ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3, Issue 10 October, 2014 Page No. 8901-8904

A Review Paper on Data Embedding in Scrambled Digital Video for Data Security & Authentication

Jamna Kaur[1] , Rachna Rajput[2]

[1]Guru Kashi University, Department of CSE,
Talwandi Sabo, Punjab, India
jamnaparmarg7@gmail.com

[2]Guru Kashi University, Department of CSE,
Talwandi Sabo, Punjab, India
Rachna12cse@gmail.com

Abstract: ***In the recent years with the development of internet technologies, video technologies have been broadly used in TV, communication and multimedia, So security is required on video data. A technique for embedding data in scrambled AVI video is described. The embedding technique is applied to the video sequence jointly with the video scrambling algorithm. The scrambling operation together with the data embedding process are performed prior to AVI encoding, and the scrambled and data-embedded video is AVI encoded with a minimal increase in the AVI bit rate. In this study a data embedding in scrambled video for the security and authentication of data.***

Keywords : Multimedia security, contents access control, video scrambling etc .

1. Introduction

Due to rapid development of various multimedia technologies, more and more multimedia data are generated and transmitted in the medical, commercial, and military fields, which may include some sensitive information which should not be accessed by or can only be partially exposed to the general users. Therefore, security and privacy has become an important. The main goal of cryptography is keeping data secure form unauthorized attackers. Therefore data is encrypted through process of Encryption. The reverse of data encryption is data decryption With digital video transmission, encryption technologies are needed that can protect digital video from attacks during transmission. Due to the huge size of digital videos, they are usually transmitted in compressed formats such as MPEG. An AVI transparent video scrambling technique that allows the unauthorized user to have an arbitrarily degraded view of the current program has been proposed earlier. Some broadcast service operators would like the viewing of such a sufficiently corrupted video on the screen of the unauthorized viewer to allure potential customers without sacrificing the level of robustness provided by digital encryption techniques. In this technique, the scrambling is performed prior to the AVI encoding, and the scrambled video is AVI encoded with only a minimal increase in the AVI transport stream (TS) bit rate (or alternately a minimal degradation of the picture at fixed bit rate). This is achieved by performing a linear scrambling of the video in blocks as follows: The incoming picture frames are split into scrambler blocks (SB) of size equal to integer multiples of an AVI macro- block size. The SB boundaries are block-synchronous with the AVI block structure. The RGB streams in a SB are coded using a linear transformation of pixel values containing a random mixture of brightness, contrast changes and negative/ positive switching with different parameters for each of the RGB components. The proposed scrambler is inserted between the RGB source and the component input of any AVI compliant encoder no modifications are required to the AVI encoder. The degradation level of the displayed video is controlled by the service operator and the level may be changed arbitrarily anytime. This technique is applicable to any digital broadcast scheme that is based on the AVI compression. The scrambling is totally independent of the AVI level and profile, frame frequency, the particular sampling scheme and the delivery method. A smartcard is used on the subscriber side for security. The scrambling technique provides image level scrambling at a level of security comparable to the bit stream level encryption of the existing conditional access techniques. The scrambling parameters and other data as required by the service need to be transmitted to the decoder. Hence, means of delivery of such data in some way is necessary. It is possible to embed such data into the picture within the context of the above scrambling technique. This paper describes a data embedding scheme to be utilized in the video scrambling system and described data embedding approach requires an understanding of the principles of the particular video scrambling.

1.1 Need Of Video Encryption

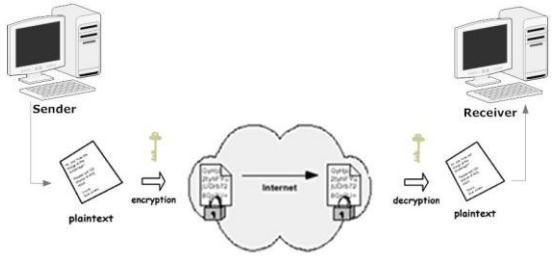
Encryption of images and videos are important due to following reasons:

1.1.1 For preventing unwanted viewing of transmitted video, for example from law enforcement video surveillance being relayed back to a central viewing centre.
1.1.2 To protect the private multimedia messages that is exchanged over the wireless or wired networks.
1.1.3 Video Encryption is helpful in securing videos used in services like video on demand (VOD), Video conferencing-learning.
1.1.4 For protecting medical videos which may contain private information of a patient from unauthorized access by malicious users.
The video encryption based on study of Deformation and Formation Algorithm which is useful in protecting various type of videos that contain private information.

1.2 Basic Concept Of Video Encryption

The encryption and decryption of a plain text or a video stream can be done in two ways:

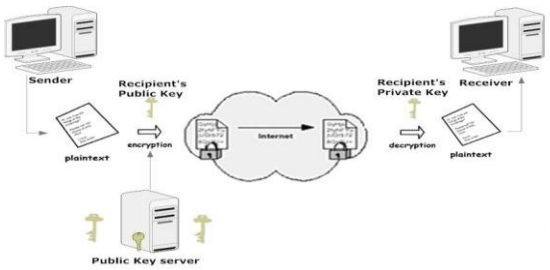
1.2.1A Secret Key Encryption



A single secret key can be used to encrypt and decrypt the video streams. Only the sender and the receiver have this key. Basically, the security level of the symmetric keys encryption method is totally depends on how well the users keep the keys protected. If the key is known by an intruder, then all data encrypted with that key can be decrypted. Most common algorithms in these categories are Data Encryption Standard (DES), Triple DES, and Advance Encryption.

1.2.2 Public key encryption

There are two keys, one for encryption and the other for decryption. The public key, which is known for all senders, is used for encryption.While the private key, which is owned only by the receivers, is used for decryption. It is based on a two-key crypto system in which two parties could securely communicate over a non-secure communications channel without having to share a secret key and solves the problem of secret key distribution by using two keys instead of a single key



1.3 Various Approaches Used For Encryption

1.3.1 Full-encryption

A video encryption algorithm that performs encryption on the entire video bit stream belongs to this class of algorithms. It suitable for real time video as requires heavy computation and has slow speed.

1.3.2 Selective Encryption

Also known as partial encryption & is a subcategory of variable encryption. The algorithms in this class selectively encrypt the bytes within video frames. As these algorithms are not encrypting each and every byte of video data, it reduces computational complexity.

2 Various Digital Video Encryption Schemes

2.1 Naïve Approach

It is a type of full encryption approach in which a conventional cryptosystem is used in the encryption step. The most straight-forward method to encrypt every byte in the whole Moving Picture Experts Group (MPEG) stream using standard encryption schemes such as DES or AES. However,this algorithm not applicable for heavy video, because it is very slow especially when we use triple DES. Because of the encryption operation the delay increases therefore it is not suitable for real time video encryption.

2.2 Pure Permutation Algorithm

It simply scrambles the bytes within a frame of MPEG stream by permutation. It is extremely useful in situation where the hardware decodes the video, but decryption must be done in software. The pure permutation algorithm is vulnerable to known-plaintext attack, and hence its use should be careful considered, because by comparing the cipher text with the known frames, the adversary could easily figure out the secret permutation list. Once the permutation list is figured out, all frames could be easily decrypted. Notice that knowing one I frame of MPEG stream is enough to decrypt the permutation list based on Shannon's Theorem.

2.3 Zig-Zag Permutation Algorithm

In this method, instead of mapping the 8x8 block to 1x64 vector in "Zig-zag" order, it maps the individual 8x8 block to a 1x64 vector by using a random permutation list (secret key). Zig-Zag permutation algorithm consists of three main steps:
1. Generate a list of 64 permutations.
2. Complete splitting procedure.
3. Apply the random permutation to the split block.

Since mapping Zig-Zag order and mapping according to the random permutation list have the same computational complexity, the encryption and decryption add very little overhead to the video compression and decompression processes

2.4 Chaos Based Encryption Algorithms

This is one of the popular algorithms in the field of neural network to perform encryption & decryption as it is a low cost algorithm & is suitable for large amount of data.

2.5 Video Encryption Algorithm (VEA)

In this algorithm the I- frame blocks carry the most important information so the scheme sufficient to encrypt only the sign bite of the DC coefficients in the I-frame blocks by simply XORs sign bites of DC coefficients with a secret key. The security level of this scheme depends on the length of the key. However, too long key size may be infeasible and impractical. On the other hand with a short key size, the system could be easily broken.

3 Comparision Of Video Encryption Algorithm.

We have currently known encryption algorithms for secure video streams and evaluated them with respect to three metrics: security level, encryption speed, and encrypted MPEG stream size. The Navïe Algorithm and Video Encryption Algorithm (VEA) are the most secure algorithms, where Zig-Zag Permutation Algorithm has serious security flaws and can not withhold the known plaintext attack nor the ciphertext only attack. With respect to encryption speed, Pure Permutation Algorithm and Zig-Zag Permutation Algorithm are very fast, and Navïe Algorithm is very slow due to applying DES on whole MPEG stream. When comparing the algorithms in terms of size metric, VEA, Pure Permutation Algorithm and Navïe Algorithm do not change their size, which is very much desirable. On the other hand, Zig-Zag Permutation Algorithm significantly increase the stream size which defeats the compression purpose of MPEG encoding. In summary when applying different encryption algorithms to MPEG encoded video and its choice depends on the applications.

4 Literature Survey

There are various papers available in journals which are based Video Encryption .Some of them are All videos that are needed to be protected from suspicious users require Encryption.To solve this problem of security, a wide variety of encryption techniques have been discussed in this . This paper describe the description and comparison between encryption methods and representative video algorithms are discussed. With respect not only to their encryption speed but also their security level and stream size.

[Ref.1] In this relation between quality of video Encrypting and choice of encryption algorithm are discuss. This study indicates that the classification of encryption algorithm according to two categories, Namely Full Encryption & selective encryption. It shows that full encryption requires more computational cost & has less speed due to large data to be encrypted. The classification is also done on the basis of various performance parameters such as Encryption ratio, Cryptographic security.

[Ref.2] This study focuses on a novel scheme to efficiently secure variable length coded (VLC) multimedia bit streams. The proposed scheme employs code word diffusion and content based shuffling techniques to achieve security. The main idea of this encryption scheme is to make the decoding of the VLC codes in the bit streams computational infeasible in the absence of a private key. Here the contents are divided into random size blocks. Within each block, a few bits are flipped such that the correlation present among codeword is diffused. Next the blocks are randomly shuffled.

[Ref. 3] This study focuses on a novel scheme to efficiently secure variable length coded (VLC) multimedia bit streams. The proposed scheme employs code word diffusion and content based shuffling techniques to achieve security. The main idea of this encryption scheme is to make the decoding of the VLC codes in the bit streams computational infeasible in the absence of a private key. Here the contents are divided into random size blocks. Within each block, a few bits are flipped such that the correlation present among codeword is diffused. Next the blocks are randomly shuffled.

[Ref. 4] There are many algorithms in existence for scrambling of the video frames and to encrypt them. The proposed scheme treats the video as a framing sequence. The frames are sequenced by a provided algorithm. Secondly an index number is provided for each frame. Then the frames are encrypted to hide the information using thresholding method. Then the frames are sent in a random order. At the receiver side, the encrypted frames are decrypted. By using the index values the distributed frames are arranged again in a correct order. Proper keys are used to scramble the frames of the video initially. The content of the frames remains the same.

[Ref.6] we give a method to generate an encrypted video by encrypted Video-frame.Based on novel secure video scheme, an effective and generalized scheme of video encryption. It is a matrix computation scheme which uses a concept of Video-frame and xor operation. This paper proves that proposed scheme is able to fully encrypt the video frame and have a better performance that can be measured by different Parameters. Further we can extend our approach into a digital video stenography.

[Ref.8] In this study, classification and description of various video encryption algorithms are presented. In this Naïve algorithm provides highest level of security but it is very slow in nature and cannot be used in real time. Permutation based algorithms are generally faster but they do not provide sufficient level of security. Selective encryption algorithms reduces computational complexity by selecting only a minimal set of data to encrypt but their security and speed level generally vary based on which and how many parameters they encrypt.

5 Conclusion

In this paper I have studied the digital video encryption algorithms for the video security. I have analyze both security and performance aspects of the proposed method and secure from as a cryptographic point of view. These are video frames studied for the authentication of the video security to provide the good results. For future research, it is proposed that this novel scheme be developed to full encrypt video sequences. The following are some point to improve our proposed system. Further improvement to the security level can be achieved by encrypting the I-Frame blocks in P- and B-Frames.

References

[1] M. Abomhara,, Omar Zakaria, Othman O. Khalifa "An Overview of Video Encryption Techniques", International Journal of Computer Theory and Engineering, Vol. 2, February, 2010.

[2] Amit Pande, Prasant Mohapatra, Joseph Zambreno," Using Chaotic Maps for Encrypting Image and Video Content", IEEE International Symposium on Multimedia ,2011.

[3] A.Shiva Krishna Reddy ,K. Srimathi, R. Rajalakshmi, "The IndexingAlgorithm for Scrambled Frames in Video Encryption "International Journal of Advanced Research in Computer Science and Software Engineering Volume 4,February 2014.

[4] Yogita Negi ,"A Survey on Video Encryption Techniques, International Journal of Emerging Technology and Advanced Engineering Volume 3, Issue 4, April 2013.

[5] Mayank Arya Chandra, Dr. Ravindra Purwar, Dr. Navin Rajpal ,"A Novel Approach of Digital Video Encryption", International Journal of Computer Applications Vol 49, July 2012.

[6] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki," A Modified AES Based for Image Encryption", World Academy of Science, Engineering and Technology 3 2007.

[7] Sivakami, R. Nagakrishnan, Ellammal "A Digital Watermarking System For Video Authentication using DCT", Integrated Journal of Engineering Research and Technology (IJERT), Vol 01, Jan-Feb 2014.

[8] Jolly shah and Dr. Vikas Saxena," Video Encryption: A Survey",International Journal of Recent Trends in Engineering, IJCSI International Journal of Computer Science Issues, Vol. 8, March 2011.

[9] G.Madhuri, B.VijayKumar, V. Sudheer Raja, M. Shasidhar "Data Embedding in Scrambled Digital Video for Security", Int. J. on Recent Trends in Engineering and Technology, Vol. 6, Nov 2011.

Author Profile

Jamna Kaur received the B.Tech degree in Computer Science Engineering from Punjab Technical University Jalandhar in 2011. Currently she is pursuing M.Tech degree in Computer Science Engineering from Guru Kashi University, Talwandi Sabo, Bathinda (Punjab). Her research interests include Digital Video proceesing.