is almost uniformly distributed. Thus, the encrypted frame does not provide any evidence to use in any statistical attack on the proposed technique. The proposed method makes statistical attacks difficult.

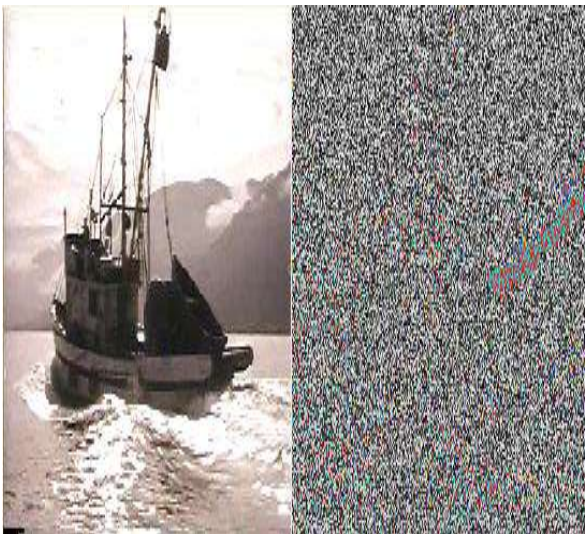

Figure 3. Encrypted frame

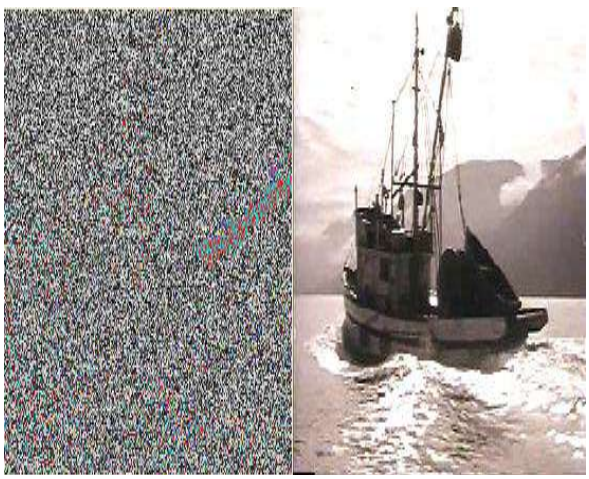

Figure 4. Decrypted frame

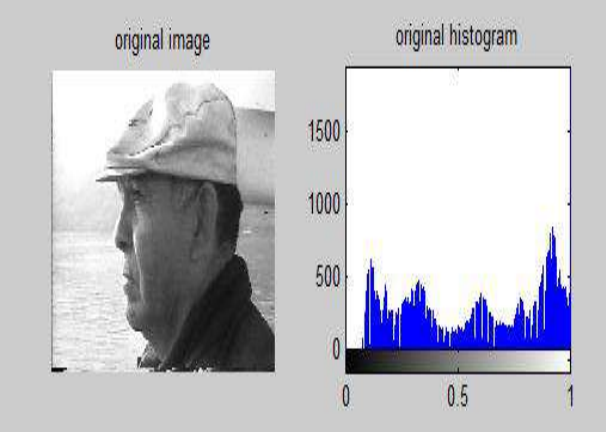

Figure 5. Histogram of original frame

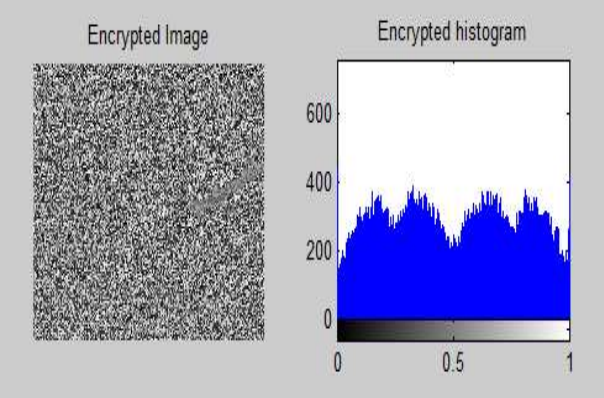

Figure 6. Histogram of encrypted frame

5. CONCLUSION AND FUTURE WORK

Security and Protection of video data shared over the network is utmost important. A video file is different from a text or binary file. Moreover, different multimedia applications need different level of security, therefore specific algorithms are needed which are specially designed to encrypt video data. A new method of encrypting an MPEG video was introduced which combines the beneficial features of zig-zag permutation, selective scheme and AES. The experimental results shows that proposed method is secure enough to be applied in entertainment industry applications as well as personalized video sharing applications.

The future work includes extending this work to experiment with other video formats as well. Researchers should focus on designing new algorithms that maintains a tradeoff between security, computational time, cost and size of video.

REFERENCES:

[1] Atul Kahate, Cryptography and Network Security, (Second Edition 2008)

[2] G.A. Spanos and T.B. Maples, "Security for Real-Time MPEG Compressed Video in Distributed Multimedia Applications," in Conference on Computers and Communications, 1996, pp. 72-78.

[3] J. Meyer and F. Gadegast, "Security Mechanisms for Multimedia Data with the Example MPEG-1 video," Project Description of SECMPEG, Technical University of Berlin. 1995

[4] Qiao L, Nahrstedt K., Comparison of MPEG encryption algorithms, International Journal of Computer and Graphics,1998;22(4);437-48

[5] L.Tang, "For Encrypting and Decrypting MPEG Video Data Efficiently", in Proceedings of the Forth ACM International Multimedia Conference, 1996, pp. 219-230.

[6] B. Bhargava, C.Shi, S.Y. Wang, "MPEG Video Encryption algorithms", Multimedia tools and applications 24(1)(2004)

[7] C. Shi and B. Bhargava, "A Fast MPEG Video Encryption Algorithm," in Proceedings of the 6th ACM International Conference on Multimedia, 1998, pp. 81–88

[8] C. Shi and B. Bhargava, "An efficient MPEG video encryption algorithm," in Proceedings of the 17th IEEE Symposium on Reliable Distributed Systems 1998, pp.381–386.

[9] C. Shi, S. Y.Wang, and B. Bhargava, "MPEG Video Encryption in Real-time using Secret Key Cryptography," in Proceedings of the

International Conference on Parallel and Distributed Processing Algorithms and Applications, 1999

[10] Ravindra Purwar et.al. "A Novel Approach of Digital Video Encryption" in International Journal of Computer Applications

[11] N. Hemrajani, D. Goyal "Novel Selective Video Encryption for H.264 Video" in International journal of Information Security Science.

[12] K. John Singh et.al. "A Survey on Joint Compression and Encryption Techniques for Video Data" in Journal of Computer Science.