Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 2, Issue 13; July-September, 2015 pp. 71-75

http://www.krishisanskriti.org/Publication.html

Video Encryption using Improved AES with DWT.

Manisha Sharma[1] and Kamaljeet Kaur[2]

[1,2]Seth Jai Parkash Mukand Lal Institute of Engineering and Technology (JMIT), Radaur
E-mail: mishusharma06@gmail.com

Abstract—*Today data security over the network is a serious concern as the amount of multimedia data is increasing at an exponential rate due to evolution of internet. To secure multimedia data it is encrypted before transmission. Encryption using improved AES with DWT is quite efficient since it provides the real time encryption of digital multimedia contents. In this paper cryptography is used to encrypt the video data and achieves high security. Video encryption has various fields including internet communication, multimedia systems, medical imaging and military communication. A modified algorithm of Advanced Encryption Standard (AES) algorithm with DWT is proposed here to reduce the computational efforts/ complexity of algorithm which also improve the encryption performance such as speed and PSNR and can be used in real time. The results are compared for the standard metrics such as PSNR, MSE and SSIM and found to be comparable with existing ones with less computational efforts.*

1. INTRODUCTION

Encryption is process of converting ordinary information (called plaintext) in unintelligible text (called cipher text). Encrypted data must be deciphered, or decrypted, before it can be read by the recipient. This process called Decryption. The evolution of internet over the past decades has catalyzed the generation of large quantity of digital multimedia content. The amount of multimedia content available on the internet is increasing at an exponential rate. With the rapid progress in communication technology, popularity of multimedia data has also increased. The progress in multimedia distribution technology has resulted in easy availability of multimedia content to various users over the communication channel .User/customers of the multimedia data are now able to perform real–time audio and video conferencing, listen to music, view streaming video clips etc. They also view film and news on the World Wide Web (www).Since multimedia data are transmitted over open network and more frequently and such as they are highly insecure. These types of networks need to be encrypted before transmission to prevent the opponent from unauthorized users. Typically, reliable security in storage and transmission of digital images and videos is needed in many real applications, such as pay-tv, imaging system, military image database as well as confidential video conferencing [1]. This necessitates secure encryption algorithms for multimedia data protection. The traditional naive encryption methods use conventional AES algorithm. There is a need of improved in an AES algorithm to reduce the time required for encryption because video require more processing time about 1 GB video takes two hours. Improved AES encrypt the confidentially. The encryption techniques should be fast enough and require a small overhead in comparison to traditional AES techniques.

2. RELATED WORK

Over the past few years, encryption has emerged as the leading Alice to solve problems of content authentications for multimedia data (e.g. audio, image and video).With active research in technologies related to network and multimedia, transfer of multimedia data over the network has become very easy, making the security and privacy issues in multimedia computing more and more important. Various encryption algorithms have been proposed in recent years as possible solutions for the protection of multimedia content such as Naïve algorithm, selective algorithm, pure permutation and video encryption algorithm. An efficient MPEG video encryption algorithm[2] used a secret key randomly changing the sign bits of encoded differential values of DC coefficients of I pictures and leave AC coefficients of I frames unchanged and the sign bits of encoded differential vales of motion vectors of B and P frames. This VEA is fast enough to secure video- on- demand, video conferencing and video email and reduced encryption computations. A DCT- based MPEG-2 transparent scrambling algorithm [3] overcome the drawbacks of scrambling in spatial domain by inserted into the MPEG-2 encoding system. The scrambler transforms only the element value in INTRA macro-blocks. The proposed algorithm optimizes the encryption process and improves encryption speed spatial and temporal properties of video retrieval and display process. A lightweight MPEG video encryption [4] using three approaches, which are permutation, XOR template and hybrid at the macro block level. The proposed method achieved security and faster speed which eliminated the use of costly contemporary encryption/decryption algorithm. A chaos based selective encryption scheme [5] has been proposed on the H.264/AVC standard. To mask the selected H.264/AVC

syntax elements four digitized Renyi chaostic maps employed to generate a pseudorandom bit sequence. The proposed algorithm is highly sensitive to the secret key and possesses good perceptual security. The proposed algorithm offers a format compliant, fast and secure selective encryption of H.264/AVC video sequences by destroying their commercial values. A chaos-based image encryption algorithm [8] using differential cryptanalysis on the alternate structure (IEAS) which lead to an effective differential attack on it when the key parameter is even. When it is odd not good enough for image encryption therefore should not be used in applications requiring high-level security. A powerful encryption scheme [13)] as a modification of AES algorithm on Shift Row Transformations step for the video encryption. In the Shift Row Transformation, if value of the first row and the first column is even, then the first and fourth row is unchanged, and each byte in the second and third row of the state is cyclically shifted right over different number, else the first and third row is unchanged, then each byte of the second and fourth row of the state is cyclically shifted left over different number of bytes. This modification allows for greater security and increased performance. An indexed chaotic sequence based selective encryption of compressed video [14] which exploits the characteristics of compressed video which selectively encrypts the compressed Intra coded frames and predictively coded frames from each Group of picture (GOP). This method of encryption is quite efficient since it provides the real time encryption of digital multimedia content and desirable amount of security.

3. ADVANCEDENCRYPTION STANDARD

The AES algorithm is used in some applications that require fast processing such as smart cards, cellular phones and image-video encryption [12]. AES is block cipher with a fixed block size of 128 and a variable key length of 128,192 and 256 bits. The four transformations operate on the a rectangular array of dimensions 4x4 that is called state. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain text into the final output of cipher text. Each round consists of several processing steps, including one that depends on the encryption key.

- Key Expansion using Rijndaell's key schedule
- Initial Round
  1. Add round key
- Rounds
  1. Sub Bytes- every byte in the state is replaced by another one, using the Rijndael's S BOX
  2. Shift rows- Every row of the state is shifted cyclically a certain number of steps.
  3. Mix column- A mixing operation which operates on the columns of the state, combining the four bytes in each column.
  4. Add Round Key- Each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule
- Final Round(no mix-column)
  1. Sub Bytes
  2. Shift Rows
  3. Add round key

After the initial add round key a round function (sub bytes, shift rows, mix column and add round key) is applied to data block. A set of reverse rounds are applied to transform cipher text back into the original plain text using the same encryption key. Based on the above analysis, a simpler design of confidential encryption for YUV videos and attempt to overcome the problems in existing schemes.

4. THE PROPOSED ALGORITHM

A video is a sequence of images. Video contains large space and have spatial redundancies .To overcome we use the transform to decompose the image in difference frame of bands by using DWT wavelet method which extract the motion vector for compression the frames before encryption algorithm are transformed .DWT decompose the frames of video and remove the redundancies. After the decomposition inverse DWT applies

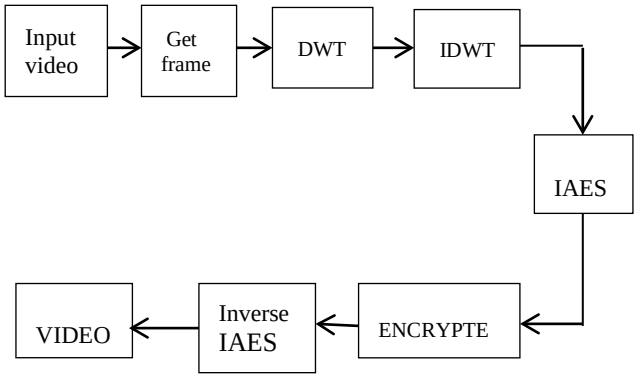


Fig. 1: Proposed algorithm

To overcome the problem of high calculation and computation overhead, analysis of Advanced Encryption Standard (AES) is done and improved it, to improve the encryption standard and speed. In this paper, a new encryption scheme as a modification in shift row, mix column and key expansion of AES algorithm for video encryption is proposed. In the shift row transformation, the Value of the first row and first column note, if it is even then then the first and fourth row is unchanged, and each byte in the second and third row of the state is cyclically shifted right over different number.

A. Step of Modification in shift Row

(i). if the element of first row and first column is even then first and fourth row remain unchanged and each bytes in the

second and third row of the state is cyclically shifted right over different number.

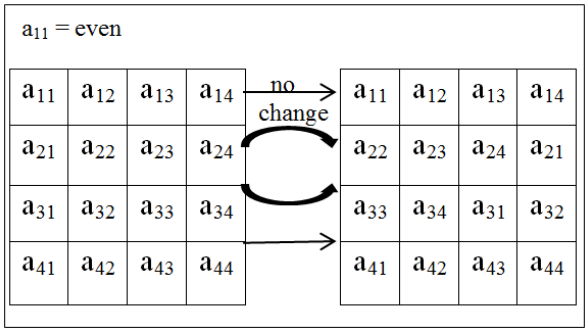


Fig. 2.state [a_{11}] even

(ii) If the element of first row and first column is odd then first and third row remain unchanged and each bytes in the second and fourth row of the state is cyclically shifted right over different number.

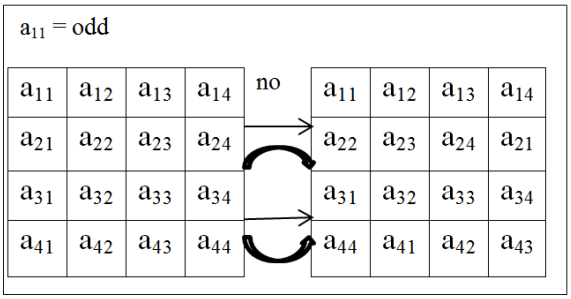


Fig. 2.state [a_{11}] odd

B. step for mix column modification

(i). In the mix column the 128-bit data arranged as a 4 *4 state matrix are operated column by column. The four elements of each column form a four-term polynomial that is multiplied by constant polynomial C(X) ={03}X^3+{01}X^2 +{01}X +{02} with module X^4+1 gets the new state matrix

(ii). In the modification after getting the state matrix from step 1 then interchanging the rows and column of the matrix.

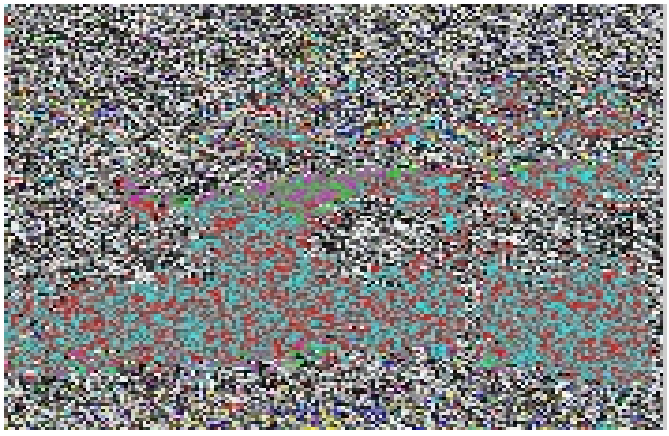
5. EXPERIMENT RESULTS"

In this paper, we are decomposing video prior to the encryption .so we analyzed the quality of decrypted video frame .we also study various performance on the security and speed.

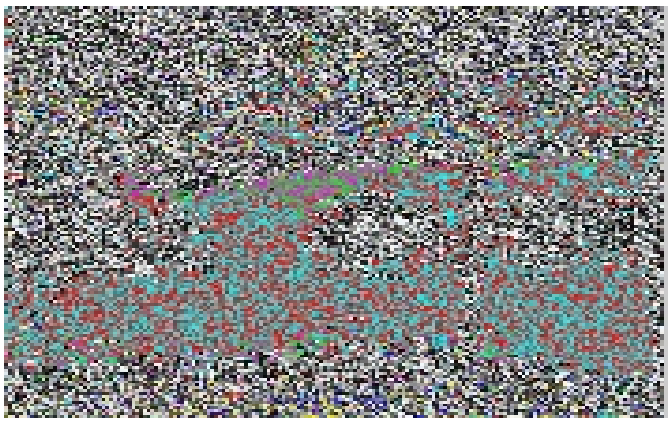
(A) Key Space analysis

In this paper we performed the strength of cryptography algorithm based upon the key spaceanalysis which should be sufficiently large enough to make brute force attack infeasible. In case of brute force attacks, an attacker has to make attempt to try all possible keys whose number is quiet large, to break the cipher[13].The proposed algorithm has a huge key space which is 2^128 possible keys. If an adversary tries to break cipher, since the key space of this algorithm is very high he would have enable to break the cipher.

(a) Original frame of video(container.yuv)



(b)encrypted video frame(compressed) with key



(b) Decrypted video frame with wrong key(1 bit change)

(d) Decrypted video frame with correct key

Fig. 6: (a) Original frame before encryption. (b) Encrypted frame with key. (c) Decrypted frame with wrong key. (d) Decrypted frame with correct key.

(A) Quality Analysis

We analysis the MSE and PSNR and SSIM value to analysis the quality of video .There is a chance of degradation video quality because we used the compression technique before encryption.

(i) Mean square error

MSE is another important evaluation parameter for measuring the quality of compressed image generally used along with the *PSNR* analysis. It compares the original data and reconstructed data and results the level of distortion. The MSE between the original data and the reconstructed data is:

$$MSE = \frac{1}{MN}\sum\sum(A_{i,j} - B_{i,j})^2$$

$A_{i,j}$ is the frame of video before encryption and $B_{i,j}$ is the reconstructed frame after decryption. MSE value should be low. Lower the MSE means minimum error and reconstructed frame is similar to the original frame. In our result we get the MSE value low it means quality of decrypted frame high.

(ii) Peak signal to noise ratio

Peak Signal to Noise Ratio (*PSNR*) has been the most popular tool for the objective quality measurement of the compressed video. The term peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation. PSNR expressed in decibel it calculation is

$$PSNR = 20*\log_{10}(\frac{(255*255)}{sqrt(MSE)})$$

255 is the maximum possible value of the luminance. PSNR high means good quality (the reconstructed frame is similar to original frame) and low means bad quality.

(a) Table for container-qcif.yuv(176*144)

quality	PSNR(db)	MSE	SSIM
50	47.28	1.63	0.98
75	49.34	1.35	0.99
100	49.74	1.27	0.99

(iii) Structural Similarity Index (SSIM)

The Structural similarity (SSIM) index is a method for measuring the similarity between two images (using the structural distortion measurement instead of the error). The SSIM index can be viewed as a quality measure of one of the images being compared provided the other image is regarded as of perfect quality. The value of SSIM is between -1 and 1.Higher the SSIM value good similarity between reconstructed frame and original frame. The SSIM value of our proposed algorithm is about .97.

(C). Speed Analysis

In many video applications, the fast and real time effect is needed. Improved AES provide good speed takes 4.5ms per frame to encrypt the videos hence can be used in real time application compared with other algorithm[14].The speed calculate on processor Intel(R) core i5 ,RAM -4GB and 64-bit operating system.

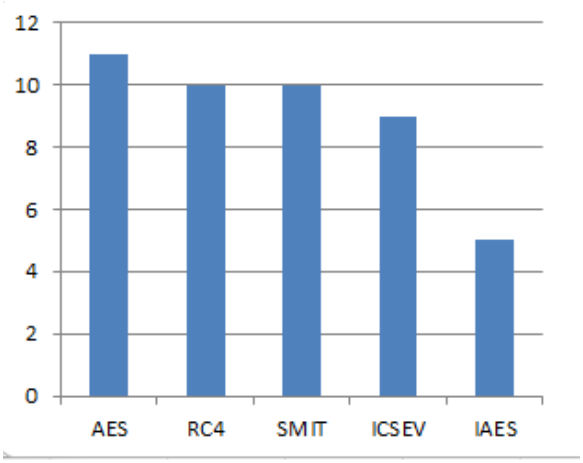


Fig. 7: Speed Analysis

6. CONCLUSION”

This paper, we presented an improved AES with compression domain DWT for video encryption. Using an improved version of AES, an efficient and robust encryption is provided. The improvement is done by modification on Shift Row Transformation step of AES algorithm and modification on mix column transformation. This takes less time to encrypt the video than simple AES so used in real time applications. Performance matrices reveal that proposed work has improved results. In future we will hybrid the security mechanism that will be fuzzy based.

REFERENCE

[1] S Li and others, ‘A General Cryptanalysis of Permutation-Only Multimedia Encryption Algorithms’, *IACR’s Cryptology ePrint Archive: Report*, 2004 .

[2] C Shi and B Bhargava, ‘A Fast {MPEG} Video Encryption Algorithm’, *6th {ACM} Int. Conf. on Multimedia*, 1998, 81–88.

[3] C. Narsimha Raju and others, 'Fast and Secure Real-Time Video Encryption', *Proceedings - 6th Indian Conference on Computer Vision, Graphics and Image Processing, ICVGIP 2008*, 2008, 257–64.

[4] Jie Cui and others, 'An Improved AES S-Box and Its Performance Analysis', *International Journal of Innovative Computing, Information and Control*, 7 (2011), 2291–2302.

[5] Oi-Yan Lui and Kwok-Wo Wong, 'Chaos-Based Selective Encryption for H.264/AVC', *Journal of Systems and Software*, 86 (2013), 3183–92 .

[6] Yuefa Hu and Xingjun Wang, 'A Novel Selective Encryption Algorithm of MPEG-2 Streams', 2012, 2315–18.

[7] D Canright, 'A Very Compact S-Box for AES', *Ches 2005*, 2005, 441–55.

[8] Leo Yu Zhang and others, 'Cryptanalyzing a Chaos-Based Image Encryption Algorithm Using Alternate Structure', *Journal of Systems and Software*, 85 (2012), 2077–85.

[9] Saeed Bahrami and Majid Naderi, 'Encryption of Multimedia Content in Partial Encryption Scheme of DCT Transform Coefficients Using a Lightweight Stream Algorithm', *Optik - International Journal for Light and Electron Optics*, 124 (2013), 3693–3700

[10] Markus Diett, 'On the Security of Digital Video Broadcast Encryption', 2007.

[11] Gp Nason and Bw Silverman, 'The Discrete Wavelet Transform in S', *Journal of Computational and …*, 1994, 6–15 .

[12] Abdulkarim Amer Shtewi and others, 'An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image C.ryptosystems', 10 (2010), 226–32

[13] Modyin Il, 'Modified AES Based Algorithm for MPEG Video Encryption', 1(2010), 1–14.

[14] Saumya Batham, 'ICSECV : An Efficient Approach of Video Encryption', 2014, 0–5.