RESEARCH ARTICLE OPEN ACCESS

Design of Perceptual Encryption Algorithm for Video (MPEG)

S.Stephen
Assistant Professor, Dept.of BCA, Immaculate College for Women, Viriyur.

Abstract:

In this project, some existing perceptual encryption algorithms of MPEG videos are reviewed and some problems, especially security defects of two recently proposed MPEG video perceptual encryption schemes, are pointed out. Then, a simpler and more effective design is suggested, which selectively encrypts fixed-length codeword (FLC) in MPEG-video bit streams under the control of three perceptibility factors. In the existing system concept of partial degradation were not been used, but in the proposed system concept of partial degradation has been implemented. The proposed design is actually an encryption configuration that can work with any stream cipher or block cipher. Compared with the previously-proposed schemes, the new design provides more useful features, such as strict size-preservation, on-the-fly encryption and multiple perceptibility, which make it possible to support more applications with different requirements. In addition, four different measures are suggested to provide better security against known/chosen-plaintext attacks.

I. INTRODUCTION

The wide use of digital images and videos in various applications brings serious attention to the security and privacy issues today. Many different encryption algorithms have been proposed in recent years as possible solutions to the protection of digital images and videos, among which MPEG videos attract most attention due to its prominent prevalence in consumer electronic markets In many applications, such as pay-per-view videos, pay-TV and video on demand (VoD), the following feature called “perceptual encryption” is useful. This feature requires that the quality of aural/visual data is only partially degraded by encryption, i.e., the encrypted multimedia data are still partially perceptible after encryption. Such perceptibility makes it possible for potential users to listen/view low-quality versions of the multimedia products before buying them. It is desirable that the aural/visual quality degradation can be continuously controlled by a factor p, which generally denotes a percentage corresponding to the encryption strength. Figure 1 shows a diagrammatic view of perceptual encryption. The encryption key is kept secret (not needed when public-key ciphers are used) but the control factor p can be published. Video Encryption is an extremely useful method for the stopping unwanted interception and viewing of any transmitted video or other information, the scrambling is the easy part. It is the un-encryption that's hard, but there are several techniques that are available. However, the human eye is very good at, spotting distortions in pictures due to poor video decoding or poor choice of video scrambling hardware. Therefore, it is very important to choose the right hardware or else your video transmissions may be un-secure or your decoded video may not be watchable.

II.EXISTING SYSTEM:

In the existing system, concept of video encryption were provided with some security defects .Video encryption is the concept of encrypting the mpeg video file to provide encrypted output .In the existing system ,encryption was made by encrypting the mpeg video file by taking as input .The video file has been encrypted by using some random key values, where the keys cannot be determined by some unauthorized person, even though file has been encrypted by some keys ,no security concepts could be provided for output, since original clarity of video file should not been shown or there should be no chance for the unknown determine Hence these are the main drawback which are available in existing system. So we need a new System in which all the drawbacks of the existing one are to be overcome and the system should support the requirements.To overcome this drawback, concept of partial degradation is used in proposed system.

III.PROPOSED SYSTEM:

Advanced security is provided for entire application. The main drawback of the existing conventional systems involving security defects are solved in the proposed systems. The proposed system is the one which allows us to use or provide security, by partially degrading the video file. In the proposed system following feature called perceptual encryption is used. In many applications like pay-per-view videos, pay TV and video on demand feature called perceptual encryption can be used.

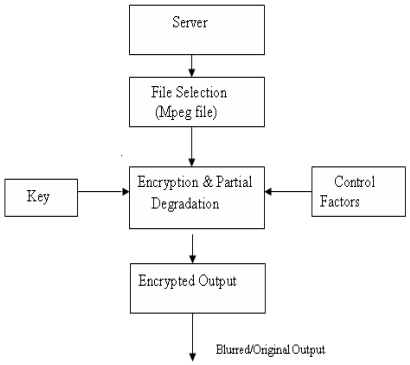
By using this concept video files are first degraded partially and degraded output is encrypted. This feature requires that the quality of aural/visual data is only partially degraded by encryption, i.e., the encrypted multimedia data are still partially perceptible after encryption. Such perceptibility makes it possible for potential users to listen/view low-quality versions. It is desirable that the aural/visual quality degradation can be continuously controlled by a factor p, which generally denotes a percentage corresponding to the encryption strength. The following control factors are Pmr, Psd, and Pmv.

The advantage of this Partial Degradation:

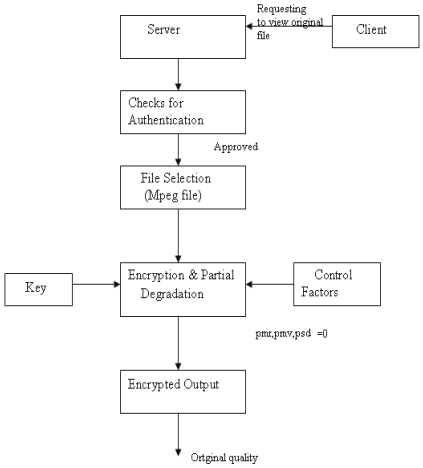
1. It has less complexity and server can easily use this for degrading the video file.
2. It allows the server to change the control factors values, according to which quality of the encrypted output to be displayed.
3. The video file in .mpg format can be easily obtained.

FUNCTIONAL DIAGRAM:-

Functional diagram shows all the functions of the project. The functional diagram representing various functionalities has been drawn.



The above figure 2 represents the basic operation performed during encryption process. Usually the server does a process of first selecting the mpeg file .After the Video file has been selected, it encrypts mpeg file by performing partial degradation by using some random keys and by varying the important control factors. The encrypted output will be of low quality image / original image.



The above figure 3 represents the operations performed, when the customer or a person wants to view a particular file. If a person wants to view a file, server does a process of approval process, which determines whether person is paid member. Once the person is confirmed, server does a process of selecting the file which the person wants to get access. By selecting it performs encryptions and partial degradation on that video file to obtain original quality. Finally by making control factors values as 0's we can obtain pure high quality video file as output.

CIPHER BLOCK CHAINING:-

Cipher block chaining (CBC) is a mode of operation for a block cipher (one in which a sequence of bits are encrypted as a single unit or block with a cipher key applied to the entire block). Cipher block chaining uses what is known as an initialization vector (IV) of a certain length. One of its key characteristics is that it uses a chaining mechanism that causes the decryption of a block of cipher text to depend on all the preceding cipher text blocks. As a result, the entire validity of all preceding blocks is contained in the immediately previous cipher text block. A single bit error in a cipher text block affects the decryption of all subsequent blocks. Rearrangement of the order of the cipher text blocks causes decryption to become corrupted. Basically, in cipher block chaining, each plaintext block is XORed with the immediately previous cipher text block, and then encrypted.

Identical cipher text blocks can only result if the same plaintext block is encrypted using both the same key and the initialization vector, and if the cipher text block order is not changed. It has the advantage over the Electronic Code Book mode in that the XOR'ing process hides plaintext patterns. Ideally, the initialization vector should be different for any two messages encrypted with the same key. Though the initialization vector need not be secret, some applications may find this desirable.

V. CONCLUSIONS

In this project, several techniques and possible methods are discussed for providing security for output videos and creating Blurred / Low quality of an image. It brings a new way to display the video files in a secure manner. The project is highly useful for point-to-point communication to communicate the data in a secured manner. The availability of windows platform makes the project available for a wide range of users. The software is checked with various trial

messages over a network and successful retrieval is obtained which makes this project a successful one.

VI. REFERENCES

[1] Chieh-Jen Cheng, Chao-Ching Wang, Wei-Chun Ku, Tien-Fu Chen , and Jinn-Shyan Wang, "Scalable High-Performance Virus Detection Processor Against a Large Pattern Set for Embedded Network Security" Commun. vol. 51, pp. 62–70,2011.

[2] www.echoecho.com

[3] www.roseindia.net.

[4]http://www5.in.tum.de/forschung/visualisierung.

[5] Perceptual cryptography on PEG2000 compressed images or videos," in *Proc. Int. Conf. Computer and Information Technology.*

[6] Y. Bodo, N. Laurent, and J.-L. Dugelay, "A scrambling method based on disturbance of motion vector,".

[7] AsymmetricKey.ppt.

[8] Cipher Block Chaining http://www.vocal.com.

[9]http://www.webopedia.com/TERM/T/VIDEO ENCRYPTION.html

[10]http://publib.boulder.ibm.com/infocenter/wsphelp/index.jsp?topic=/com.sun.api.doc/java/math/BigInteger.html (For Glossary)

[11]http://java.sun.com/docs/books/tutorial/essential/io/charstreams.html.