International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 2, Issue 6 (June 2013), PP. 54-58
www.irjes.com

Partial Video Encryption Using Random Permutation Based on Modification on Dct Based Transformation

S.Rajagopal[1], M.Shenbagavalli[2]
[1]*Assistant professor, National Engineering college*
[2]*PG Student, National Engineering college*

ABSTRACT: *Generally videos are of larger volume. Video encryption is also known as video scrambling. It is one of the powerful techniques for preventing unwanted interception. In this paper a robust Perceptual Video Encryption technique is applied by selecting one out of multiple unitary transforms according to the encryption key generated from random permutation method at the transformation stage.By rotating the phase angle in the DCT based transformation stage of the input residual video frame, anew class of unitary transforms can be generated. Different rotation angle can be choosen which provides number of Unitary Transforms. By alternately applying these transforms based on pre-designed secret key, partial encryption is achived. For the transmission of encrypted video, the encrypted video frames are quantized and encoded. To overcome the drawbacks of Huffman coding, adaptive arithmetic encoder is used at the coding stage. Thus the encrypted bit stream is obtained. Thus the decryption is done to obtain the original video.Also the performance factors under various parameters are analyzed. This methodology will be useful for video-based services over networks.*

I. INTRODUCTION

The wide use of digital images and videos in various applications brings serious attention to security and privacy issues today. Data encryption is a suitable method to protect data. Till now, various encryption algorithms have been proposed and widely used (DES, RSA, IDEA, AES etc.), most of which are used for text and binary data. It is difficult to use them directly in video encryption as video data are often of large volumes and require real time operations. In practical applications, for a video encryption algorithm, security, time efficiency, format compliance and compression friendliness are really important. Among them, security is the basic requirement, which means that the cost of breaking the encryption algorithm is no smaller than the ones buying the video's authorization.

II. ANALYSIS OF VIDEO ENCRYPTION

Siu-Kei Au Yeung et al (IEEE SIGNAL PROCESSING LETTERS, VOL. 16, NO. 10, OCTOBER 2009) proposed that novel video encryption technique is used to achieve partialencryption where an annoying video can still be reconstructed even without the security key. In the existing methods the encryption usually takes place at the entropy-coding stage or the bit-stream level. The proposed scheme embeds the encryption at the *transform* stage during the encoding process. Number of new unitary transforms that are demonstrated to be equally efficient as the well-known DCT and thus used as alternates to DCT during the encoding process. Partial encryption is achieved through alternately applying these transforms to individual blocks according to a pre-designed secret key. The partial video encryption scheme is divided into two parts: 1) random (secret) key generation and 2) alternating transforms according to the secrete key. Almost all video encryption algorithms rely on a random key generator to produce a sequence of pseudo-random codes. To this end, RC4 turns to be the most commonly-used random key generator. The key-stream is then generated using the pseudo-random generation algorithm (PRGA).Analysis on the security level of this partial encryption scheme is carried out against various common attacks such as Known-plain text and chosen-plain text attacks, Ciphertext-only attack. Thus a class of unitary transforms that are generated by some plane-based rotations and explained that these new transforms perform as equally well as or even slightly better than DCT. *The partial* video encryption can be achieved at a low cost is the major advantage. But these results do not offer a high security.

WANG Li-feng et al (The Journal of China Universities of Posts and Telecommunications 2008) proposed that security video communication is a challenging task, especially for wireless video applications. A perceptual video encryption scheme is stated here based on exploiting the special feature of entropy coding in H.264. The encryption scheme is composed of coded block pattern permutation. Experimental results show that the proposed perceptual scheme can achieve high security at a relatively low compression ratio and bandwidth cost, as well as rather low complexity and time cost, so it is suitable for security multimedia services for mobile device and wireless application.

Jolly shah and Dr. Vikas Saxena (IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011) proposed that multimedia data security is becoming important with the continuous increase of digital communications on internet. The encryption algorithms developed to secure text data are not suitable for multimedia application because of the large data size and real time constraint. In this paper, classification and description of various video encryption algorithms are presented. Analysis and Comparison of these algorithms with respect to various parameters like visual degradation, encryption ratio, speed, compression friendliness, format compliance and cryptographic security is presented.

M. Abomhara et al (International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010) proposed that with the rapid development of various multimedia technologies, more and more multimedia data are generated and transmitted in the medical, commercial, and military fields, which may include some sensitive information which should not be accessed by or can only be partially exposed to the general users. Therefore, security and privacy has become an important. Over the last few years several encryption algorithms have applied to secure video transmission. This paper shows the existence of security problems and other weaknesses in most of the proposed multimedia encryption schemes and also description and comparison between encryption methods and representative video algorithms were presented. With respect not only to their encryption speed but also their security level and stream size.

K. John Singh and R.Manimegalai (Journal of Computer Science 2012) proposed that Joint compression and encryption is employed to enable faster and secured transmission of video data. Compression and encryption algorithms can be classified into two main Categories, Independent encryption technique and joint compression and encryption technique. Independent encryption techniques can further be classified as heavy weight and light weight encryption algorithms. There are many algorithms available in the joint compression and encryption technique. Thus found that joint compression and encryption algorithms reduced 40% of the memory storage size and they increased execution speed up to 21%. Joint compression and encryption algorithms perform better in terms of speed and security when compared to independent encryption algorithms. This is because they employ compression before encryption.

III. PROPOSED METHOD

Objective

Compression and encryption are combined together to transmit the video at faster rate and with high security. Generally compression is done before encryption. The main objective is to encrypt the video signal before compression that provides better security rate. Inorder to save the vital datas,the encryption process is done prior to compression.

Problem statement

On sending any video data over the network it consumes more time. This is due to the huge size of the video file when compared to text file. Therefore, video data should be compressed before sending to the destination. Another important factor during data transfer is security, for that the videos must be encrypted before transmission. Video encryption involves different algorithms. Joint compression and encryption is employed to enable faster and secured transmission of video data.

Load Video and Frame Conversion

Video contains more frames, separate image is called a frame, all frames are the same size, mmread function will be used for loading and showing the input video sequence. The loaded video sequence should be converted into frames (i.e still images) using mmreader function.

Unitary Transform

The unitary transform is known as the modified form of DCT. Two dimensional unitary transforms play animportant role in image processing. The term image transform refers to a class of unitary matrices used for representation of images.In analogy with I-D unitary matricsare represented by an orthogonal series of basis functions , similarly an image can be represent in terms of a discrete set of basis arrays called "**basis images**". These are generated by unitary matrices. Alternatively an $(N \times N)$ image can be represented as $(N^2 \times 1)$ vector. An image transform provides a set of coordinates or basis vectors for the vector space.

It is derived from the four-point DCT's flow-graph structure by selecting a different set of rotation angles ($\theta 1 + \delta 1, \theta 2 + \delta 2$) *with* ($\theta 1, \theta 2$) = ($\pi/4, 3\pi/8$).

If the inverse of a square matrix A=[a_1 a_2 .....a_n] (a_i for the ith column vector of $\mathbf{A}$) is equal to its conjugate transpose, i.e., $\mathbf{A}^{-1} = \mathbf{A}^{*T}$, it is a *unitary matrix* and can define a *unitary transform* of a vector: X=[x_1,.....x_n]^T

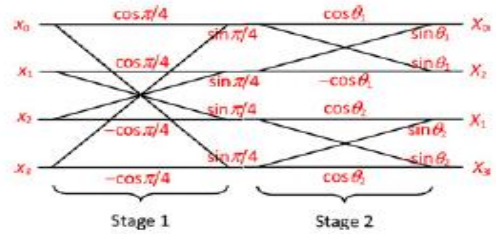


Figure 1 Flow graph of the four-point DCT

Encryption Key Generation by Random Permutation

A random permutation is a permutation containing a fixed number n of a random selection from a given set of elements. There are two main algorithms for constructing random permutations. The first constructs a vector of random real numbers and uses them as keys to records containing the integers 1 to n. The second starts with an arbitrary permutation and then exchanges the ith element with a randomly selected one from the first i elements for i = 1, ..., n.Random Permutation is a method that can generate one permutation of size n out of n! Permutations. This Random permutation is generated from certain key by considering all the elements of this given key in the generation process. The permutation is stored in one-dimensional array of size equal to the permutation size (N).

Taking Inverse DCT and Display Encrypted Video

The inverse discrete cosine transform reconstructs a sequence from its discrete cosine transform (DCT) coefficients. The inverse DCT can be computed by multiplication with the inverse of the DCT matrix. The "twiddle factors" are the complex conjugates of the DCT factors and the reordering is applied at the end rather than the beginning.

Quantization and Encoding for the Generation of Encrypted Bit Stream

Quantization is the process of reducing the number of possible values of a quantity, thereby reducing the number of bits needed to represent it. In video compression, quantization is a process that attempts to determine what information can be discarded safely without a significant loss in visual fidelity. The quantization process is inherently lossy because of the many-to-one mapping process. It reduces the accuracy of the transformer's output in accordance with some pre-established fidelity criterion. Reduces the psychovisual redundancies of the input image. This operation is not reversible and must be omitted if lossless compression is desired. The quantization stage is at the core of any lossy image encoding algorithm. Quantization at the encoder side, means partitioning of the input data range into a smaller set of values. There are two main types of quantizers: scalar quantizers and vector quantizers. A scalar quantizer partitions the domain of input values into a smaller number of intervals. If the output intervals are equally spaced, which is the simplest way to do it, the process is called uniform scalar quantization; otherwise, for reasons usually related to minimization of total distortion, it is called non uniform scalar quantization.

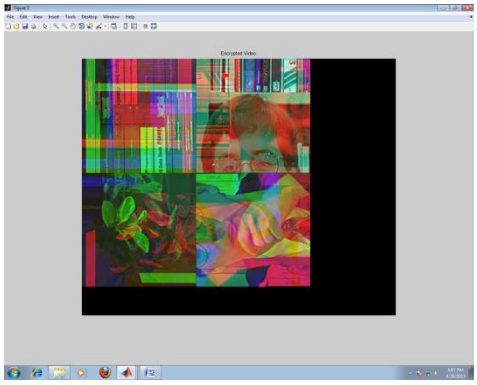
Encoder creates a fixed or variable-length code to represent the quantizer's output and maps the output in accordance with the code. In most cases, a variable-length code is used. An entropy encoder compresses the compressed values obtained by the quantizer to provide more efficient compression. Most important types of entropy encoders used in lossy imagecompression techniques are arithmetic encoder, huffman encoder and run-length encoder.

Arithmetic Encoder

Arithmatic encoder generates the binary arithmetic code corresponding to the sequence of symbols specified in the vector sequence. The input image is encoded and result is a column vector represented in binary format.

Decryption and Reconstruction of original frames

The encrypted frames are then decrypted using the key generated by means of random permutation and by applying the inverse transformation function. Thus the original frames are reconstructed



IV. RESULTS AND DISCUSSION

This section gives the result of the encrypted video using the key generated by random permutation. Also the performance parameters such as MSE & PSNR for each original frame with their encrypted frames are plotted.

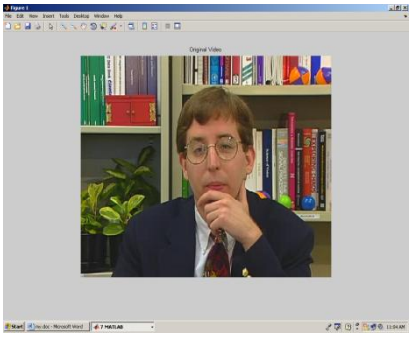


Figure 2 Original video

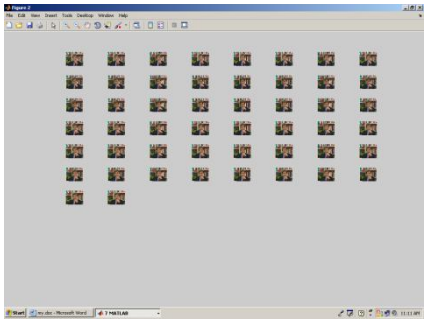


Figure 3 Separation of frames from the video

Here all the frames are seperated from the input video file and stores them in the buffer. The buffer is known as m.cdata in the MatLab. This buffer stores the pixel values of each and every frame separately, which can be used for further process.

Fig 4: Encrypted video

Fig 5: Decrypted video

Fig 6: MSE analysis of the video according to the proposed system

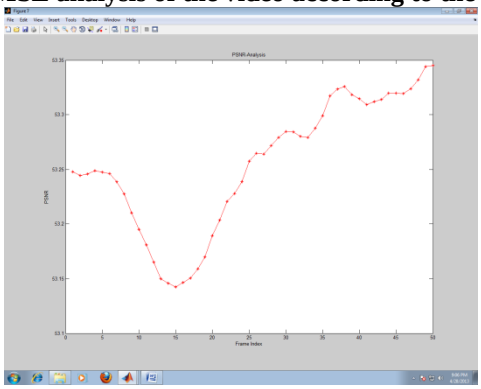
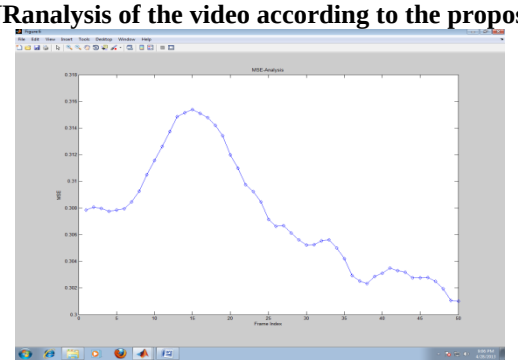


Fig 7: PSNRanalysis of the video according to the proposed system



V. CONCLUSION

Thus the two criteria's such as transmission speed and higher security level are important for the successful transmission of the video. In most of the cases only encryption is done whish ensures the security but the transmission speed is much less. Thus in this paper, joint encryption and compression are applied for the video for high speed secure transmission also their performance is measured by means of parameters such as MSE & PSNR. Hence the result obtained found to be promising.

REFERENCES

[1]. Siu-Kei Au Yeung, Shuyuan Zhu, and Bing Zeng," Design of New Unitary Transforms for Perceptual Video Encryption", IEEE transactions on circuits and systemsfor vide technology, vol. 21, no. 9, september 2011

[2]. S. K. Au Yeung, S. Zhu, and B. Zeng, "Partial video encryption based on alternating transforms," *IEEE Signal Process. Lett.*, vol. 16, no. 10, pp. 893–896, Oct. 2009.

[3]. F. Wang, W. Wang, J. Ma, C. Xiao, and K. Wang, "Perceptual video encryption scheme for mobile application based on H.264," *J. China Univ. Posts Telecommun.*, vol. 15, no. 1, pp. 73–78, Sep. 2008

[4]. J. Zhou, Z. Liang, Y. Chen, and O. Au, "Security analysis of multimedia encryption schemes based on multiple Huffman table," *IEEE Signal Process. Lett.*, vol. 14, no. 3, pp. 201–204, Mar. 2007.

[5]. D. Xie and C. Kuo, "Multimedia encryption with joint randomized entropy coding and rotation in portioned bitstream," *EURASIP J. Inform. Security*, vol. 2007, no. 35262, pp. 1–18, 2007.

[6]. S. Li, G. Chen, A. Cheung, B. Bhargava, and K. Lo, "On the design of perceptual MPEG-video encryption algorithms," *IEEE Trans. Circuit Syst. Video Technol.*, vol. 17, no. 2, pp. 214–223, Feb. 2007.

[7]. Y. Mao and M. Wu, "A joint signal processing and cryptographic approach to multimedia encryption," *IEEE Trans. Image Process.*, vol. 15, no. 7, pp. 2061–2075, Jul. 2006.

[8]. C. Wu and C. Kuo, "Design of integrated multimedia compression and encryption systems," *IEEE Trans. Multimedia*, vol. 7, no. 5, pp. 828– 839, Oct. 2005.

[9]. C. Wang, H. Yu, and M. Zheng, "A DCT-based MPEG-2 transparent scrambling algorithm," *IEEE Trans. Consumer Electron.*, vol. 49, no. 4, pp. 1208–1213, Nov. 2003.

[10]. L. Qiao and K. Nahrstedt, "Comparison of MPEG encryption algorithm," *Int. J. Comput. Graphic*, vol. 22, no. 4, pp. 437–448, 1998