Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MULTIMEDIA ENCRYPTION USING ADVANCED SECURE WAVELET TRANSFORM AND CHAOTIC ARITHMETIC CODING

[1]CHIRANJIT SAHA, [1]YACHNA GUPTA, [1]SAKSHI SACHDEVA, [2]K. JOHN SINGH

[1]Master of Computer Application, School of Information Technology and Engineering,

VIT University, Vellore, Tamil Nadu, India

[2]Assistant Professor (Selection Grade), School of Information Technology and Engineering,

VIT University, Vellore, Tamil Nadu, India

E-mail: [1]chiranjit.saha2012@vit.ac.in , [1] yachna.gupta2012@vit.ac.in,
[1]sakshi.sachdeva2012@vit.ac.in , [2]johnsinghaj@yahoo.com

ABSTRACT

Due to highly increase of enhanced computer and communications between them and also dramatic increase in electronic media, security plays an important role for those organizations where the data is very much critical and important for them. As multimedia is the most popular data shared in the web so it is very much required for the protection over it through an advanced encryption technique so that no one can spoof into it. As now days many internet attackers are there who are very much interested in spoiling the data or stealing the data. It is because the older techniques such as conventional cryptology where a long bit of string are mainly difficult to memorize such a random string. It can easily attacked by using brute force attacked technique. Instead of using traditional cryptology techniques like voice, fingerprint test, retina test etc. it helps to uniquely identify the person and a secure method for stream cipher. Since multimedia data are transferred over open network so more security need to be given to the data .In this paper, we have used the idea of advanced secure wavelet transform and chaotic arithmetic coding . Here we have used the idea of chaotic coding that is the encryption of multimedia files and transmitting over a secured frequency that is the wavelet transform. It enhances the multimedia contents and it should not be compromised. Wavelet transform is a transform in which it is capable of providing the time and frequency information simultaneously, hence providing us a time-frequency representation of the signal. The idea here it gives a new kind of chaotic stream cipher where due to wavelet transmission the data is secured and don't get lost or we can say outsiders cannot view the data unless they know the wavelet transmission frequency and also the encryption arithmetic coding though which it is encrypted . A systematic study on how to strategically integrate different atomic operations to build a multimedia encryption technique. The paper also describes of how to generate an initial key or initial condition from the concept of chaotic arithmetic coding and thus encrypt or decrypt the multimedia data by using this function. The robustness and effectiveness of this new version of scheme is verified by its security strength and also with the comparison with its overall computational cost against the other techniques. The proposed system can guarantee its security and fastness without noticeable increase in encoded image size.

Keywords: *Wavelet Transformation, CKBA, Watermarks, Joint Compression and Encryption, Chaotic Arithmetic Coding, Biometric, Brute Force Attack.*

1. INTRODUCTION

Multimedia image encryption has continued to have a major increasing impact and many key areas of technology including telecommunication, digital television and media, digital and audio, instrumentation, bio- medicine. While standards image and video compression methods exist and that is extensively used nowadays, there is an ever growing demand for better encryption techniques [6]. As in the early 20th century encryption mainly done through mechanically using a pen and a paper. However, due to rapid growth in the era of the computer technology the encryption was required to be fast and efficient. Due to the drift in the age of computers the images like Biometric images, face reorganization images, finger print and retina checking where multimedia security holds a great importance.

Fractals and wavelets provide two different avenues for research. Documents are being digitalized these days to reduce the paper work and to speed the computation of the whole process. As there are some risks of document forgery and the security needs to be given when the document is transmitted over an open network. Traditional cryptography methods like symmetric and asymmetric are restricted to a text only that is these methods cannot be use in case of large multimedia files like image and video. Previously the encryption of JPEG (*Joint Photographic Experts Group*) image file use to take place in such a way that the file is first compressed and then the encryption of the compressed files takes place using advanced encryption standards. For example real time encryption of a multimedia files like images and video using traditional cipher text requires computational overhead, because of huge amount of data involved in transmitting and decrypting. Multimedia images are an array of pixels values which we can think of as a list of numbers. The compression problems consist of two main parts:

- Encoding.
- Decoding.

Encoding attempts to represents the original list of numbers in a different way, hopefully requiring less storage than the original list. If the decoded image is always exactly the same as the original, then the encoding decoding algorithms is said to be a lossless algorithms. If the decoded image differs from the original image, then the algorithm is lossy algorithm. The wavelet methods are lossy algorithms as are most compression algorithm.

Lossy compression cannot be used alone to guarantee a fixed bit rate. If we want to put multimedia data over a modem link for high definition television to a 6 MHz channel, we have to accept that compression process will result in some loss that is we will not get exactly what we put in compression.

In this paper we have proposed a highly powerful scheme which protects the multimedia files from getting changed. Wavelet transformation is a very powerful computational tool used for multimedia applications .This is very useful for compression of image files, small files are useful for saving images occupying less memory thus transmitting more reliably. FBI and NASA used this technique for compressing multimedia files [6]. It is used for cleaning the sound and also reduces the images. There are two different kinds of wavelet, for first type: once the signal has been transformed it is easy to recover original signal whereas for the second type: it's mainly for analyzing the signal. No copy of original signal is required but computation time is more compared to the first type. In chaotic arithmetic coding can be determined by a secret key which keeps on changing [5]. Whereas the compressed multimedia file is protected by another chaotic map .Hence it's a two level protection enforces security thus, resulting in high key context. This work will help us to find a new augmented multimedia control model for encryption and compression with the above ideas and reduces the total computational time.

2. EXISTING SYSTEMS

Instead of using the conventional technique for encryption we can also use some other modern technique that is the Biometric technique for fingerprint, face recognition and others. Using this technique the high resolution image can be easily encrypted and decrypted latter [1]. The main reason for using this technique is that it is everlasting and mostly people use this technique. New researches are also going on to get more compressed and reliable secure file for transmission through open network. Whereas, it also having some disadvantages like biometric specific threats and the privacy risk. In the same way chaos based cryptosystem are utilized to find solutions to the privacy and security problem of biometric data given in [3]. Biometric data are encrypted using chaotic cryptographic scheme hence making them difficult to decipher any attack. Many chaotic multimedia images and videos encryption methods are also proposed which combines the shuttle operations and non linear dynamic chaos system. In the same way many new image methods based on hyper chaos are also proposed that used an image total shuffling matrix to mix the pixel position of plain multimedia data and then states combination are used to change the grey values of shuffled image.

As an essential method of designing a safe video encryption method, secret multiple Huffman Table (MHT) have been given in some design [2]. Some major importance of using this kind of joint compression encryption method is that high compression ratio and encryption can be made possible in a single process, which makes it easy. As this a very time consuming technique which takes additional time to perform the required task .After further studies of security of multimedia encryption scheme on the above algorithm the cryptanalysis has some drawbacks in MHT technique. [7]

In ISCAS 2000 a new chaotic key based algorithm for image encryption was designed. This paper focus that CKBA has weaken the chosen/known plain text attack with only one image and its security to brute force cipher text only attack is over estimated by the authors [5]. This is to say CKBA is not secure at all from cryptographic viewpoint.

Earlier works have been carried out in the same field for the multimedia encryption. A non-linear chaotic algorithm which uses power function and tangent function instead of linear function. It provides large key space and high level security, also keeping acceptable efficiency.

Similar research has been done by Song Zhao, Hengjian Li and Xu Yan for safety and encryption of fingerprint pictures. In their paper they formed a novel chaotic fingerprint images encryption scheme along with shuttle operation and nonlinear dynamic shaos system. The proposed system in this research shows that the image encryption method provides an efficient and safe way for fingerprint image encryption and storage.

Also the research done by Muhammad khurram khan and Jiashu zhang for performing template security in biometric authentication system is relevant to us. In this paper they present a chaos-based cryptosystem to solve the privacy and security related problems in remote biometric authentication for the network. There research shows that the security, performance and accuracy of the system that is presented are useful for the practical implementation in real world.

In the similar way new image encryption technique was given by Tiegang Gao and Zengqiang Chen .There paper was based on image total shuffling matrix to mix the position of image pixel and after that uses a hyper chaotic function to complex the relation between the plain image and cipher image. This encryption technique has the advantage of large key space and high security.

By Sahar Mazloom and Amir Masud Eftekhari-Moghadam, a coupled non liner chaotic map along with novel chaos-based image encryption scheme was used to encrypt the color images .they made use of chaotic cryptography along with a stream cipher structure. A 240 bit secret key was used to generate the initial condition and to enhance the security of the proposed system [7].

From the researches it is estimated that the plain text and chosen plaintext attacks would be very meaningful if same key is used to encrypt more than one plaintext, particularly in the case that a large number of plaintexts are encrypted all with the same key. For a cipher the ability to resist plaintext attack is very important and mostly needed. It is because the key management will be very complex, inconvenient and not efficient in many applications, if any key should be used to encrypt more than one plaintext, then it is not advised to apply CKBA to encrypt MPEG video files [5]. Once a plain-frame in the encrypted MPEG video stream is known for an unauthenticated user, he can easily get all other plain-frames that are the complete video stream.

Multimedia data is transmitted over wide number of networks, so a reliable security is required to protect the multimedia content. Many encryption techniques are specially designed for protecting multimedia applications [6]. Major aim of selective encryption is to lessen encrypted data while we are focusing in security level.

Secret Multiple Huffman Tables (MHT) is used in encrypting some video content explained in [2]. The main advantage of using this technique is that joint compression-encryption is attained simultaneously. It modifies the system design which requires high compression and high degree of encryption ratio thus making it flexible. Hence the required time is reduced for performing encryption. This technique aims at increasing the model space thus maintaining the efficiency of computation [7]. It includes a final bit stream for every multimedia content which has to be compressed. The present scenario shows there are some limitations of this technique.

To improve limitations, a new more effective technique is designed for transmission of multimedia, named OMHT (optimized) [2]. OMHT mainly uses statistics data model based on a set which has data elements that has to be encrypted generating different tables thus increasing efficiency of compression. It is difficult task to work on security as well as bitrates overhead. Compression and encryption of multimedia content degrades security and ratio of compression. OMHT has two parallel paths that are why no addition time is taken. Analysis shows that OMHT provides improved performance over generic encryption and MHT in context of security and multimedia compression [2].

Recent researches are working on algorithms rather than theoretical approach, named as digital watermarks [4] which provides authentication of images and prevent the data of image. We will here discuss purpose and requirement of digital watermarking.

What is the watermarking problem?

Digital watermarking process enforces putting new methods for multimedia content. Watermarking technique comprises of inserting information i.e. applying watermark in image and has a verification algorithm to detect the remaining image under process. Watermark is inserted into the spatial domain of image [4]. There are two types of transforms namely DCT (discrete cosine transform) and the wavelet transform.

It required dealing with image marking for verifying author and securing the content. These are more concerned in detecting threats of the attacks. It is necessary to detect and localize every change in image. Secondly, images are marked in a way that unauthorized copies of images are detected. This is known as robust watermarks. Research aims for invisible watermarks whereas several visible watermarks are available for protection of copy. Invisible watermark are used for exploiting information called as perceptual watermarks. In our vision, transform-based watermarks (DCT, Wavelet) are used. [4]

Image-adaptive (IA) watermarks are methods are used for adjusting the amplitude of the watermark [4]. It protects images from signal processing attacks. Our main focus is on IA-DCT (discrete cosine transform) and IA-W (wavelet). Compression weak watermarks in image so it is needed to maximize strength of watermark during compression. JPEG images use DCT whereas algorithm based on wavelet is called CEZW (Color embedded zero-tree wavelet) compression. IA-W is of much importance and it uses wavelet domain [4]. Visual models are capable of applying more robustness in watermarks. They allow user to change the amplitude of watermarks as per the content of the image. Many useful applications have their focus on source coding or compression. It removes redundancy as well as unimportant information in designing algorithm for optimal compression. Main focus is on frequency sensitivity, luminance sensitivity and contrast masking. We have to find just noticeable difference (JND) for each level of frequencies. This indicates that we can change the given transform coefficient. Similarly, JND's are used to add watermark with greater amplitude in coefficients of transform.

We can even extend the visual model by including the luminance sensitivity. Luminance sensitivity is used to measure and detect the effect of noise. It is an estimation with which we used for visual masking and does not focus on properties of masking because of their high frequency data.

Frequency sensitivity is an adaptive method for utilization of the human visual system properties used for compression of image. It depends only on the viewing conditions [4]. We prefer a dynamic model which allows better quantization. It can be done with contrast masking. Contrast masking is a process which detects the signal in respect of another signal. In order to produce better effect, both the signals should be of same spatial frequency, location and orientation.

The frequency of IA-DCT is based on 8*8 DCT regions. In IA-W, a hierarchical decomposition of threshold frequency sensitivity. It consists of watermark parts which include both local as well as spatial support [4]. Watermark component of local spatial is used for local visual masking effects and global spatial support is used for low pass filtering.

3. ENCRYPTION BASED ON CHAOTIC AND ARITHMATIC CODING

Algorithm for Encryption

Step 1 .Divide the entire multimedia content into grid of 8*8 square matrix.

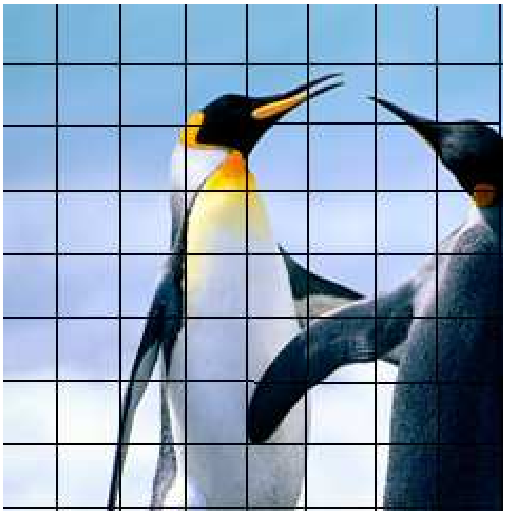

*Fig.1 Dividing Image Into 8*8 Grid.*

Step 2. Now perform the matrix transpose of the pixels of the small squares that are created by the 8*8 grid.

Step 3. Add all the pixel values that lie on the diagonal of the multimedia content and find the modulo of this number with 255 and store this number in a variable 'd'.

Step 4. Now increase the value of each pixel by'd'. And if the number exceeds by 255. Then subtract it by 255 and then increase the pixel value by this number. Do not make any changes in the pixel values that lie on the diagonal.

Step 5. Now finally divide the multimedia content into a grid of 4*4 and again perform transpose on these squares.

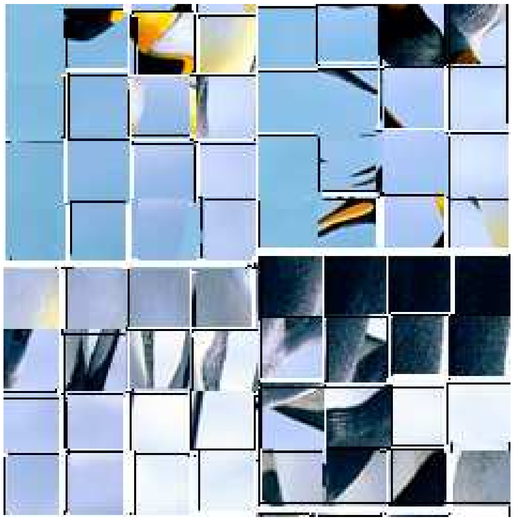

*Fig. 2 Dividing Image Into 4*4 And Performing Transpose Of Each Square.*

Algorithm for Dencryption

Step 1. First divide the image into a grid of 4*4 and again perform transpose on these squares.

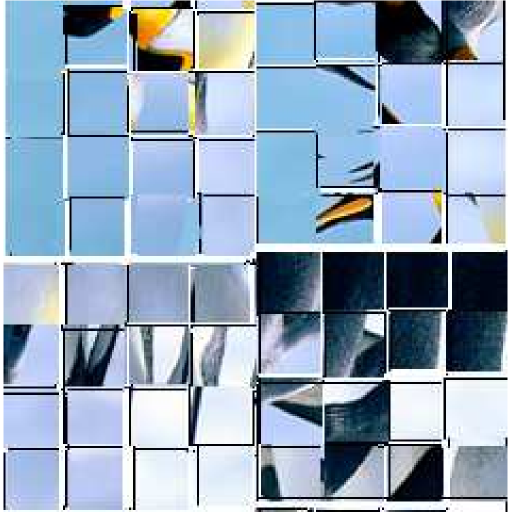

*Fig. 3 Dividing Image Into 4*4 And Performing Transpose Of Each Square.*

Step 2. Add all the pixel values that lie on the diagonal of the multimedia content and find the mod of this number with 255 and store this number in a variable d.

Step 3. If the value of each pixel is less then d then add 255 to the pixel value and then subtract d from it and change the value of pixel to this number (except for diagonal pixels).
Else
Simply subtract the value of 'd' from pixel value (except for diagonal pixels) .

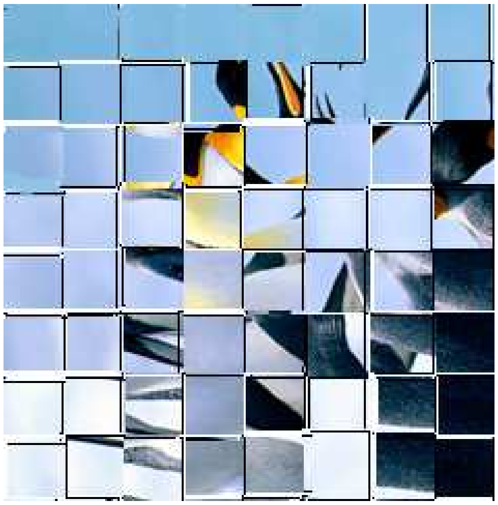

Fig. 4 Input Image For Decryption.

Step 4. Divide the entire image into grid of 8*8 square matrix. Now perform the matrix transpose of the pixels of the small squares that are created by the 8*8 grid.

Disadvantages:

- This algorithm works for only images with square dimension.

Advantages:

- No separate add on such as a key values have to be stored.
- Calculations required for encryption and decryption are very simple.

4. ANALYSIS

Text images consist of grey and color images which provide better performance in compression and encryption using OMHT technique [2]. Analysis of OMHT technique is based on compression ratio (CR), number of bits per symbol (BPP), the mean square error (MSE) and the peak signal of noise ratio. After analyzing the efficiency of MHT [2], KSAC and RAC we found that encryption and compression can be achieved in a one step [7]. The tables as well as order in which they are applied are very much prone to plain text attack. This scheme is less efficient in comparison with the standard approach which uses random bit per input symbol. Encryption technique CKBA is not secure enough to cipher text from theoretical as well as experimental point of view [5]. In order to improve its performance we should provide control parameters as a secret sub-key.

5. CONCLUSION

Non linear chaotic algorithm provides large key space and high level security, and also has acceptable efficiency. The chaotic fingerprint images encryption scheme provides an efficient and safe way for fingerprint image encryption and storage [7]. Chaos-based cryptosystem shows that the security, performance and accuracy of the system that is presented are useful for the practical implementation in real world [5]. Image encryption technique based on image total shuffling matrix has the advantage of large key space and high security [3]. A coupled non liner chaotic map and a novel chaos-based image encryption technique used a 240 bit secret key to generate the initial condition and to enhance the security of the system. The plain text and chosen plaintext attacks would be very meaningful if same key is used to encrypt more than one plain text.MHT scheme is not much effective when we are encoding all images and video types since all images have different data of statistics. Joint compression-encryption OMHT technique is used for attaining good performance of compression and security [2]. OMHT technique results in efficient use of memory storage space and attains a stable peak signal with respect to noise ratio. It does not cause any harm in compression ratio. The cost of encryption occupies only a little of the computation cost of compression. Images cannot be decoded properly as receivers do not know secret code (encrypted code) [1].It is efficient for matching the transform framework of compression techniques with the encryption techniques. Data at lower rates is critical in the matching domains. In IA-W watermarking technique CEZW compression damages less watermarks in comparison to JPEG [4]. IA-W technique is best among all transformation techniques when we are dealing with CEZW compression.

REFRENCES:

[1] R. Bose and S. Pathak, “A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system,” *IEEE Trans. Circuits and Systems I*, vol. 53,no. 4, pp. 848–857, April 2006.

[2] Shaimaa A. El-said , Khalid F.A. Hussian , & Mohamed M.Fouad “*Securing Image Transmission Using In- Compression Encryption Technique International Journal of Computer Science and Security , IJCSS*”, Vol 4, No. 5, pp. 466 – 481.

[3] Abdullah Sharaf Alghamdi , Hanif Ullah “*A Secure Iris Image Ecryprtion Technique Using Bio-Chaotic Algorithm*” .Vol 2, pp. 78 – 84 ,4th April 2010.

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

[5] Shujun Li , Xuan Zheng “*Cryptanalysis of a Chaotic Image Encryption method*”. Vol 2, pp. 708-711.

[6] . C.-P. Wu and C.-C. J. K. Kuo. “*Design of integrated multimedia compression and encryption systems*”. IEEE Transactions in Multimedia, vol. 7, no. 5, pp. 828–839, 2005.

[7]. G. Jakimoski and K.P. Subbalakshmi “*Cryptanalysis of some Multimedia encryption Schemes*” 3rd April 2008, vol 10, pp no 330-334.