Secure Multimedia Data using H.264/AVC and AES Algorithm

[1]Deepali P. Chaudhari, [2]Vaibhav Eknath Narawade
[1]Dept. of computer, M.G.M.C.E.T., Kamothe, Navi Mumbai, India
[2]Dept. of Information Technology, P.V.P.P., College of Engineering, Mumbai, India

Abstract
The demand of multimedia information is increasing rapidly. Therefore, multimedia security has become one of the most aspects of communications with the continuous increase in the use of digital data transmission. Many approaches are there to secure multimedia information. In this paper Selective Encryption is proposed along with compression on multimedia information. This paper proposed a new system of video encryption. The proposed system aim Selective Encryption is performed by using the Advanced Encryption Standard (AES) algorithm and Compression is performed using H.264/AVC Standard. The system includes two main functions; first is the encoding/encryption of video stream, through the execution of two processes (the input sequences of video is first compressed by the H.264/AVC encoder, and the encoded bit stream (I-frame) is partially encrypted using AES block cipher). And the second function is the decryption/decoding of the encrypted video through two process (specify the encrypted I-frame stream, decryption of the I-frame, and decoding with H.264/AVC decoder).

Keywords
Encryption/Decryption, H.264/AVC, Video Compression, Advance Encryption Standard (AES)

I. Introduction

With the rapid growth of processing power and network bandwidth, many multimedia applications have emerged in the recent past. As digital data can easily be copied and modified, the concern about its protection and authentication have surfaced. Multimedia data requires either full encryption or selective encryption depending on the application requirements. For example military and law enforcement applications require full encryption. Nevertheless, there is a large spectrum of applications that demands security on a lower level, as for example that ensured by Selective Encryption. Selective Encryption encrypts part of the plaintext and has two main advantages. First, it reduces the computational requirements, since only a part of plaintext is encrypted. Second, encrypted bitstream maintains the essential properties of the original bitstream. Selective Encryption just prevents abuse of the data. In the context of video, it refers to destroying the commercial value of video to a degree which prevents a pleasant viewing experience [1]. Encryption of video and audio multimedia content is not simply the application of established encryption algorithms, such as AES, to its binary sequence. It involves careful analysis to determine and identify the optimal encryption method when dealing with video data [3, 12].

II. H.264/AVC

H.264 is an industry standard for video compression first published in 2003, for the process of converting digital video into a format that takes up less capacity when it is stored or transmitted. It builds on the concepts of earlier standards such as MPEG-2 and MPEG-4 Visual and offers the potential for better compression efficiency (i.e. better-quality compressed video) and greater flexibility in compressing, transmitting and storing video.

Video compression (or video coding) is an essential technology for applications such as digital Television, DVD-Video, mobile TV, videoconferencing and internet video streaming. Standardizing video compression makes it possible for products from different manufacturers (e.g. encoders, decoders and storage media) to inter-operate. An encoder converts video into a compressed format and a decoder converts compressed video back into an uncompressed format.

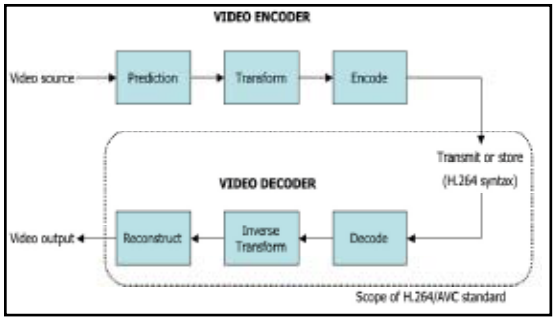

Fig. 1:

As shown in fig.1, H.264 video encoder carries out prediction, transform and encoding processes to produce a compressed H.264 bitstream. An H.264 video decoder carries out the complementary processes of decoding, inverse transform and reconstruction to produce a decoded video sequence.

A. Encoder processes

1. Prediction

The encoder processes a frame of video in units of a Macroblock (16x16 displayed pixels). It forms a prediction of the macroblock based on previously-coded data, either from the current frame (intra prediction) or from other frames that have already been coded and transmitted (inter prediction). The encoder subtracts the prediction from the current macroblock to form a residual.

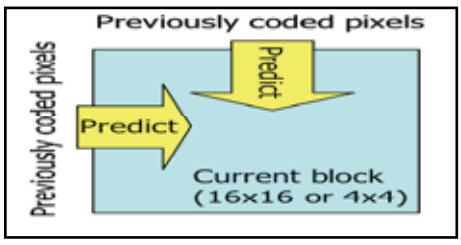

Fig. 2:

The prediction methods supported by H.264 are more flexible than those in previous standards, enabling accurate predictions and hence efficient video compression. Intra prediction uses 16x16 and 4x4 block sizes to predict the macroblock from surrounding, previously-coded pixels within the same frame (fig. 2). Inter prediction uses a range of block sizes (from 16x16 down to 4x4) to predict pixels in the current frame from similar regions in previously-coded frames (fig. 3).

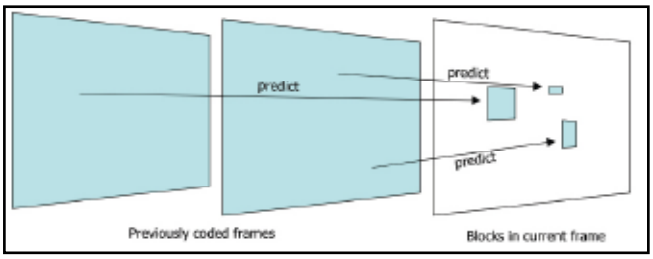

Fig. 3:

2. Transform and quantization

A block of residual samples is transformed using a 4x4 or 8x8 integer transform, an approximate form of the Discrete Cosine Transform (DCT). The transform outputs a set of coefficients, each of which is a weighting value for a standard basis pattern. When combined, the weighted basis patterns re-create the block of residual samples. Fig. 4, shows how the inverse DCT creates an image block by weighting each basis pattern according to a coefficient value and combining the weighted basis patterns. The output of the transform, a block of transform coefficients, is quantized, i.e. each coefficient is divided by an integer value. Quantization reduces the precision of the transform coefficients according to a Quantization Parameter (QP). Typically, the result is a block in which most or all of the coefficients are zero, with a few non-zero coefficients. Setting QP to a high value means that more coefficients are set to zero, resulting in high compression at the expense of poor decoded image quality. Setting QP to a low value means that more non-zero coefficients remain after quantization, resulting in better decoded image quality but lower compression.

3. Bitstream encoding

The video coding process produces a number of values that must be encoded to form the compressed bitstream. These values include:

- Quantized transform coefficients
- Information to enable the decoder to re-create the prediction
- Information about the structure of the compressed data and the compression tools used during encoding
- Information about the complete video sequence.

These values and parameters (syntax elements) are converted into binary codes using variable length coding and/or arithmetic coding. Each of these encoding methods produces an efficient, compact binary representation of the information. The encoded bitstream can then be stored and/or transmitted [2, 4].

B. Selective Encryption

Selective encryption is a technique of encrypting some parts of a compressed data file while send-off others unencrypted. It is a strategy that small fraction of encrypted bits can reason a high ratio of damage to a file. Instead of encrypting the whole file bit by bit, only highly sensitive bits are changed as shown in fig. 4 [11]. Moreover selective encryption reduces required total encryption work and saves system resources as it just encrypts some part of video stream for example The basic selective encryption is based on the H.264/AVC I-frame, P-frame, and B-frame structure. It encrypts the I-frame only because, conceptually P- and B- frame are useless without knowing the corresponding I-frame [7-9]. We propose a technique that selectively encrypts some parts of compressed video file while guarantee the security of the original file. We reduce the time for encrypting video file, but also system complexity. The idea of this scheme is to encrypt different levels of selective parts of H.264/AVC stream by using the feature of H.264/AVC layered structures [3].

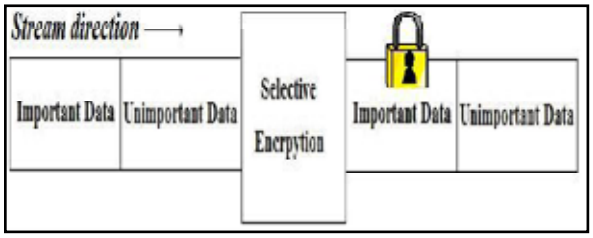

Fig. 4:

1. Advanced Encryption Standard (AES)

In 1997, the NIST called for submissions for a new standard to replace the aging DES. The contest terminated in November 2001with the selection of the Rijndael cryptosystem as the Advanced Encryption Standard (AES). The Rijndael cryptosystem operates on 128-bit blocks, arranged as 4 × 4 matrices with 8-bit entries. The algorithm can use a variable block length and key length. The latest specification allowed any combination of keys lengths of 128, 192, or 256 bits and blocks of length 128, 192, or 256 bits. AES may, as all algorithms, be used in different ways to perform encryption. Different methods are suitable for different situations [10].

2. Strong keys

Encryption with AES is based on a secret key with 128, 192 or 256 bits. But if the key is easy to guess it doesn't matter if AES is secure, so it is as critically vital to use good and strong keys as it is to apply AES properly. Creating good and strong keys is a surprisingly difficult problem and requires careful design when done with a computer. Keys derived into a fixed length suitable for the encryption algorithm from passwords or pass phrases typed by a human will seldom correspond to 128 bits much less 256. To even approach 128- bit equivalence in a pass phrase, at least 10 typical passwords of the kind frequently used in day-to-day work are needed. Weak keys can be somewhat strengthened by special techniques by adding computationally intensive steps which increase the amount of computation necessary to break it.

3. The Round Transformations

There are four transformations:

(i). Add Round Key

Add Round Key is an XOR between the state and the round key. This transformation is its own inverse.

(ii). Sub Bytes

Sub Bytes is a substitution of each byte in the block independent of the position in the state. This is an S-box. It is bisection on all possible byte values and therefore invertible (the inverse S-box can easily be constructed from the S-box). This is the non-linear transformation. The S-box used is proved to be optimal with regards to non-linearity. The S-box is based on arithmetic in GF (2^8).

(iii). Shift Rows

Shift Rows is a cyclic shift of the bytes in the rows in the state and is clearly invertible (by a shift in the opposite direction by the same amount).

(iv). Mix Columns

Each column in the state is considered a polynomial with the byte values as coefficients. The columns are transformed independently by multiplication with a special polynomial c(x). c(x) has an inverse d(x) that is used to reverse the multiplication by c (x) [3, 10].

4. The Rounds

A round transformation is composed of four different transformations as shown in fig. 5. The Round keys are made by expanding the encryption key into an array holding the Round Keys one after another. The Key expansion works on words of four bytes. Each round key is a 4-word (128-bit) array generated as a product of the previous round key, a constant that changes each round, and a series of S-Box lookups for each 32-bit word of the key. The Key schedule Expansion generates a total of Nb (Nr + 1) words. The final round is like a regular round, but without the mix columns transformation [3, 10].

III. Proposed System Overview

Selective encryption is a technique for encrypting only parts of a compressed video stream to reduce computational complexity Selective encryption is not a new idea. It has been proposed in several applications, especially in multimedia system. Selective encryption can be used to reduce the power consumed by the encryption function for digital content. Since particular parts of the bit stream are encrypted, selective encryption can also enable new system functionality such allowing previewing of content. For selective encryption to work, we need to rely on a characteristic of the compression algorithm to concentrate important data relative to the original signal in a relatively small fraction of the compressed bitstream. These important components of the compressed data become candidates for selective encryption. In our selective encryption, an I-Frame bit stream of H.264/AVC, bitstream is encrypted to minimize computational complexity or provide new functionalities for uses of the encrypted bit stream while at the same time providing reasonable security of the bit stream. The block diagram of our proposed selective encryption method for video compressed, using the H.264/AVC video coding method is shown in fig. 6. The input video is first compressed by the H.264/AVC encoder. The output bitstream of the H.264/AVC encoder consists of individual types of data, the video frames (pixels), Intra frame, inter frames, and etc. The encoded bit stream (I-frame) is partially encrypted using AES block cipher with key size of 128 bits, which is XOR-ed with the cipher key to generate the cipher data. Keeping the rest of the data unencrypted because we believe that encrypting I-frame only is more signification. Due to the fact that conceptually P- and B- frame are useless without knowing the corresponding I-frame. In this proposed system, the bits to be encrypted are chosen with respect to the considered video standard to ensure full compatibility, achieved by selecting the bit (I-Frame bitStream) for which each the encrypted configuration modify negligibly the decoding process contexts in sense where their introduction does not create de-synchronization nor lead to non-compliant bitstream. As such, an encryption operation leading to a change of symbol table used in the coding process is not negligible whereas an encryption operation that leads to interpreting a given I-Frame bits. In each case, it is important to note that the bits should maintain this capacity in every coded bitstream, and that it can not be envisaged to consider cases where given configuration of bitstream will allow immediate or delayed resynchronization. The interest to choose carefully the way to encryption is performed is double:

1. Ensures the compatibility with the requirements of the considered video standard.
2. Makes it difficult for cryptanalysis attacks to find an angle to break the encryption key, as it is aimed at making all solutions possible, hence removing possibilities to rule out some cases based on non-respect of standard syntax. Fig. 5, Diagram of the Proposed Selective Encryption Method [3].

IV. The Proposed Scheme Structure

To protect the video streaming information from against theft, alteration or misuse before transmission or storage our system encrypts the output of the H.264/AVC bitstream (I-frame bitstream) by the applied encryption algorithm (AES) which is mentioned early. The block diagram for the operation can be performed as shown in fig. 5.

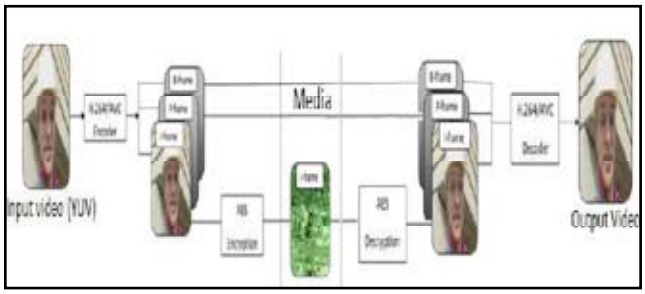

Fig. 5:

V. Conclusion

This paper a proposed system to study video data security by a review and investigation on multimedia security technologies and successful to achievement main above goals, which enhancing the Selective Video Encryption Using Computation between H.264/AVC and AES Encryption Algorithm The requirements for H.264/AVC encryption and decryption are as follow.

1. For the video encryption the encryption considers the security, time efficiency, format compliance and error robustness, basically. The I-Frame encryption being the basis of P-frame and B-Frame in H.264/AVC bit-streams should be more securely protected than the enhancement layers.
2. For the video decryption The quality of decrypted contents has to be degraded than the quality of original contents if the given bit-stream is decrypted with only the layer keys of a lower level than the given bit stream level. Therefore, the proposed encryption system provides the low computational complexity, low bit-overhead, and format compliance in encoding basically. Moreover, it offers the coding efficiency through the selective encryption and the security through the use of same keys as well as the sufficient quality degradation of video content.

References

[1] Z. Shahid, M. Chaumont, W. Puech,"Fast Protection of H.264/AVC by Selective Encryption of CAVLC and CABAC for I & P frames", Journal of IEEE transactions on circuits and systems for video technology.

[2] Iain Richardson,"White Paper: An Overview of H.264 Advanced Video Coding", Vcodex Ltd, 2007.

[3] M. Abomhara, Omar Zakaria, Othman O. Khalifa, A.A Zaidan, B.B. Zaidan,"Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standard", International Journal of Computer Theory and Engg., Vol.2, No. 2 April.

[4] ThomasWiegand, Gary J. Sullivan, Gisle Bjøntegaard, Ajay Luthra, Senior Member, IEEE,"Overview of the H.264/AVC Video Coding Standard", IEEE Transactions on Circuits And Systems for Video Technology, Vol. 13, No. 7, 2003.
[5] Thomas, N., Lefol, D., Bull, D., Redmill, D.,"Transcoding Selectively Encrypted H.264 Bitstreams", International Conference on Consumer Electronics, ICCE07, Digest of Technical Papers, pp. 1- 2, 2007.
[6] O. Nemčie, M. Vranješ, S. Rimac-Drlje,"Comparison of H.264/AVC and MPEG-4 Part 2 Coded Video", 49th International Symposium ELMAR07, pp. 12-14, September 2007, Zadar, Croatia.
[7] Su-Wan park, Sang-Uk shin.,"Efficient Selective Encryption Scheme for the H.264/Scalable Video Coding(SVC)" , Fourth International Conference on Networked Computing and Advanced Information Management,Volume 01, pp. 371-376 , 2008.
[8] Thomas, N., Lefol, D., Bull, D., Redmill, D.,"Transcoding Selectively Encrypted H.264 Bitstreams", International Conference on Consumer Electronics,. ICCE07. Digest of Technical Papers.pp. 1- 2. 2007.
[9] Yuanzhi Zou, Tiejun Huang, Wen Gao, Longshe Huo. Nov,"H.264 video encryption scheme adaptive to DRM", IEEE Transactions on Consumer Electronics, pp. 1289–1297, 2006.
[10] Pravin B. Ghewari, Mrs. Jaymala K. Patil, Amit B. Chougule, "Efficient Hardware Design and Implementation of AES Cryptosystem", International Journal of Engineering Science and Technology Vol. 2(3), 2010.
[11] Deniz Taskin, Cen Taskin, Nursen Sucsuz.,"Selective encryption of compressed video files", International scientific conference, 23-24 Nov 2007, Gabrovo.
[12] Christan Boesgaaed (2003),"A Short Introduction To AES", [Online] Available: http://www.itu.dk/courses/DSK/E2003 DOCS/aes_introduction.pdf

Deepali P. Chaudhari received her B.Tech. degree in Computer Science & Technology from S.N.D.T. University, Mumbai, Maharashtra, India and appeared for M.E. degree in Computer Engineering from Mahatma Gandhi Missions College of Engineering & Technology, Mumbai University, Maharashtra, India. She is working as a Lecturer in Comuter Engineering Department in Shivajirao Jondhale College of Engineering, Mumbai.

Vaibhav E. Narawade has received his B.Tech. degree in Computer Engineering from Dr. Babasaheb Ambedkar Technological University, Maharshtra, India, and M.E. degree in Information Technology from Vivekanand Education Society's Institute of Technology, Mumbai University, Maharashtra, India. He is working as a Associate Professor & Head of Information Technology Department in Padmabhushan Vasantdada Patil Pratisthan's College of Engineering, Mumbai. His research interests are Multimedia, Image processing, Virtual Private Networking, Data Mining & S/w Engineering.