SECURE META DATA HIDING IN ENCYPTED VIDEO STREAM USING AES

Shaista Siddiqui[1], Samta Gajbhiye[2],

[1] Research scholar, Department of Computer Science and Engineering,
Shri ShankaraCharya Technical Campus, Bhilai, CG, India.
[2] Sr. Associate Professor &Head, Department of Computer Science and Engineering,
Shri Shanakracharya Technical Campus, Bhilai, CG, India

ABSTRACT

With the advancement in the use of Internet, security concerns have been increased in public these days. Encryption techniques have gained importance to carry out the communication of sensitive data. Rapid development in multimedia technology has led to the transmission of multimedia data in various fields like commercial, medical, military fields which generally includes sensitive or private data 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. Over the last few years several encryption algorithms have applied to secure video transmission. While a large number of multimedia encryption schemes have been proposed in the literature and some have been used in real products, cryptanalytic work has shown the existence of security problems and other weaknesses in most of the proposed multimedia encryption schemes. In this paper, a brief discussion of the previously developed encryption techniques has been discussed; also a method is proposed to efficiently hide the meta data in encrypted video streams to enable secure communication of sensitive data over the internet.

Keyword: - *symmetric encryption, asymmetric encryption, Meta data, video stream, AES, DES, RSA, Public Key, Secret key*

1. INTRODUCTION

Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers or un intended users while stored and transmitted. Data cryptography mainly is the scrambling of the content of data, such as text, image, audio, video and so forth to make the data unreadable, invisible or unintelligible during transmission or storage called Encryption. The main goal of cryptography is keeping data secure form unauthorized attackers. The reverse of data encryption is data Decryption, which recuperate the original data [1][2]

The various algorithm available for security services like Data confidentiality, Integrity and Authentication to protect against the attacks like release of message content, modification of message and masquerade etc.[3]

Data Hiding is the process of secretly embedding information inside a data source without changing its perceptual quality. Data Hiding is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. Generally, in Data Hiding, the actual information is not maintained in its original format and thereby it is converted into an alternative equivalent multimedia file like image, video or audio which in turn is being hidden within another object. This apparent message is sent through the network to the recipient, where the actual message is separated [4]

1.1 Need Of Video Encryption

Currently, Internet and digital media are getting more and more popular. So, requirement of secure transmission of data also increased. Encryption of images and videos are important due to following reasons:[5]

1. For preventing unwanted viewing of transmitted video, for example from law enforcement video surveillance being relayed back to a central viewing centre.
2. To protect the private multimedia messages that is exchanged over the wireless or wired networks.

3. Video Encryption is helpful in securing videos used in securing videos used in video conferencing – learning.
4. For protecting medical videos of patients which may contain sensitive data and medical history, from unauthorized users.

1.2 Classification Of Encryption Algorithm

The algorithms in cryptography are categories into the two classes, Symmetric and Asymmetric algorithm. In Symmetric algorithm both the sender and receiver shares the same secret key for encrypting and decrypting. In Asymmetric encryption the user use pairs of keys.One key is for encryption and other key is decryption. Symmetric algorithms are faster as asymmetric involves the use of complex mathemtical functions for the processing.[6]

1.2.1 Symmetric Algorithm

In this type of algorithm both sender and receiver shares the same private or secret key for encrypting and decrypting. The key should be kept secret to obtain privacy. These algorithm do not consume much of the computing power. Examples are DES, 3DES, AES

1. DES: Data Encryption standard is a symmetric –key block cipher algorithm, in which the size of the block is 64 bit series of substitution and permutation.. The data and key bits are shifted then permuted after the permutation the bits are XOred, and sent through 8 s-boxes in each round.DES is widely used for encryption of pin numbers bank transactions.
2. AES: Advanced Encryption Standard is also a symmetric key algorithm. AES can be used for 10,12 or 14 rounds and can have variable block size and key size. The combinations of key sizes of 128,192 or 256 bits can be used. AES has several number of rounds in which each round is made of some stages. Various types of transformation such as substitution permutation network, mixing of column , adding of keys, are used. All the rounds except the last round uses the four transformation.

1.2.2 Asymmetric Algorithm

In Asymmetric encryption the user use pairs of keys .One key is for encryption and another is for decryption. The decryption key is kept secret also called “private key” or “secret key”, while “public key” is send to all for encrypting messages .Everybody having the public key is able to send encrypted messages to the owner of the secret key. Examples are RSA, DSA, and ELGAMAL**.**

1.3 Classification Of Video Encryption Algorithm

Video encryption algorithms can be classified in four categories [3]

1. Fully layered Encryption

In this case the complete content of video is first compressed and then encryption is done with the use of standard algorithms like DES, RSA, AES, etc. Because of its heavy computation ans slow speed this algorithm is not appropriate to be used in real time applications.

2. Permutation Based Encryption

The different permutation algorithms are used to scramble or encrypt the content of video. The scrambling of each and every byte is not necessary . Some algorithms use permutation list as secret key to encrypt video contents.

3. Selective Encryption

The video frames are encrypted with use of selective encryption algorithm in which not each and every byte of the video is encrypted. Selective encryption is a technique to save computational power, overhead, speed, time. Selective encryption is faster as compared to the full encryption of the data [7].

4. Perceptual Encryption

The requirement of the perceptual encryption is that quality of aural/visual data is only degraded by encryption to some extent i.e., the encrypted multimedia data are still partially perceptible after encryption. The quality degradation of aural/visual can be continuously controlled by a factor p.

2. PREVIOUS WORK

Many techniques has been introduced in the recent years to secure the video that are being transmitted over the network. Generally these videos are large in size and are transmitted after compression. Some of these techniques are discussed below.

2.1 Naïve Algorithm

The most straight-forward technique to encrypt every byte in the whole Moving Picture Experts Group (MPEG) stream can be done by using standard encryption schemes such as DES or AES. The MPEG bit-stream as text data and does not use any of the special structure [10]. Naïve algorithm provides the security benefits to whole MPEG stream as every byte is encrypted, and no algorithm is able to break like triple DES or AES. For the large size video it is not appropriate solution as it is very slow in particular when we use triple DES. The delay increases in the encryption operation and overload will be unacceptable for real time video encryption.

2.2 Pure Permutation

In this the bytes are simply scrambles by permutation within a frame of MPEG stream. In the condition where the hardware decodes the video it is very useful, but software should be used for decryption. This technique should be used carefully as it is more vulnerable to plaintext[11] . Since with the knowledge of ciphertext with the known frame, one can easily detect the permutaton list and once the permutation list is figured out, all other frames can be easily encypted

2.3 Zig-Zag Permutation

In Zig-Zag permutation[12] with the use of random permutation list (secret key) it maps individual 8x8 block to 1x64 vector instead of mapping the 8x8 block to 1x64 vector in "Zig- Zag" order. Since mapping according to random permutation list and mapping zig zag order have the equivalent computational complexity, very little overhead is added.

2.4Video Encryption Algorithm

Bharagava Shi, and Wang in [13] [14] have given four different video encryption algorithm i.e Algorithm I,Algorithm II(VEA), Algorithm III(MVEA), and Algorithm IV(RVEA)

Algorithm I is highly vulnerable to both ciphertext only attacks and known plaintext attack. With the knowledge of some of video frames, it can be compared with the encrypted frame to figure out the secret permutation p.[15]

Algorithm II(VEA): The security level of this algorithm depends on the key length. Long keys are infeasible and impractical where as short key system can be easily broken.

Algorithm III(MVEA): This algorithm was a modification to the algorithm III. Intead of encrypting only the sign bits of DC coefficient in the I frame bock, thr sign bits of the differential values of DC coefficient and motion vectors in P- frames and B frames are encrypted with the secret key which makes it more random and more viewable.

Algorithm IV(RVEA): Algorithm IV was proposed by Bhargava et al [14] called as real time video encryption algorithm. The major difference between RVEA and MVEA is that RVEA uses a traditional symmetric key cryptography to ecrypt the sign bits of DCT Coefficient and the sign bits of motion vcectos.

2.5 Selective Encryption Algorithm

Selective encryption technique provides quick security by only encrypting a selected portiob of a bit stream. Since this technique is comparatively faster than full encryption so it is widely used. Moreover this technique also saves the computational time, speed, power, overhead

3 .Problem Identification

- Video from various applications like medical data of patients, surveillance data from sensitive places may contain sensitive information which should not be revealed to unauthorized person.

- Thus encryption of such data is desirable. Moreover, when the amount of such data is increases, it becomes difficult to categorize, manage, store, retrieve data efficiently.
- Thus a mechanism of securely attaching meta data to video streams is required which can be decrypted without decrypting the entire video.

4. Proposed Work

The whole procedure can be accomplished in two phases:

1) Data Hiding
2) Data Extraction

4.1 Data Hiding

- Encrypt the video using a secret key.
- Hide the desired data using a different key.

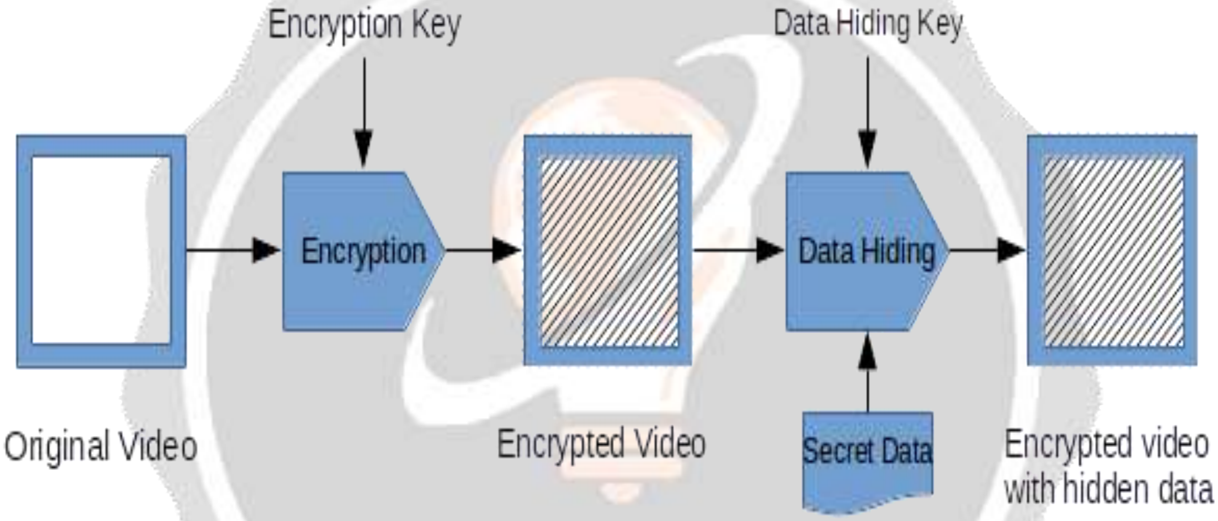

Fig-1: Work flow of phase 1(Data hiding)

The original video is first encrypted using an encryption key. The encrypted video is then ready to be embedded with meta data. For this, the meta data is embedded in the encrypted video using another data hiding key. Thus the result obtained is an encrypted video with the hidden data in it. The point to be noted is that the key used for encrypting the video and for hiding the meta data is different. This will be beneficial when we don't want the original video to be accessed by the unauthorized, but we want the meta data t be available for them.

4.2 Data Extraction

- Decrypt the meta data from the video using the same data hiding key as used during the data hiding phase.
- Decrypt the encypted video using the same key used in phase 1

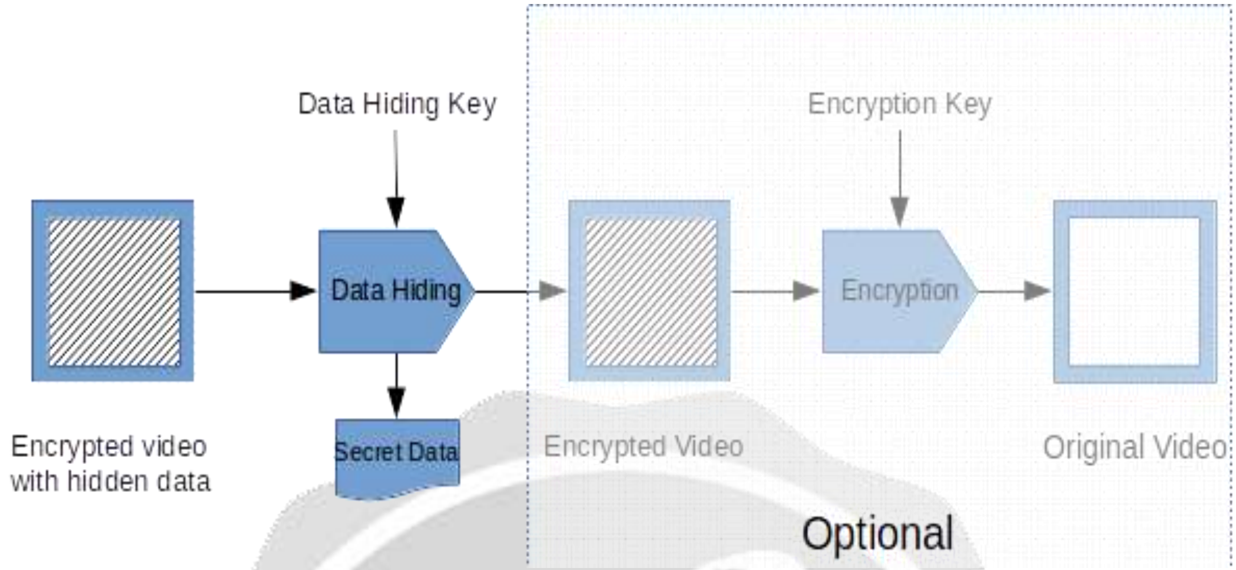

Fig -2: Work flow of phase 2(Data Extraction)

During the extracton phase, the meta data can be extracted from the encypted video without the need of decyption of video Thus preserving the secrecy of of sensitive video data. For extracting the meta data, user can use the same data hiding key used while embedding the data. If requied, the original video can also be obtained by decrypting the video using the same key as used while encrypting

5. RESULT

With this approach, we were successfully able to maintain the privacy of sensitive data. The feature that meta data can be extracted without the need of decrypting the encrypted sensitive video enabled us to achieve the goal. This approach will be very useful in medical field where the sensitive video of operations and also sensitive data must be secured with the access of unauthorized users.

6. CONCLUSION AND FUTURE WORK

Using this approach, it will become possible to maintain privacy of sensitive video data from various sources and reveal only meta data to authorized personnel. It could also be used for hiding nay data within a video stream and extract and view it later by authorized personnel..

Our future work can be to accomplished it on H.246/AVC encoded video stream which would result in better performance as it would avoid leakage from video content which can help address the privacy and security concern. More secure algorithm like IDEA can be used to encrypt the video

7. REFERENCES

[1].Kahn, David,(1980). Cryptology Goes Public, CommunicationsMagazine, IEEE, available from:http://ieeexplore.ieee.org/iel5/35/23736/01090200.pdf?tp=&isnumber=&arnumber=1090200.(Accessed December 28, 2008).

[2]. M. Abomhara, Omar Zakaria, Othman O. Khalifa.. ʻAn Overview of Video Encryption Techniques.ʼInternational Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 20101793-8201

[3]. Saurabh Sharma, Pushpendra Kumar Pateriya2, Lakshmi3.A Study Based on the Video EncryptionTechnique. International Journal of P2P Network Trends and Technology- Volume3Issue1- 2013

[4]. Arup Kumar Bhaumik, Minkyu Choi, Rosslin J.Robles, and Maricel O.Balitanas.'Data Hiding in Video'International Journal of Database Theory and Application Vol. 2, No. 2, June 200

[5].Shashi Mehrotra Seth, Rajan Mishra, Comparative Analysis Of Encryption Algorithms For Data Communication International Journal of Computer Science and Technology.

[6] Yogita Negi, 'A Survey on Video Encryption Techniques'International Journal of Emerging Technology and Advanced EngineeringWebsite: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 4, April 2013)

[7] Adam J. Slagell. Known-Plaintext AttackAgainst a Permutation BaseVideoEncryption Algorithm. Available from http://eprint.iacr.org/2004/011.pdf(Accessed on January 1, 2013).

[8] [10] Shiguo lian, Multimedia Content Encryption: Algorithms and Application, CRC Press, 2008.

[9] Adam J. Slagell. Known-Plaintext Attack Against a Permutation Based VideoEncryption Algorithm. Available from http://eprint.iacr.org/2004/011.pdf (Accessed on January 1, 2013).

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

[11] C. Shi and B. Bhargava, "A Fast MPEG Video Encryption Algorithm," Proceedings of the 6th International Multimedia Conference, Bristol, UK, September 12-16, 1998.

[12] C. Shi, S.-Y. Wang and B. Bhargava, "MPEG Video Encryption in Real-Time Using Secret key Cryptography," 1999 International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'99), Las Vegas, NV, June 28 - July 1, 1999.

[13] T. Seidel, D. Socek, and M. Sramka, "Cryptanalysis of Video Encryption Algorithms ," to appear in Proceedings of The 3rd Central European Conference on Cryptology TATRACRYPT 2003 Bratislava Slovak Republic, 2003