A Lossless Digital Encryption System for Multimedia Using Orthogonal Transforms

Dr. Mohammad V. Malakooti [1]
Faculty and Head of Department of Computer Engineering,
Islamic Azad University, Dubai, UAE
malakooti@iau.ae

Mojtaba Raeisi Nejad Dobuneh [2]
Graduate Student of Department of Computer Engineering,
IAU, Dubai, UAE
ghomadian@yahoo.com

Abstract—**In this research work, we have developed a novel lossless digital encryption system for multimedia using the orthogonal transforms for the encryption of all types of image and audio formats. In addition, we have used the symmetric properties of the orthogonal transforms to calculate the inverse of the orthogonal matrices during the execution of the decryption process to speed up the operations and reduce the cost of performance. Several classical image encryption approaches such as Discrete Cosine Transform (DCT), Hadamard Transform (HT) as well as Malakooti Transform (MT), have been proposed and used. We also have proposed, a new Malakooti-Raeisi (MR) Key Gen Algorithm that can be used to encrypt and decrypt the voice signals by applying the XOR operation over the voice signals and Key Gen Sequences. The proposed Key Gen algorithm along with above orthogonal transforms have been used to increase the levels of security as well as the robustness of our algorithm during the image encryption/decryption process. We have encrypted/decrypted voice signals and a few images with only the M-R Key Gen values to show the ability of our algorithm for the encryption/decryption of both voice signals and images with a high accuracy and a reasonable security without using any other transforms. Our algorithm has a wide range of applications such as real time voice transmission, secure voice chat, and secure video encryption.**

Keywords: Cryptography; Image Encryption; Key Generator Algorithm; DCT; Malakooti Transform; HT; Voice Security; Decryption and Symmetric Encryption

I. Introduction

The field of encryption and security is becoming very important in the twenty first century when a massive amount of information is transmitted over the Local Area Networks as well as the Internet. The digital data and images account more than two-third of information that is transmitted over the local area networks and Internet [4]. Thus, a highly reliable and robust encryption algorithm is required when the information is transmitted over the unsecured channels. Data encryption and data embedding are the most important means that can be used to transmit the desired data with a high degree of security and reliability while is passing through the unsecured channels [5]. Encryption is the process of transforming information (plaintext) into a special form called Cipher by using some type of algorithm to make it unreadable to anyone except those who have the knowledge of the Algorithm and its secret keys [3]. Militaries, governments, private companies have used the encryption for a long time to facilitate secret communication. The conventional cryptographic systems mainly have been developed for protecting alphanumeric data rather than the image and audio signals. The encryption of audio signals with traditional encryption required considerable amount of computational power and time. A fast, reliable, and robust algorithm is required to encrypt both image and audio with less computation time and high degree of accuracy.

In the paper, we have developed a lossless digital encryption system for the multimedia using orthogonal transforms that is capable of encrypting any type of image and audio formats into robust encrypted image and audio. In addition, we have used the symmetric properties of the orthogonal transforms to calculate the inverse of the orthogonal matrix during the decryption process to speed up the operations and reduce the cost of performance [10].

Our algorithm is based on the symmetric algorithm along with a newly developed key gen algorithm called Malakooti-Raeisi (M-R) Key Gen Algorithm. The M-R Key Gen Algorithm is a self-generating key algorithm with the faster processing time and better efficiency regarding to the storage space and processing time as compared with the existing ones. The M-R Key Gen algorithm along with one of the orthogonal transform has applied on several different images and the decrypted image and original image compared for the error analysis. The Mean Square Error (MSE) analysis for the orthogonal transforms clearly indicated that DCT error is almost zero, HT error is exactly zero, and the MT error is exactly zero for the transform size of 64 or less but the error approaches to a small non-zero value when the size of transform matrices increase to 128 or higher than that.

We also encrypted the voice signals by applying the XOR operation over the voice signals and the M-R Key Gen values to speed up the operation for the real time and online voice encryption. The imperial results clearly showed that the orthogonal transform operation is not required for the voice signals due to its nature and only the XOR operation of the voice signals with the M-R Key Gen values can destroy the intelligent content of the voice signal and change it to a noisy type of signals.

II. Problem Statement

The challenges of multimedia such as digital images, documents, audio, and video come from two facts that multimedia data size is usually very large and need to be processed in the real time [1]. To obtain a high secure

978-1-4673-0734-5/12/$31.00 ©2012 IEEE

transmission performance when applied to a high bit-rates multimedia data, it requires high processing resources and fast algorithm due to the complexity of computations used in the modern multimedia communications.

DCT has been widely used in various signal-processing applications such as data compression and encryption due to its orthogonal properties [2], [6-7]. The orthogonal transformed-based data encryption techniques have become attractive for many recent communication systems and cryptography due to its fast operations and low cost inverse transform calculation. We proposed a fast and efficient digital encryption method based on the orthogonal transforms DCT, HT, or MT to decrease the process time, increase the levels of security, as well as obtain the high accuracy in the decryption process.

By exploiting the properties of the orthogonal transforms, we have shown that their inverse can be obtained by just taking the transpose of the matrix divided by a constant number. We also used additional steps on the encryption process by performing the XOR operation of the M-R Key Gen values and the transformed image data to increase the levels of security as well as the robustness of our algorithm during the image encryption/decryption process. Once the MT has been used as underlying orthogonal transform the M-R Key values is not required during the XOR operation and first row of the MT can be used as the self-generating secret keys for the encryption. This property makes the MT Encryption and Decryption systems more efficient and robust as compared with the HT, DCT Encryption Decryption systems.

III. Malakooti Transform Algorithm

A new orthogonal transform, the Malakooti Transform (MT), analogous to the Hadamard transform has been developed to represent the multimedia digital contents with a set of coefficients called the M-coefficients. These coefficients contain the useful information about the spectral characteristic of the underlying multimedia digital sequences and can be used for multimedia transmission and compression. Many digital signals are highly redundant; speech, image, and other periodic signals fall into this category. The MT can be applied on any online audio/video signal to represent the desired one with fewer coefficients, resulting in a saving of transmission bandwidth and memory. The MT also can be used as an efficient and robust orthogonal transform for the cryptography and watermarking.

This transform like the Hadamard transform has a complete orthonormal set and has an important role in signal and image processing applications. The elements of the HT are either 1 or –1 while the elements of the MT are usually different than 1 and –1 and can be generated by a recursive algorithm along with two constant parameters to control the elements of MT.

These parameters enable us to generate many MT blocks of different size and different values that can be used for the compression, encryption or watermarking.

The columns of the MT are all perpendicular to each other and can be used to form a vector space so that any vector outside the vector space can be represented as the linear combination of those linearly independent, orthogonal vectors. The orthogonal property of these vectors, columns of MT, makes the MT to be an orthogonal transform that can be used for the encryption and decryption processes with the high speed and little cost for the operations. Because the inverse of orthogonal transform required by decryption process can be obtained easily by dividing each element of the MT, transpose with a constant value formulate by Malakooti Transform Algorithm. For this reason and many others, unitary transforms or an orthonormal transforms should receive more attention that other transforms which have no unitary property.

IV. Generation of Malakooti Transform Matrix

Assume that the value of M_0 in order-0 MT, M_0, is equal to one

$$M_0 = 1 \tag{1}$$

and the order-1 MT matrix, M_1, is formed according to following formula:

$$M_1 = \begin{bmatrix} aM_0 & abM_0 \\ -abM_0 & aM_0 \end{bmatrix} \tag{2}$$

Where a and b are constant parameters.

The matrix M_1 is 2*2 anti-symmetric unitary matrix, because

$$M_1^t M_1 = M_1 M_1^t = cI \tag{3}$$

Where the matrix I is a 2*2 identity matrix and constant parameter c is equal to the determinant of M_1. Thus,

$$c = a^2(1+b^2) \tag{4}$$

Moreover, M_1 inverse is given as:

$$M_1^{-1} = \frac{M_1^t}{c} \tag{5}$$

Similarly, the order-2 MT matrix, M_2 can be obtained according to following formula:

$$M_2 = \begin{bmatrix} aM_1 & abM_1 \\ -abM_1 & aM_1 \end{bmatrix} \tag{6}$$

The matrix M_2 is 4*4 anti-symmetric unitary matrix, because

$$M_2^t M_2 = M_2 M_2^t = c^2 I \tag{7}$$

Where the matrix I is an 4*4 identity matrix, c is given in (4) and the inverse of M_2 is calculated according to following formula:

$$M_2^{-1} = \frac{M_2^t}{c^2} \tag{8}$$

Without loss of generality, the order-k MT matrix, M_k, is 2^k *2^k anti-symmetric unitary matrix, and can be obtained according to following formula:

$$M_k = \begin{bmatrix} aM_{k-1} & abM_{k-1} \\ -abM_{k-1} & aM_{k-1} \end{bmatrix} \tag{9}$$

In addition, M_k inverse is given according to

$$M_k^{-1} = \frac{M_k^t}{c^k} \tag{10}$$

Let us assume that a=1, b=2, to generate the elements of the orthogonal matrices, $M_1$and M_2

$$M_1 = \begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix} \tag{11}$$

$$M_2 = \begin{bmatrix} 1 & 2 & 2 & 4 \\ -2 & 1 & -4 & 2 \\ -2 & -4 & 1 & 2 \\ 4 & -2 & -2 & 1 \end{bmatrix} \tag{12}$$

We can generate any size of MT matrix recursively and use it to encrypt the selected image block by multiplying the MT matrix with the elements of the image block and applying additional XOR operation to increase the levels of security. Moreover, we can obtain the decrypted image accurately and efficiently by multiplying the inverse of MT matrix with the encrypted image using the orthogonal property of MT to perform a low cost calculation for the inverse operation. One can easily see that MT matrix has excellent features that can be used to encrypt the image, voice, and data with low cost and high accuracy, using its orthogonal property. Moreover, the first row MT can be used as the secret key sequences for the XOR operation during the encryption and decryption processes. Thus, we can say that MT is an orthogonal transform with a self-key generating property in which its elements are generated recursively by the MT algorithm and two constant parameters a and b.

V. Malakooti-Raeisi Key Gen Algorithm

In this section, we have discussed about our self-key generating algorithm that has been used along with three orthogonal transforms, Discrete Cosine transform, Hadamard transform, and Malakooti transform. We have used our M-R Key Gen Algorithm along with those orthogonal transforms to obtain a fast, robust, and reliable model for the encryption and decryption of the voice and image. We have shown the advantage of our key gen algorithm compared with those key generating algorithms that have been used to generate random numbers for the encryption process in which required a memory space to retrieve the key information for the encryption process [11].

We also have shown that our self-key generation algorithm has some interesting properties because only three prime numbers are required to generate key sequences of any size for XOR operation of encryption and decryption processes. Most of the key generators algorithm only generates the sequence of pseudo random numbers and are not supported by any structural algorithm in which the generated key values must be sent along with encrypted information for the decryption process [9]. Moreover, our key gen algorithm can be used for the real time voice encryption as well as the secure chat but old key generator procedures can only be used for the off line cryptography.

VI. Image Encryption Algorithm

The procedure for the Image Encryption Algorithm is as following:

1. Read the selected Image from an Image File.
2. Change the Image File into Bitmap.
3. Get the pixel of the Image Bitmap and put them into three matrices, ImgR, ImgG, and ImgB. (Each matrix is for one Color.)
4. Write the elements of the Selected Orthogonal transform (DCT, HT, and MT) into Matrix Format.
5. Divide the original image into smaller blocks of 8*8, 16*16, 32*32, 64*64, or even 128*128.
6. Multiply the selected Orthogonal Transform with each block of image, the same size as Orthogonal Transform, to obtain the encrypted image for that block.
7. Save all encrypted blocks into the matrix format to obtain three encrypted matrices for three different colors (ImgEncR, ImgEncG, and ImgEncB).
8. Combine three encrypted matrices (ImgEncR, ImgEncG, and ImgEncB) to form a single encrypted matrix that represents the encrypted image.

Fig. 1 shows the result of image encryption using the orthogonal transforms DCT, HT, or MT without using M-R Key Gen to compare its robustness with the case that both orthogonal transform and M-R Key Gen are used:

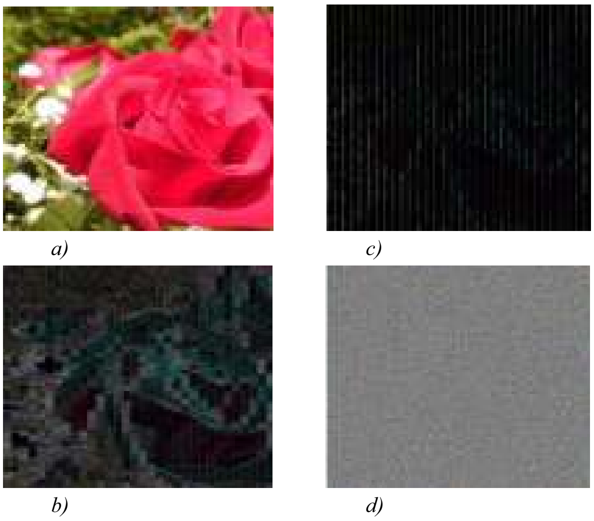


Figure1. a) Original Image, b) Image Encrypted With HT c) Image Encrypted With DCT, d) Image Encrypted With MT

VII. Image Decryption Algorithm

The procedure for the Image Decryption Algorithm is as following:

1. Read the Encrypted Image from a File.
2. Get the pixel of the Encrypted Image Bitmap and put them into three matrices, ImgDecR, ImgDecG, and ImgDecB (Each matrix is for one Color).
3. Write the elements of the selected Orthogonal Transforms (DCT, HT, and MT) into Matrix Format.

4. Divide the encrypted image into smaller blocks of 8*8, 16*16, 32*32, 64*64, or even 128*128.
5. Multiply the Inverse of the Orthogonal Transform with each block of encrypted image, the same size as Orthogonal Transform, to obtain the decrypted image for that block.
6. Save all decrypted blocks into the matrix format to obtain three decrypted matrices for three different colors (ImgDecR, ImgDecG, and ImgDecB).
7. Combine three decrypted matrices (ImgDecR, ImgDecG, and ImgDecB) to form a single decrypted matrix that represents the decrypted image.
8. Calculate the Mean Square Error of the Original Image and Decrypted Image (ideally must be zero).

VIII. Key Generation Algorithm

The MR-Key Gen Algorithm is based on the following steps:

1. Enter two large prime numbers for the values of P and Q, and a constant number for value of M, i.e. 3
2. Multiply two large prime numbers together PQ=P*Q.
3. Initialize the value of index I to 1, I=1.
4. Calculate A (I) = P*Q mod 4096.
5. Calculate B (I) = [P*Q \ 4096]
6. Generate new values for P and Q as following
   6.1 P = [(A (I) + 1) * M]
   6.2 Q = B (I) + I
7. Save the value of A (I) as the secret key value.
8. Return to step 2 to generate next key value.

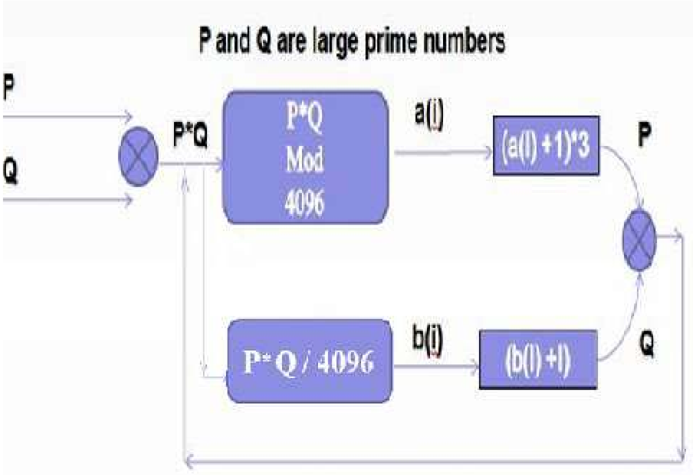


Figure2. Malakooti–Raeisi Key Gen Algorithm Block diagram

The elements of the A (I) array are the key Gen values that can used for the voice encryption/decryption process or the XOR operation of the encryption and decryption processes.

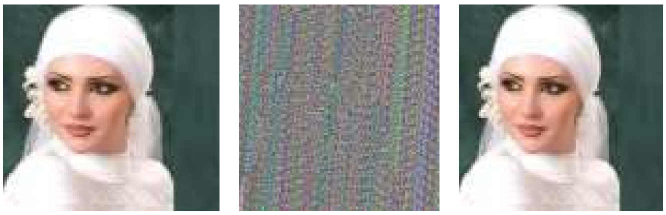
Fig. 5 has depicted the result of XOR operation of the voice selected voice signal with the values of M-R key to obtain a fast and cost effective algorithm for the voice encryption. It has shown clearly that the encrypted image is totally corrupted and unrecognizable from the original one.

We also have combined the M-R Key Gen values with orthogonal transforms to obtain highly secured image as following:

a) Original Image b) Encrypted Image c) Decrypted Image

Figure3. Encrypted and Decrypted of Red Rose using the M-R Key Gen and DCT

We also have encrypted/decrypted a few images with only the M-R Key Gen values to show that our algorithm is able to encrypt and decrypt the image with a high accuracy and reasonable security without using any other transforms.



a) Original Image b) Encrypted Image c) Decrypted Image

Figure4. Encrypted and Decrypted of Original Image using only the M-R Key Gen

IX. Voice Encryption/Decryption Process

The voice signals are highly susceptible to the variation of its sample values and a smaller disturbance can easily change the quality of the voice as well as the voice contents. In this paper, we only have used the M-R key Gen sequence to encrypt the voice signal as opposed to the Image encryption that both orthogonal transforms and XOR operations are used. The M-R Key Gen algorithm can be used to encrypt the voice signals by XOR operation of the voice samples and the Key Gen values rather than using combination of the orthogonal transforms and M-R Key Gen values. The process of the voice decryption operations is similar to the voice encryption ones but the same M-R Key Gen Values must be used to obtain the correct result.

For the encryption of the voice signal, we have skipped the first 44 bytes of the wave files that are considered to be the header information of the voice signals [8]. Then, we have encrypted each byte of the selected voice signal by using XOR operation of M-R Key Gen values with the voice samples. The decryption process of the voice signal can easily be obtained by the XOR operation of the encrypted voice signal with the M-R Key Gen sequences. The result of encrypted and decrypted voice signal has depicted in Fig. 5.

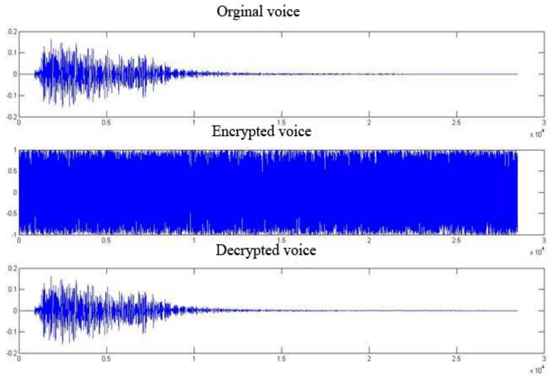


Figure5. Graph of Encrypted/Decrypted Wave File

X. Comparison of DCT, HT, and MT

The Mean Square Error of the encrypted images using DCT were almost close to zero, 5.079 E-9, when the size of the orthogonal transform matrices were 32 or less than 32. The imperial result showed that MSE for DCT block size of 64,128 are almost the same as MSE error of block size 32. Similarly, the MSE of the encrypted images using both MT and HT were exactly zero due to the structure of their transforms, where all elements of the transforms are integer values as oppose to non-integer values for DCT. Once the size of transform block increases to 128 or higher, the MSE of the encrypted images using MT transform has changed from zero to the small nonzero values, 5.749 E-17.

TABLE I. Mean Square Error for DCT, MT, and HT

Transform/ MSE	**N=32**	**N=64**	**N=128**
DCT	5.079 E-9	5.640 E-9	6.249 E-09
MT	0	0	5.749 E-17
HT	0	0	0

XI. Conclusion And Future Directions

In this paper, we purposed a loss less digital encryption model based on the orthogonal transforms for both voice signals and images. Our encryption method is based on the block cipher symmetric encryption in which we used the same key for both encryption and decryption processes. The encrypted signals can be obtained from the multiplication of the orthogonal transform and the multimedia information along with the additional XOR operation with the secret keys to increase the levels of security and robustness. The values of secret keys were obtained from the M-R key generator for DCT and HT transforms but we did not use the values of the M-R key generator for MT and instead we used the values of the first row of the MT to speed up the operation and increase the efficiency.

We have tested our algorithm with several images and three orthogonal transforms DCT, HT, and MT. When the DCT and HT are applied for the encryption process without using the key Gen algorithm, the encrypted images shown some similarity with the original images for the orthogonal transforms of small size 8, 16, and 32. However, when the size of the orthogonal transform is increased to 64 or above the similarity between the original image and encrypted image will be reduced so that no one can recognize the original image from the encrypted one. Moreover, we have shown that the similarity of the original image and encrypted image can be vanished for the small size of the orthogonal transform if the key gen algorithm is used along with the orthogonal transform for the encryption process or the first row of the MT is used as the key values.

More study need to be done to perform the encryption and decryption processes using parallel algorithm or some type of smart algorithm that can benefits the structure of these orthogonal transforms and decrease the required time for the matrix multiplication operations. Moreover, any robust key generator algorithm or algorithm that can use the elements of the transforms matrices as the secret keys can decrease the process time, increase the storage space as well as the levels of securities for the multimedia encryption.

References

[1] R. Rudraraju, B.A, “Digital Data Security Using Encryption”, Master's Paper, University of Texas at San Antonio, 2010.

[2] N. Singh, “Image Compression and Encryption Using Discrete Fractional Cosine Transform”, Deemed University of India, 2004.

[3] U. Sahu, K. S. Dash, “Image Encryption, and Authentication Using Orthogonal Transformation on Residual Number System”, National Institute of Technology of Rourkela, 2008.

[4] S. Changxiang, Z. Huangguo, F. Dengguo, C. Zhenfu & H.Jiwu, “Survey Of Information Security”, Science In China Press 2007.

[5] H. Cheng, X. Li, “Partial Encryption of Compressed Images and Videos”, IEEE Transactions on Signal Processing, Vol. 48 No. 8, August 2000.

[6] A. Cuddy, E. Walden, S. Zalewski, “The Discrete Cosine Transform”, 2001.

[7] S. A. Khayam, “The Discrete Cosine Transform Theory and Application”, Michigan State University, 2003.

[8] M. Brandau, “Implementation of a Real-Time Voice Encryption System”, Master’s Paper University Polytechnic Catalonia, 2008.

[9] N. Ajlouni, A. El Sheikh, A. A. Rasheda, “New Approach in Key Generation and Expansion in Rijndael Algorithm”, the International Arab Journal Information Technology, Vol. 3, No. 1, 2006.

[10] P. Kotzanilolaou, C. Douligeris, ”Network Security: Current Status and Future Directions”, pp.459-480, 2007.

[11] M. Raeisi, ” Developing a Loss less Digital Encryption System for Multimedia using Orthogonal Transforms”, Master Thesis, March 2011, Department of Computer Engineering, Islamic Azad University, UAE branch.

978-1-4673-0734-5/12/$31.00 ©2012 IEEE