An Improved Selective and Lossless Encryption Algorithm for Real Time Video Transmission

Ruchi Doshi  
Lecturer, Deptt. of Technology  
BlueCrest College, Ghana, West Africa  
doshiruchi18@gmail.com

Kamal Kant Hiran  
Head, Deptt. of Information Technology  
Sikkim Manipal University, Ghana  
kamalhiran@gmail.com

ABSTRACT: Encryption and Decryption of the digital video is very important when it comes to security. As the use digital techniques for transmitting and storing digital videos are increasing; it is becoming an important issue how to protect the confidentiality, integrity and authenticity of videos. Selective encryption is a new trend in video content protection. Selective encryption is a technique to save computational complexity by only encrypting a portion of a compressed bitstream while still achieving adequate security. This new proposed Selective encryption algorithm can encrypt only a subset of the data. The objective of selective encryption is to reduce the amount of data to encrypt while preserving a sufficient level of security. It consists of encrypting only a subset of the data. The proposed selective encryption algorithm in this study has been tested on some videos and showed good results.

Keywords: Selective encryption, decryption, confidentiality, integrity and authenticity.

1. INTRODUCTION
Data security is a necessary part of network transmissions in the world today. Advances in multimedia technologies have popularized applications like video conferencing, pay-per-view, Video- On Demand, video broadcast, etc. In such applications, confidentiality of the video data during transmission is extremely important. Secure transmission of information through insecure communication channels also requires encryption at the sending side and decryption at the receiving side. The main goal of selective encryption is to reduce the amount of data to encrypt while achieving a required level of security. The general approach is to separate the content into two parts. The first part is the public part; it is left unencrypted and made accessible to all users. The second part is the protected part; it is encrypted. Only authorized users have access to protected part. One important feature in selective encryption is to make the protected part as small as possible.

An ideal video encryption algorithm for real-time video applications devices must possess the following characteristics:

[1] Provide an acceptable level of security  
[2] Minimize computational and storage overhead  
[3] Comply with standard video compression formats
2. ENCRYPTION & DECRYPTION

The process of converting plaintext to ciphertext is called encryption; restoring plaintext from ciphertext is called decryption. Both the encryption and decryption algorithms take a key (K) and plaintext/ciphertext as input. Plaintext is a set of pixel values arranged in an orderly manner. Encrypting videos constitutes reordering these pixel values so that they convey no visual information about the original image. An video can also be encrypted in the compressed domain. Encryption is the process of encoding messages or information in such a way that hackers cannot read it, but that authorized parties can. In an encryption scheme, the information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. There are many kinds of video encryption algorithms that can be used depending on the situation that the video is being transmitted in.

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. The process of decoding data that has been encrypted into a secret format. Decryption requires a secret key or password. Decryption is the reverse process of encryption. While encryption is coding the data into a secret format so that others cannot read or access it, decryption is decoding the data back to the original format.

2.1 Basic definitions:

**Plaintext:** This is the original information which a user wishes to transmit to the receiver. Plaintext is fed into the encryption algorithm as input.

**Encryption Algorithm:** It is an algorithm which transforms plaintext using various transforms, to make it unreadable to anyone except those possessing special knowledge about the secret key.

![Encryption and Decryption of a Cipher](image)

**Secret Key:** The secret key is nothing but a collection of bits varying from 1-128 bits. It is also input to the encryption algorithm along with the plaintext. It plays a major role in the encryption because details of the cryptographic algorithm being used are already available with the attacker.

**Ciphertext:** This is the text after the encryption is made on the plaintext. Ciphertext is a stream of data which does not convey any information about the plaintext. For a given message two different keys will produce two different ciphertext.

**Decryption Algorithm:** It is inverse of the encryption algorithm, which takes the ciphertext and secret key as input, and produces original plaintext as output.

**Public and private keys:** These are pair of keys in which one is used for encryption and the other is used for decryption in public key cryptography.

The process of converting plaintext (P) to ciphertext (C) using an algorithm is called enciphering or encryption (E). On the other hand, restoring plaintext from ciphertext is called deciphering or decryption (D). Similarly in the case of images=videos, plaintext is a set of pixel values arranged in an orderly manner. Encrypting images=videos constitutes substituting=transforming these pixel values so that they convey no visual information about the original
image. An image=video can also be encrypted in the compressed domain. In this case, DCT coefficients are encrypted in such a way that the content is made meaningless for the unauthorized user. Only authorized users can decrypt the original content.

2.2 Selective Encryption
Selective encryption reduces required total encryption work and saves system resources as it just encrypts some part of video stream. In traditional video content protection schemes, called fully layered, the whole content is encrypted. Selective encryption is a technique which only encrypts a portion of a compressed bitstream. It consists of encrypting only a subset of the data. Selective encryption is sometimes called partial 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.

![Figure 2] Compression, Encryption of the Video

An important property of the selective encryption is that the encrypted bitstream can be decoded by standard decoders so that both the encrypted and unencrypted portions of the compressed bitstream can be exactly decoded and displayed. With the function of selective encryption, many purposes can be achieved. Input to this process will be ciphertext and with the help of the key it produces the output, which will be the original plain text.

![Figure 3] Selective Encryption Algorithm

Selective encryption can be used to reduce the power consumed by the encryption function for digital content when the content is protected by a digital rights management systems. Selective encryption is a technique to save computational complexity or enable interesting new system functionality by only encrypting a portion of a compressed bitstream while still achieve security.
3. LITERATURE SURVEY

The basic idea of the selective encryption algorithm proposed in [2] is to selectively encrypt I-frames of the MPEG stream; DES on DC coefficients (preferably in CBC mode to avoid dictionary attack) and random permutation on the AC coefficients instead of the standard zigzag. The authors Shi and Bhargava [9], proposed video encryption algorithm (VEA) which uses a secret key to randomly change the signs of all DCT coefficients in an MPEG stream (this is justified by the fact that DCT sign bits are very random, thus neither predictable nor compressible).

The authors Z. Shahid, M. Chaumont and W. Puech, [20], present a new version of VEA reducing computational complexity; it consists in encrypting the sign bits of differential values of DC coefficients of I-frames and sign bits of differential values of motion vectors of B- and P-frames. In [6], a selective bitplane encryption (using AES) is proposed, several experiments were conducted on 8-bit grayscale images, and the main results retained are the following:

(1) Encrypting only the MSB is not secure; a replacement attack is possible [7],
(2) Encrypting the first two MSBs gives hard visual degradation, and
(3) Encrypting three bitplanes gives very hard visual degradation.

Zeng and Lei [11], selective encryption in the frequency domain (8 × 8 DCT and wavelet domains) scheme consists of selective scrambling of coefficients by using different primitives (selective bit scrambling, block shuffling, and/or rotation). A selective encryption algorithm is proposed for JPEG2000 standard [9]. A quality factor controls the strength of the encryption algorithm. The encryption algorithm is performed in a bottom-up order where detail data (high-resolution coefficients) are encrypted first.

<table>
<thead>
<tr>
<th>S. No</th>
<th>Algorithm Name</th>
<th>Security</th>
<th>Size</th>
<th>Speed</th>
<th>Encryption Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Naive</td>
<td>High</td>
<td>No Change</td>
<td>Slow</td>
<td>100%</td>
</tr>
<tr>
<td>2</td>
<td>Selective</td>
<td>Moderate</td>
<td>Increase</td>
<td>Fast</td>
<td>1-100%</td>
</tr>
<tr>
<td>3</td>
<td>Zig-Zag</td>
<td>Very Slow</td>
<td>Big Increase</td>
<td>Very Fast</td>
<td>100%</td>
</tr>
<tr>
<td>4</td>
<td>Video Encryption</td>
<td>High</td>
<td>No Change</td>
<td>Fast</td>
<td>50%</td>
</tr>
<tr>
<td>5</td>
<td>Permutation based</td>
<td>Low</td>
<td>No Change</td>
<td>Super-fast</td>
<td>100%</td>
</tr>
</tbody>
</table>

Table 1. Comparison of different Video Encryption algorithm

The basic approach proposed in [10] is a randomization of the arithmetic coder. This is achieved by randomly swapping the most probable symbol (MSP) and least probable symbol (LSP) intervals. Since only the interval magnitude is important for encoding, the compression performance remains unchanged. Both total and selective encryptions are possible by choosing the layers or resolution levels to encrypt. Selective region encryption is made possible since JPEG2000 is a code block-based algorithm. To encrypt a region of interest, we have to apply the
encryption on the code blocks contributing to precincts of the region considered. In [16], JPEG2000 lightweight encryption scheme is proposed. Only lower resolutions are compressed with classical dyadic wavelet transform. For higher resolutions, the algorithm relies on a secret transform domain constructed with anisotropic wavelet packets (AWPs). The aim of this proposal is to allow transparent encryption for applications requiring low-resolution preview. Therefore, low resolution is accessible by all users and decodable with any JPEG2000 compliant codec. H. Um and E. J. Delp [1]. Video compression algorithms generally address motion compensation and residual error coding. An extension of the quad tree compression algorithm is used to encode both motion vectors and residual errors. Since the residual error is an image frame, partial encryption scheme for quad tree image compression can be directly applied to residual error coding. For low-resolution videos where the maximum height of the tree may be small enough to allow exhaustive tree enumeration, the motion vectors are completely encrypted. The authors Su-Wan Park, Sang-Uk Shin, [17]: The frequency domain scrambling technique divides the transform coefficients into blocks/segments and performs some or all of the following three operations: selective bit scrambling, block shuffling and block rotation of the transform coefficients and motion vectors. Two compression schemes are used to illustrate the approach: wavelet transform based compression and 8x8 DCT based compression. In the simulations, several combinations of the three scrambling operations are tested in the wavelet and DCT domains.

4. PROPOSED VIDEO ENCRYPTION ALGORITHM

The Video Encryption Algorithm has some limitation when it comes to encryption of higher resolution video data. As the proposed algorithm includes both higher resolution video and normal video, this algorithm is more generalized and can be applicable to variety of applications. In this algorithm, we use AES instead of DES for encryption of selected video information. Since AES supports more key length, more security level. In order to reduce the amount of processing overhead and to meet the security for real time video applications, selective encryption techniques have been proposed. The idea of this scheme is to encrypt different levels of selective parts of MPEG stream by using the feature of MPEG layered structures (e.g. encrypting all headers and I frames, encrypting all I frames and all I blocks in P and B frames). The basic selective encryption is based on the MPEG 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. The proposed selective encryption algorithm for video encryption is mentioned below:

Proposed Selective Video Encryption Algorithm:

While (not end of the MPEG video)
{
    Counter =0;

    Case 1: For Intra Frames (I-frame):

    if the counter< threshold_value /*threshold_value should be greater than or equal to 396*/

    if(dct value!=0)
        if(dct value==+1,-1,+2,-2)
            Select at most 128 DC and AC sign bits and encrypt with AES algorithm.
            break;

    Case 2: For Predicted Frames (for a P frame):

    if the counter< threshold_value if(dct value!=0)

        if(dct value==+1,-1,+2,-2)
            select at most 128 DC, AC and motion vectors sign bits and encrypt with AES algorithm.
break;

Case 3: Bi-directional Frames (for a B frame):

if the counter< threshold_value

if(dct value!=0)

if(dct value==+1,-1,+2,-2)

select at most 128 DC, AC and motion vectors sign bits and encrypt with AES algorithm.

break;

Put the encrypted bits to their original positions ;)

/* end function

The new selection algorithm, proposed in this paper, performs better than the RVEA when it encrypts video of higher resolution. RVEA encrypts at most 64 bits (8 bytes) for each macro blocks. Energy concentration of video frame highly relies on the small frequency AC coefficients. So, in our bits selection process we have selected first small AC coefficients for encryption, which degrades the visual quality efficiently.

5. EXPERIMENTAL RESULTS

A good encryption procedure should be robust against all kinds of cryptanalytic and brute force attacks [7]. Here we discuss the security analysis of the proposed video encryption schemes based on statistical analysis such as color histogram, correlation and peak signal to noise ratio (PSNR) etc. It is clear from figure 4 that the histograms of the input video are fairly uniform and significantly different from the respective histogram of the original video. The correlation, mean squared error (MSE) & peak signal-to-noise ratio (PSNR) is the common criterion used to evaluate visual degradation.

5.1 Correlation Coefficient Analysis: We have analyzed the correlation between original and encrypted video. For an ordinary video, pixels are usually highly correlated with its adjacent pixels either in horizontal, vertical or diagonal directions. These high-correlation properties can be quantified as the correlation coefficient for comparison. This correlation coefficient is computed with the help of MATLAB 2D correlation coefficient function which is based on following equation (1). This equation computes the correlation between original and encrypted video of same dimension.

\[
\tau = \frac{\sum_{m,n} (A_{mn} - \overline{A})(B_{mn} - \overline{B})}{\sqrt{\sum_{m,n} (A_{mn} - \overline{A})^2 \sum_{m,n} (B_{mn} - \overline{B})^2}}
\]

Where A and B are the matrices of same size and \( \overline{A} = \text{mean2}(A) \) and \( \overline{B} = \text{mean2}(B) \) ............................................. (1)

5.2 Mean Squared Error (MSE): The mean square error between the two signals is thus defined as: Let X and Y two arrays of size N×M, respectively representing the X-channel frame of reference (i.e. the original copy) and Y-channel frame of the encoded/impaired copy.
The more \( Y \) is similar to \( X \), the more MSE is small. Obviously, the greatest similarity is achieved when MSE equals 0.

5.3 Peak Signal-to-Noise Ratio (PSNR): - PSNR is a very popular quality metric in video processing. The peak signal-to-noise ratio (PSNR) is the ratio between a signal’s maximum power and the power of the signal’s noise. PSNR is defined as

\[
PSNR = 10 \log_{10} \frac{L^2}{MSE}
\]

\( L \) reflects the range of values that a pixel can take: for example, if the \( Y \) channel is encoded with a depth of 8-bit, then \( L = 2^8 - 1 = 255 \). It’s evident from the formula that the result is expressed in decibels. A small mean square error results in a high signal to noise ratio, if MSE tends to zero, then PSNR tends to infinity. Excellent values range from 30 to 50 dB, while an acceptable range in wireless transmission settles around 25dB. It is interesting to note value of PSNR, when MSE is zero or in other words, original and processed signal are same.

In a video sequence quality evaluation you have to measure these indexes for every frame, in order to achieve a collection of measurements that will form a monodimensional array (as long as the number of frames of the clip in study). We also analyzed the histogram between of the videos.

6. APPLICATIONS

- Mobile communication
- Monitoring encrypted content
- Multiple encryptions
- Scalability of encrypted content
- Database search
- Renewable security systems
7. CONCLUSION

This paper focuses on the various methods for video Encryption. From the above analysis, the following conclusions have been drawn: Selective encryption takes less time as compared to full encryption. Our proposed selection encryption algorithm encrypts 128-bits for each time. In the bits selection algorithm, priority is given to lower frequency coefficients.

On the other side, applying the AES encryption enhances the cryptographic security level of the proposed algorithm. Software implementation of this algorithm is also fast enough to meet the real-time requirement of MPEG video. We believe that this framework can be used for secure video-on-demand, peer-to-peer programs. The selection algorithm is more practical enough as per the application requirement. This algorithm includes more frame information for encryption; so security gets enhanced.

8. ACKNOWLEDGMENTS

We would like to thanks the management who constantly inspired to involve in research work and thanks to Governing Council Chairman Dr. Kapil Gupta for cordial cooperation and motivation in our work. The authors would like to thanks Dr. Abhishek Tyagi, Dean Sikkim Manipal University, Ghana Learning Centre and Mr. Gajendra Singh, Director Academics for the constructive feedback and assistance during the course of this research and special thanks to Dr. Mahendra K. Doshi for their guidance and support. We would also like to thank for the valuable information they provided us and our family members for their love and care.

AUTHORS BRIEF PROFILE:

Mrs. Ruchi Doshi is currently working as Lecturer, Department of Technology in the Blue Crest College, Ghana, West Africa. Mrs. Ruchi Doshi has obtained B.Engg. in Computer Science & Engineering from MLS University, Udaipur, India & M.B.A in Major IT and Minor HR from Rajasthan Technical University, Rajasthan, India with first class. She has more than four years of experience in academics as well in Software industry as a Lecturer & Software Engineer. She is also presented & published research papers in International & National conferences. She has been extensively involved in various research activities including supervising summer projects and postgraduate dissertations of final semester students. She is Life member of various professional bodies like International Association of Engineers (IAENG) Universal Association of Computer and Electronics Engineers (UACEE), International Association of Computer Science & Information Technology (IACSIT), Singapore.

Mr. Kamal Kant Hiran is currently working as Head, Department of IT in the Sikkim Manipal University, Ghana, West Africa. He has more than nine years of experience in academia and research. His earlier appointments were at Amity University, Suresh Gyan Vihar University and Govt. Engineering College, Ajmer as an Assistant Professor. He has published numerous research papers and articles in refereed journals and International conferences. Mr. Hiran has obtained M.Tech (Gold Medalist) in Information Communication & Technology from India with Honors and Engineering in Information Technology with first class from University of Rajasthan, India. He is Life member of various professional bodies like Institution of Engg & Technology (IET), London, UK, International Association of Engineers (IAENG), Universal Association of Computer and Electronics Engineers (UACEE), International Association of Computer Science & Information Technology (IACSIT), Singapore. He is Reviewer & member of Editorial Board team in various reputed International Journals like IJSET, IJTEE, IJSTR and IJERT.

His research interests fall broadly within the fields of image processing and computer vision. In particular he is interested in biometric security, face recognition, forensic science, pattern recognition, and medical fields. My first book, on “Mobile Cloud Computing” was published by Lambert Academic Publishing, Germany (ISBN 978-3-659-57391-0), August, 2014. His current projects include Image Clustering, Face Recognition from Video Sequences and Programming & Algorithms in Objective ‘C’ Language.
9. REFERENCES


