International Journal of Engineering Research and General Science Volume 3, Issue 3, Part-2 , May-June, 2015
ISSN 2091-2730

PRIVACY PROTECTION FOR VIDEO, IMAGE, TEXT TRANSMISSION

1. Ms. Shraddha Bhatte ,
Student, Department of Computer Engineering, Shree L. R. Tiwari College of Engineering, Mumbai University, Thane, Maharashtra, 401107, India ,shraddhabhatte@yahoo.com

2. Dr. J. W. Bakal
Principal, Shivajirao S. Jondhale College of Engineering, Mumbai University, Thane, Maharashtra,421204, India ,bakaljw@gmail.com,

3. Mrs.Madhuri Gedam
Assistant Professor, Department of Computer Engineering, Shree L. R. Tiwari College of Engineering, Mumbai University, Thane, Maharashtra, 401107, India

Abstract— The issue of personal privacy is increasingly becoming prominent with the widespread use of large media (video, image, text) transmission systems. While the deployment of media transmission systems is justified by the perception of insecurity due to terrorist threats and high criminality rate, the rightful fear of privacy invasion is turning into a significant concern. In this project, we attempt to reconcile on the one hand the need for media transmission systems and on the other hand the concern of privacy protection.

Keywords—**Privacy protection ,multimedia data,H.264/AVC algorithm ,Compression ,Encryption Scrambling**,**SHA-1.**

INTRODUCTION

Media (Video/Text/Image) transmission systems are becoming ubiquitous. They are widely deployed in many strategic places such as airports, banks, public transportation or busy city centre. While people usually appreciate the sense of increased security brought by media transmission system, they often fear the loss of privacy which comes along.

In this project we are going to focus on three forms on media transmission i.e. VEDIO, IMAGE, and TEXT. A great many algorithms of video encryption have been proposed nowadays with the necessity of data rights management, especially the selective video encryption algorithms, which ensure the security of the information and meanwhile reduce the data to encrypt. The residue data, intra-prediction modes, inter-prediction modes and motion vectors are key elements that are usually partially or completely selected to encrypt to keep the security.

In this project, a new encryption algorithm that encrypts different elements according to different intra-prediction or inter-prediction modes for the H.264 /AVC standard is proposed. This novel algorithm keeps format appliance and has little impact on compression. Most importantly, it has flexible security levels with different applications.

AES/DES is the latest text compression standard which provides a higher compression gain as compared to earlier standards.

MOTIVATION

Multimedia information, such as graphics, images, audio and video, have been widely used in VOD, video conference, video surveillance system and so forth. The wide-spread use of these systems put forward corresponding demands on transmission security and copyright protection of the Multimedia information.

Encoded Multimedia information are often of large quantity, special coding structure, and demand real-time processing. These characteristics bring forward new requirements for encryption systems, namely: security, preservation of Multimedia information format, real time processing, maintenance of compress ratio, and robustness to transmission errors, etc

PROBLEM STATEMENT

Information, such as graphics, images, text and video, have been widely used in VOD, video conference, video surveillance system and so forth. The wide-spread use of these systems put forward corresponding demands on transmission security and copyright protection of the video information**.**

|Information hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorised copying directly.

It is often thought that communications may be secured by encrypting the traffic, but this has rarely been adequate in practice, So the study of communications security includes not just encryption but also traffic security, whose essence lies in hiding information.

In this project, we intend to provide a solution to the problem arising due to loss of privacy as a result of increase in media (video/image/text) surveillance systems. Scrambling can be used to solve this problem.

The scope of H.264 can be explained as, H.264 offers greater flexibility in terms of compression options and transmission support. Similarly and AES/DES offers greater flexibility in terms of compression options and transmission support for text respectively. An encoder can select from a wide variety of compression tools, making it suitable for applications ranging from low-bit rate, low-delay mobile transmission through high definition consumer TV to professional technology production. The standard provides integrated support for transmission or storage, including a pocketsize compressed format and features that help to minimize the effect of transmission errors.

These standards has been adopted for an increasing range of applications, including:

- High Definition DVDs (Blu-Ray)
- High Definition TV broadcasting in Europe
- Apple products including iTunes video downloads, iPod video and MacOS
- NATO and US DoD video applications
- Mobile TV broadcasting
- Many mobile services

EXISTING SYSTEM

The issue of personal privacy is increasingly becoming prominent with the widespread use of large video, image, text transmission systems. While the deployment of video surveillance systems is justified by the perception of insecurity due to terrorist threats and high criminality rate, the rightful fear of privacy invasion is turning into a significant concern.

Previous works addressing the topic of privacy protection have previously reported. The system in [1] is based on an object-based representation of the scene. Basically, an altered rendering of the video is produced where some objects are masked out depending on the user authorizations, preventing the transmission of privacy-sensitive objects.

In [2], wavelet-domain and code stream-domain conditional access control techniques are proposed for JPEG 2000 to scramble code-blocks corresponding to Regions of Interest (ROI) containing for instance people or faces.

In[3] , it is extended to a region-based transform-domain scrambling method applicable to Motion JPEG 2000 or MPEG-4. More

Specifically,[4] AC transform coefficients corresponding to ROI are scrambled by pseudo-randomly inverting their signs, concealing any privacy-sensitive data. Similarly, encryption is used to conceal faces in. A secret encryption key is required in order to invert the process, thus guaranteeing privacy protection.

It is often thought that media transmissions may be secured by encrypting the traffic, but this has rarely been adequate in practice. So the study of communications security includes not just encryption but also traffic security, whose essence lies in hiding information**.**

PROPOSED SYSTEM

Information hiding techniques have recently become important in a number of application areas. It is often thought that communications may be secured by encrypting the traffic, but this has rarely been adequate in practice.

This paper concentrated on methods for hiding messages rather than for enciphering them.

DESIGN FLOW OF PROJECT

The main aim of project is privacy protection of multimedia transmission .here focus is mainly on video, image and text. Security to media (video, image ,text) transmission will give in three layers

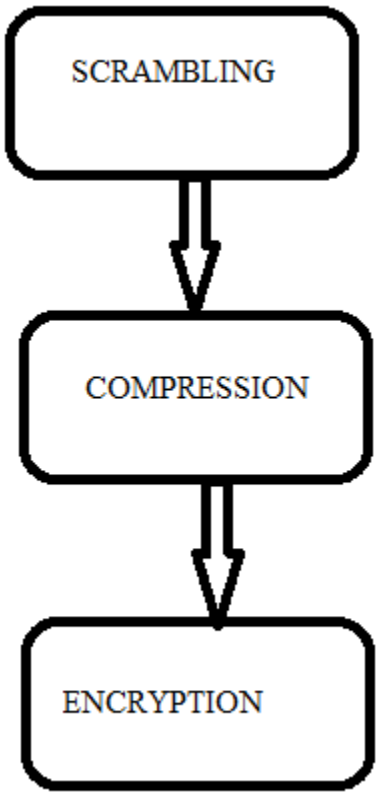

Figure [1] Basic flow diagram of proposed system

Design Details:

According to literature survey most of the existing systems used one layer of protection that is either scrambling or compression otherwise only encryption but as per the recent market need only one layer protection for maintain privacy of the media (video ,image ,text) transfer is not sufficient.

Also it is important to maintain all basic parameters like bandwidth, compression ratio, PSNR ratio, speed of transmission, quality of product after transmission, and total cast of transmission adequate.

In proposed system H.264/AVC algorithm is use for scrambling and compression of video, image.

Encryption is done using SHA-1 and AES/DES algorithms

H.264 algorithm:

H.264 can mean different things from different viewpoints. It is an industry Standard; it defines a format for compressed video data; it provides a set of tools that can be used in a variety of ways to compress and communicate visual information; it is a stage in an evolving series of standardized methods for video compression **[5]**

H.264/AVC standard:

H.264/MPEG-4 AVC is a block-oriented motion-compensation-based video compression standard developed by the ITU-T Video Coding Experts Group (VCEG) together with the ISO/IEC JTC1 Moving Picture Experts Group (MPEG). The project partnership effort is known as the Joint Video Team (JVT). The ITU-T

A valuable content scrambling approach is a raising issue as protecting contents copyright is important. Image and video scrambling is well employed, and its general way is to hide unwanted information and disclose un interpretable image and video. There have been many methods regarding image and video scrambling

The proposed approach scrambles ROI while leaving the background intact, with the resulting scrambled stream still complying with the standard syntax. System use two scrambling approaches. The first one pseudo-randomly inverts the sign of AC transform coefficients of blocks belonging to ROI similarly. The second one applies a pseudo-random permutation of the AC transform coefficients in blocks corresponding to ROI.

Compression:

Compression is the act or process of compacting data into a smaller number of bits. Video compression (video coding) is the process of converting digital video into a format suitable for transmission or storage, whilst typically reducing the number of bits. ‘Raw’ or uncompressed digital video typically requires a large bitrate, approximately 216Mbits for 1 second of uncompressed Standard Definition video.[7]

Compression involves a complementary pair of systems, a compressor (encoder) and a decompressor (decoder). The encoder converts the source data into a compressed form occupying a reduced number of bits, prior to transmission or storage, and the decoder converts the compressed form back into a representation of the original video data. The encoder/decoder pair is often described as a CODEC (enCOder/DECoder)

In H.264/AVC this is carried out by applying a transform to the residual samples and quantizing the results. The transform converts the samples into another domain in which they are represented by transform coefficients. The coefficients are quantized to remove insignificant values, leaving a small number of significant coefficients that provide a more compact representation of the residual frame.

The output of the spatial model is a set of quantized transform coefficients. The parameters of the prediction model, i.e. intra prediction mode(s) or inter prediction mode(s) and motion vectors, and the spatial model, i.e. coefficients, are compressed by the entropy encoder.

Encryption:

Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Both hardware and software implementation are faster still. New encryption standard recommended by NIST to replace DES. Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size . It can be implemented on various platforms especially in small devices. It is carefully tested for many security applications.

SHA1:

SHA1 stands for "Secure Hashing Algorithm". It is a hashing algorithm designed by the United States National Security Agency and published by NIST. It is the improvement upon the original SHA0 and was first published in 1995 [6,10]. SHA1 is currently the most widely used SHA hash function. It is currently used in a wide variety of applications, including TLS, SSL, SSH and PGP SHA1 outputs a 160-bit digest of any sized file or input. It uses a 512 bit block size and has a maximum message size of 2^{64} -1 bits.

The key string which is taken from the user is converted into a hash using SHA-1 algorithm. The first 128 bits of this hash generated is used as our key for AES encryption process.

CONCLUSION

In this paper, we have detailed our motivation for selecting the "Privacy protection for video, image, text transmission" project and literature survey for the same. We have discussed the various algorithms and methods for information hiding, scrambling and compression and AES/DES. On basis of the technical papers that we have studied, it's been concluded that all the proposed algorithms help effectively to protect privacy of data transmission. In fact, combination of those algorithms provides a simplicity and best protection to your end.

ACKNOWLEDGMENTS

I owe a deep gratitude towards my honourable guide, Dr J. W. Bakal. He rendered his valuable guidance with a touch of inspiration and motivation. I would like to thank Prof .Madhuri Gedam, my co-guide who extended every facility and helped me for completing this paper. I would also like to thank my principal, Dr. S. Ram Reddy for his moral support

REFERENCES:

[1] Thomas St¨utz and Andreas Uhl,, "A Survey of H.264 AVC/SVC Encryption', Technical Report,2013

[2]Frederic Dufaux and Touradj Ebrahimi,"Scrambling for privacy protection in video surveillance systems". IEEE Transactions , 2008

[3] Gwanggil Jeon "Block Shuffling Approach for Contents Protection", ' International Journal of Security and Its Applications , 2014

[4] Thomas Wiegand, Gary J. Sullivan, Gisle Bjøntegaard, ,Ajay Luthr, "Overview of the H.264/AVC Video CodingStandard",IEEETRANSACTIONS,2003

[5] "Fabien A.P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn "Information hiding-a survey IEEE , 1999

[6] Qiuhua Wang, Xingjun Wang , "A New Selective Video Encryption Algorithm for the H.264 Standard", **IEEE,2014**

[7] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn . "Information Hiding|A Survey", *IEEE*,1999.

[8] D. Chaum"Untraceable electronic mail, return addresses and digital pseudonyms.",*Communications of the A.C.M.*,1981.

[9] Frederic Dufaux and Touradj Ebrahimi,"H.264/AVC VIDEO SCRAMBLING FOR PRIVACY PROTECTION", IEEE, 2008

[10] A.W. Senior, S. Pankanti, A. Hampapur, L. Brown, Y.-L. Tian, and A Ekin,. "Blinkering Surveillance: Enabling Video Privacy through Computer Vision", IBM, 2003.

[11] F. Dufaux, and T. Ebrahimi "Video Surveillance using JPEG 2000", , SPIE ,2004.

[12] F. Dufaux and T. Ebrahimi , "Scrambling for Video Surveillance with Privacy", IEEE, 2006

[13] T.E. Boult ,"PICO: Privacy through Invertible Cryptographic Obscuration", IEEE, Nov. 2