Enhancing Security with the Combination of DCT & 3DES

Theint Theint Ei Htet Aung[1], Dr. Nilar Thein[2]
University of computer studies, Yangon, Myanmar.
theinttheinteihtetaung@gmail.com, cocoon.theint@gmail.com

Abstract

Information security is becoming more important in data storage and transmission. Because of widely used images in security process, it is the important confidential image data from unauthorized access. The original image was converted by using two dimensional transform and encryption 3DES with two keys. This system presented a transformation algorithm based on the image cosine transformation and a well known encryption and decryption algorithm called 3DES. This paper also analyzed the image encryption algorithms DCT and 3DES. The original image is encrypted after the transformation process. In this approach to reduce the computational requirements for huge volume of images and resulting high speed transformation and encryption system.

Keywords_ Image preprocessing, Image processing, 3DES, DCT and transmission.

1. Introduction

Nowadays many people are using the internet, so online based business growing and information transmission security are becoming more important in data storage. Encryption is used to securely transmit data in open network. Image encryption has applications in internet communication, multimedia systems, medical imaging, military communication, etc. Therefore, to protect the image data from counterfeiting, unauthorized access and danger or loss.

Image encryption plays a significant role in the field of information hiding. Image hided or encrypting methods and algorithms range from simple spatial domain methods to more complicated and reliable frequency domain. Images are different from text. So, the traditional cryptosystems to encrypt important images directly is not a good idea. The image size is almost much greater than of text.

In this paper, the Discrete Cosine Transform is the core transform of many image processing applications for reduced bandwidth image. Transformation relies on the premise that pixels in an image exhibit a certain level of correlation with their neighbor pixels. The transformation process will be used to divide the original image into a number of blocks (8x8) blocks. The transformation image is into the 3DES encryption with two keys.

The structure of this paper is as follow: section 1 introduction to the system. Section 2 describes system implementation. Section 3 explains the symmetric cipher. Section 4 explains the Data Encryption Standard. Section 5 explains about the Discrete Cosine Transform. Section 6 describes experiment and test result. Section 7 describes conclusion.

2. System Implementation

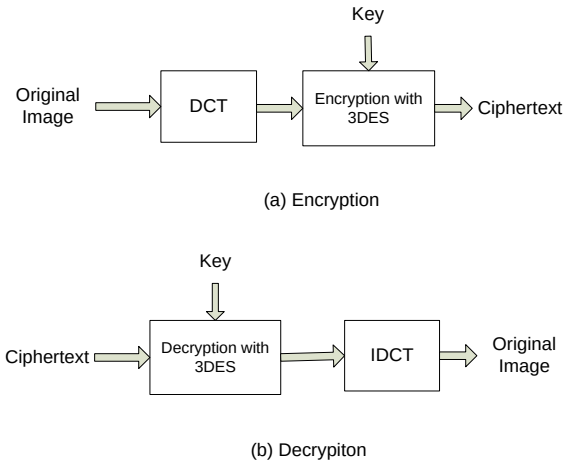

Figure 1.System Design

In this paper implementation of image encryption using DCT transformation algorithm, 3DES encryption and decryption algorithm. DCT based codes use a two-dimensional version of the transform. The 2D-DCT and its inverse (IDCT) of an NxN block. Most of the image compression used DCT transformation. 3DES take 112 bits key length for more secure. DES data are encrypted in 64 bits blocks using a 56 bits key and 8 bits are used for parity. The round key generator creates sixteen 48 bits key out of 56 bits cipher key. The encryption private key that encrypts and decrypts data are 64 bits blocks. The image encryption consists of input image to transform with DCT and encrypt with

3DES with key and output text is save in database server with key. The decryption consists of input encryption text to get from the database with key, decryption the text with key and inverse transform to image. Compare to choose the image in data storage with the inverse transform image. If same image show the original image, else shows image are not same text box alert.

3. Discrete Cosine Transform

The Discrete Cosine Transform is the core transform of many image processing applications for reduced bandwidth image [4]. The DCT is a mathematical transformation that takes a signal and transforms it from spatial domain into frequency domain [5]. A fast version of the DCT is available, like the FFT, and calculation can be based on the FFT. Both implement about same speed. Transform coding relies on the premise that pixels in an image exhibit a certain level of correlation with their neighbor pixels. Many digital image and video compression use a block based DCT, because this algorithm minimizes the amount of data needed to recreate a digitized image [5-6]. The computation of a two dimensional discrete cosine transform, based on the row-column decomposition is presented. The 2D-DCT processor design has been concentrated on small non-overlapping blocks (typical 8x8 or 16x16). Many 2D DCT algorithms have been proposed to achieve reduction of computational complexity and thus increase the operational speed and throughput [1]. The output array of DCT coefficients contains integer, these can range from -1024 to 1023. It is computationally easier to implement and more efficient to regard the DCT as a set of basic functions.

2D-DCT:

$$F(u,v) = \frac{2}{N} C(u)C(v) \sum_{n=0}^{N-1} \sum_{n=0}^{N-1} f(x,y) \cos\left[\frac{(2x+1)u\pi}{2N}\right] \cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad (1)$$

2D-IDCT:

$$f(x,y) = \frac{2}{N} \sum_{n=0}^{N-1} \sum_{n=0}^{N-1} C(u)C(v)F(u,v) \cos\left[\frac{(2x+1)u\pi}{2N}\right] \cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad (2)$$

N = size of the block that the DCT is done on.
u , v = 0,1,2,……,N-1

The 2-D basis functions can be generated by multiplying the horizontally oriented 1-D basis functions with vertically oriented set of the same functions. DCT formula is called the analysis formula or the forward transform, while inverse discrete cosine transform is the synthesis formula or inverse transform [3].

4. Symmetric Cipher

Symmetric encryption is a cryptosystem in which encryption and decryption are performed using the same key. It is also known as conventional encryption. Encryption transforms plaintext into ciphertext using a secret key and an encryption algorithm. Using the same key and a decryption algorithm, the plaintext is recovered from the ciphertext.

5. Data Encryption Standard (DES)

DES is a symmetric block cipher. Data Encryption Standard (DES) has been developed as a cryptographic standard for general use by the public. DES design was high level of security, efficient of high data rate, complete specified and easy to understand. The DES function applies a 48-bit key to the rightmost 32-bit to produce a 32-bit output.

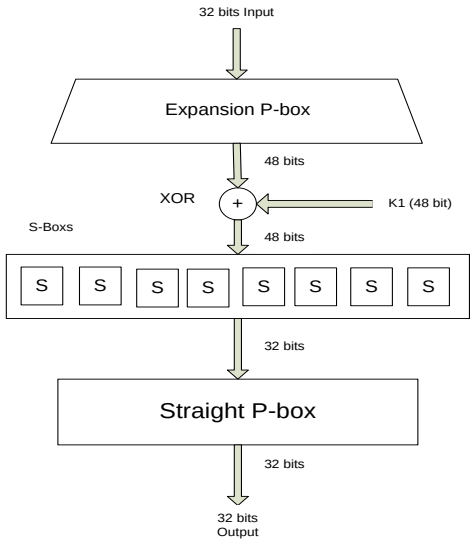

Figure 2.DES function

Double DES encryption algorithm that encrypts and decrypts data are 64 bits. 2DES encryption algorithm has two encryption stages and two keys. Double DES uses in effect, a 112 bits key. The encryption algorithm is follows:

$$C = E(K2, E(K1, P)) \quad (3)$$

$$P = D(K1, D(K2, C)) \quad (4)$$

P is a plaintext, C is a ciphertext, (K1, K2) are encryption two keys.

5.1. Triple DES with Two Keys

3DES is a symmetric block cipher algorithm the encryption private key that encrypts and decrypts data are 64 bits blocks [2]. The DES algorithm is only 56 bits strong because 8 extra bits are the parity

bits are dropped before the actual key-generation process. The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The encryption itself is based on XOR operation and most notably on lookup-tables, called S-boxes [2]. Can use triple DES with two keys (112 bits) or triple DES with three keys (168 bits).

In triple DES with two keys the total keys length is 112 bits, the encryption algorithm is follows:

$$C = E(K1, D(K2, E(K1, P))) \quad (5)$$

$$P = D(K1, E(K2, D(K1, C))) \quad (6)$$

P is a plaintext, C is a ciphertext, (K1, K2) are encryption two keys.

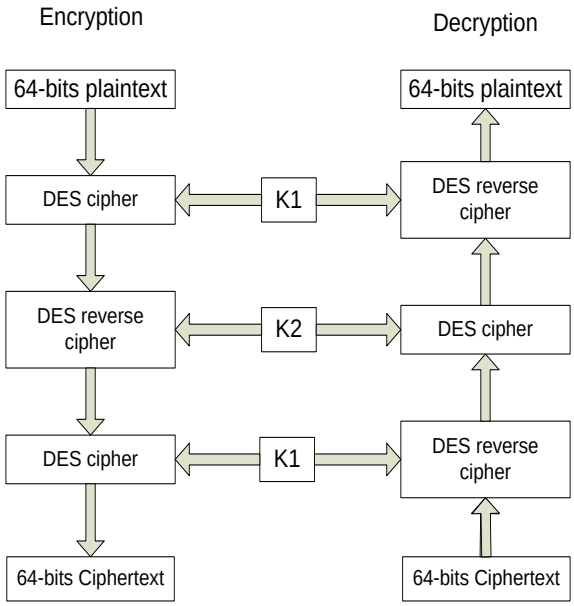

Figure 3.Triples DES with two keys

6. Experiment Result

To prove the performance of the proposed encryption method, a system has built to implement the proposed algorithm. This section shows the implementation and the result of the purposed method. Figure 4 is a (300x300) pixels input image. Figure 5 shows a (300x300) pixels transformation image and Figure 6 shows a decrypt image resulted from the system. Figure 9 shows a (1000x1000) pixels input image, and Figure 10 shows a (1000x1000) pixels transformation image. The image size is (100x100) pixel is very small and image size is 10.5 kB. The image size is the (300x300) is suitable because of image size is 93.4 kB, if the (1000x1000) pixel is very extract the image and image size is 966 kB. In (500x500) pixel image size is 265 kB. In (600x600) pixel image size is 380 kB. If the image pixel size is larger, the transformation has many delay time and size is larger.

Figure 4.(300x300) pixels Original image

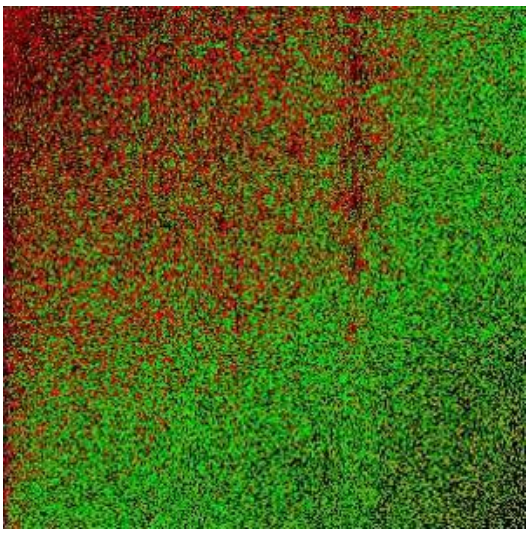

Figure 5.(300x300) pixels Transformation

Figure 6.(300x300) pixels Decryption

Figure 7.(500x500) pixels image

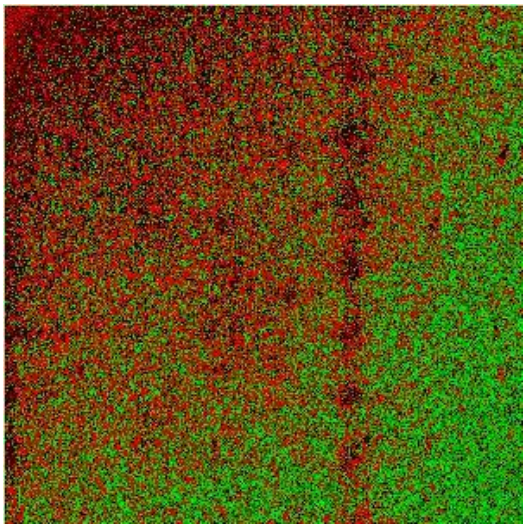

Figure 8.(500x500) pixels Transformation

Figure 9.(1000x1000) pixels original image

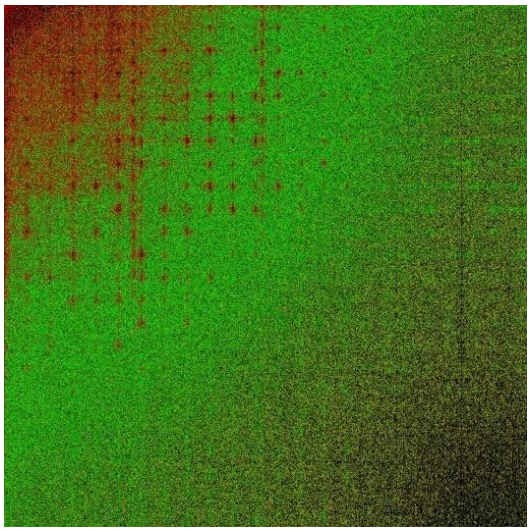

Figure 10.(1000x1000) pixels Transformation

In transformation time of the image of (300x300) pixels, the processing speed is fast. At the image of (1000x1000) pixels have delay time for transformation. So the input image of the system must be (300x300) pixels image.

7. Conclusion

In the proposed algorithm the images encryption is done by encrypting the basic frequencies of the image. This paper implemented after transformation for the encryption of digital image. The algorithm for image encryption based on image processing with DCT and 3DES. The main purpose of this paper we convert original image to using two dimensional transform and encryption 3DES with two keys. The original image is encrypted after the transformation process. Note that the image size will increase in high and width, since for each byte needs an extra bit of the sign of the pixel value. The main purposed algorithm to reduce the computational requirements for huge volume of images and resulting high speed transformation and encryption system.

8. References

[1] A.Aggoun, I.Jalloh, Two Dimensional DCT/IDCT Architecture, De Montfort University, Gateway Leicester LE1 9BH.

[2] Axel Sikora, Implementing DES/3DES with Atmel FPSLIC, Germany.

[3] Gaurav Gupta1, Himanshu Aggarwal2, Digital Image Watermarking using 2DDWT,DCT and FFT, University of Engineering, Patiala, India.

[4] Khan Wahid, Vassil Dimitrov and Graham Jullien, Error-Free Computation of 8x8 2-D DCT and IDCT using Two-Dimensional Algebraic Integer Quantization, University of Calgary, Canada.

[5] Lala Krikor, Sami Baba, Thawar Arif, Zyad Shaaban, Image Encryption Using DCT and Stream Cipher, Jordan, 2009.

[6] Syed Ali Khayam, Discrete Cosine Transform (DCT): Theory and Application, Michigan State University, March 10th 2003.