International Journal of Innovative Research in Computerand Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

||Volume 8, Issue 4, April 2020||

Image Encryption for Secure Internet Transfer using DCT with Triple DES Algorithm

Dr. G. Vinoth Chakkravarthy[1], Chowmeya Prakash[2], Priyadharsini C[3], Viveka S[4], Yatheeswari N.B[5]

Associate Professor, Department of CSE, Velammal College of Engineering and Technology, Madurai, India[1]

UG Students, Department of CSE, Velammal College of Engineering and Technology, Madurai, India [2,3,4,5]

ABSTRACT: Encryption is commonly used for encryption of text as well as images. Various encryption algorithms exist for this purpose. Here we propose to build a secured image encryption algorithm that can be used to encrypt as well as send images remotely to the intended receiver. Our system uses Triple DES algorithm for this purpose. User may submit his image for encryption. Our proposed system now gets the image and compressing the image using Discrete Cosine Transform (DCT) before being encrypted. Then we use Triple DES algorithm to encrypt the image for sending through the internet. User may now select the intended user from among the list of users having our software installed. Our proposed system now send the image in an encrypted format through an active internet connection. Even if an attacker gets the file he first has to decrypt it using proper keys which are not available to him. He then needs to decode the image into proper image format. When image reaches intended receiver he must first enter required keys. On entering the right keys the software decrypts the entire image in original format and provides it to the receiver. Thus we encrypt and securely send images over the internet using secure Triple DES encryption.

KEYWORDS: Encryption, Image Compression, DCT, Triple DES, Decryption, Pixels

I. INTRODUCTION

Any data transmission on internet takes place using the TCP/IP protocol. The image is first broken up into pieces also known as packets which carry the bits of data over the network. A packet consists of control information and user data, which is also known as the payload. Control information provides data for delivering the payload, for example: source and destination network addresses, error detection codes, and sequencing information. Typically, control information is found in packet headers and trailers. The packets when reach their destination, re-associate and end up forming the complete image again.

Image sharing, or photo sharing, is the publishing or transfer of a user's digital photos online. Image sharing websites offer services such as uploading, hosting, managing and sharing of photos (publicly or privately). This function is provided through both websites and applications that facilitate the upload and display of images. The term can also be loosely applied to the use of online photo galleries that are set up and managed by individual users, including photo blogs.

II. RELATED WORK

Apart of so many advantages of DCT and Triple DES algorithm. We conclude the both the algorithm together and improve the security of transfer an image through internet. For the survey, various operations were made, that one is using of quantization is achieved by dividing each element to drastically reduce the space. JPEG takes advantage of this by encoding quantized coefficients in the zig-zag sequences. But the system was only compressed the JPEG format images.

In another method, the spatial and spectral redundancies when certain spatial and spectral patterns between the pixels and the color components are common to each other and the psycho-visual redundancy produces from the fact that the human eye is insensitive to certain spatial frequencies. Lossy compression techniques is used in images where we can sacrifice some of the finer details in the image to save a little more bandwidth or storage space. But due to properties of the human visual system, the Psycho-visual redundancy is founded.

The IMAP block and IMAQ block of MATLAB was used to analyses and study the results of Image Compression using DCT and varying co-efficient for compression were developed to show the resulting image and error image from the original images. The inverse DCT would be performed using the subset of DCT coefficients. The discrete cosine transform (DCT) helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). But, some of the High Frequency Content will be discarded during the compression process.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

||Volume 8, Issue 4, April 2020||

Pseudo random noise (PRN), which is similar to noise and also fulfils a greater number of the standard tests for statistical randomness, can be used as a key for encryption. Based on the number of pixels in the image, Legendre sequences are generated for a set of prime numbers and concatenated to generate the required length sequence. Using Legendre PN sequence which is based on prime numbers, an image encryption technique has been proposed in this paper. Based on the number of pixels in the image, Legendre sequences are generated for a set of prime numbers and concatenated to generate the required length sequence. This sequence is then used to encrypt the secret image that generates noise like pattern.

III. SYSTEM ARCHITECTURE

The below figures were explained the System Architecture (Figure. 3.1) and data flow diagram (Figure. 3.2) of the proposed system.

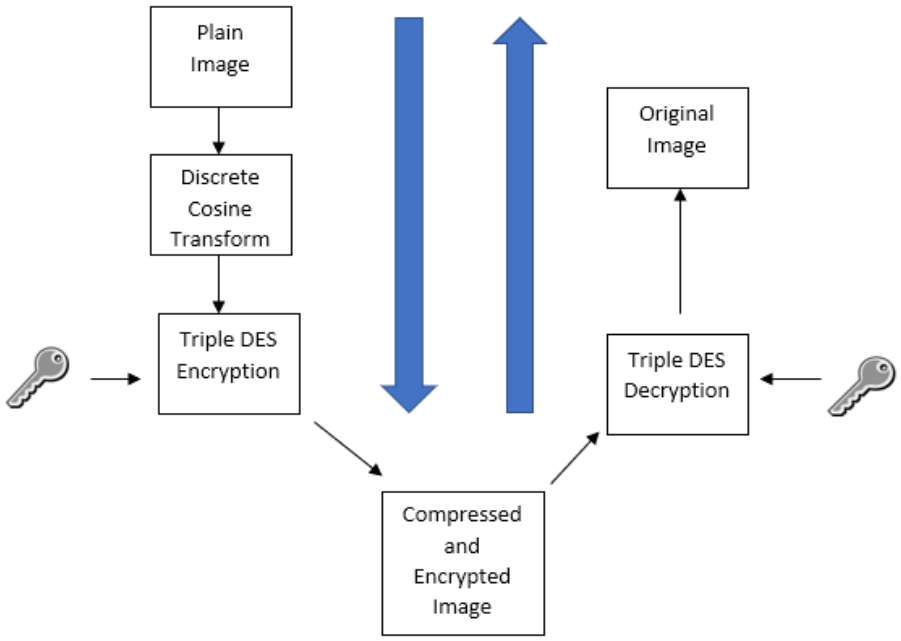

Figure. 3.1 System Architecture

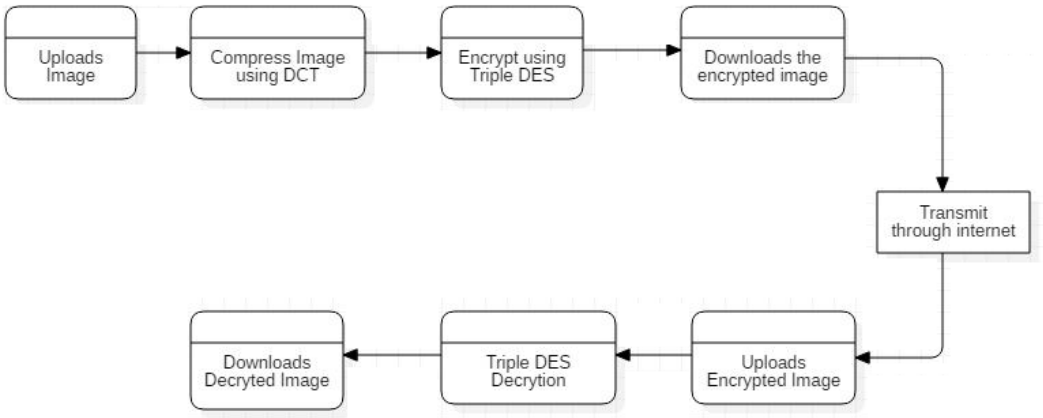

Figure. 3.2 Data Flow Diagram

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

||Volume 8, Issue 4, April 2020||

IV. METHODOLOGY

To improve the security of transferring an image through internet, we using the DCT compression and Triple DES Encryption to transfer the image. In another end, decrypt the file using the Triple DES algorithm.

a.Discrete Cosine Transform (DCT)

The discrete cosine transform (DCT) helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). The DCT is similar to the discrete Fourier transform: it transforms a signal or image from the spatial domain to the frequency domain.

A discrete cosine transform (DCT) expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression images (e.g. JPEG) (where small high-frequency components can be discarded), to spectral for the numerical solution of partial differential equations. The use of cosine rather than sine functions is critical in these applications: for compression, it turns out that cosine functions are much more efficient (as described below, fewer are needed to approximate a typical signal), whereas for differential equations the cosines express a particular choice of boundary conditions.

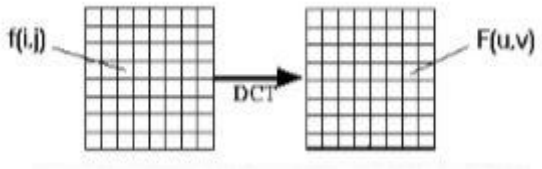

Figure. 4.1 Transformation of function into DCT

b. Triple Data Encrypt Standard (Triple-DES) Encryption

Triple-DES is a process in which we encrypt an image, text or video using 56 bit two keys or 128 bit keys. This kind of process may be secure but still has its flaws. To overcome this flaw we encrypted out file with three 56 bit keys instead of two keys. Hence making it more secure. In the previous referred case study there was only two keys were used for encryption process.

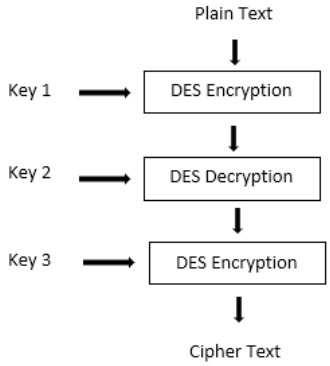

Fig. 4.2 Triple DES Encryption

Triple-Des pseudo code:
Encryption [EDE]:
Input: image_bits, key_64bit1, key_64bit2, key_64bit3
Logic:
Import sys
For img in image_bits:
For each 64bits in img:
64bitimglst.append (64bits)
//create 16 sub keys
//for three separate keys
For I in range 1 to 3

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

||Volume 8, Issue 4, April 2020||

For each 64key_bit(n) in range of 16:
56bit_16key1 = Permute (key_64bit1)
56bit_16key2 = Permute (key_64bit2)
56bit_16key3 = Permute (key_64bit3)
//rearranges the bits (shift cipher)
For l1 in 64bitimglst:
64bitimglst=Initial_permutation (l1)
//16 iterations for 1<=n<=16(n=index number of keys)
For l1 in 64bitimglst:
For I, j, k in 56bit_16key1, 56bit_16key2, 56bit_16key3:
//by applying the formula
Cipherimg64bits=Encrypt(64bitimglst, i)
Cipherimg64bits=Decrpyt(64bitimglst,j)
Cipherimg64bits=Encrypt(64bitimglst, k)
//finalpermuation
Cipherimg64bits=Inverse(Finalpermutation (Cipherimg64bits))
For cimg in Cipherimg64bits:
Cipherimg= Cipherimg+cimg
Output:
[Encrypted_image]= Cipherimg
For cimg in Cipherimg64bits:
Cipherimg= Cipherimg+cimg
Output:
[Encrypted_image]= Cipherimg

c. Triple Data Encrypt Standard (Triple-DES) Decryption

Triple-DES decryption is the reverse process of EDE encryption method. The authorized user uses the same keys that were used for encryption and decrypts the file. The keys remains the same but the sequential order changes. To perform Triple-DES decryption we read an image file as bytes and perform decryption and Encryption function as in DES and decrypt the file and save it as an image. The process time how so ever is increased as we make use of high quality images.

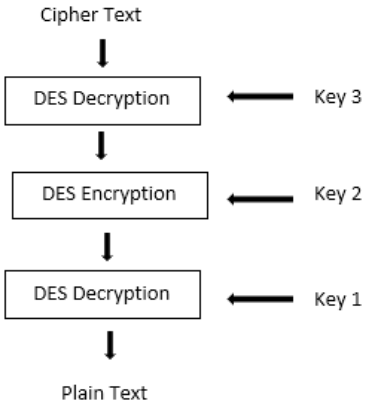

Fig. 4.3 Triple DES Decryption

Triple-Des pseudo code:
Decryption: [DED]
Input: Cipherimg _bits, key_64bit1, key_64bit2, key_64bit3
Logic:
Import sys
For cimg in Cipherimg _bits:
For each 64bits in cimg:
64bitcimglst.append (64bits)
//for three separate keys
Encrypti on key1

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

||Volume 8, Issue 4, April 2020||

Decryption
Key2
Encrypt ion
key3
For I in range 1 to 3
For each 64key_bits in range of 16:
56bit_16key1 = Permute (key_64bits)
56bit_16key2 = Permute (key_64bits)
56bit_16key3 = Permute (key_64bits)
//rearranges the bits(shift cipher)
For l1 in 64bitimglst:
64cbitimglst=Initial_permutation(l1)
//16 iterations for 1<=n<=16(n=index number of keys)
For l1 in 64cbitimglst:
For I, j, k in 56bit_16key1, 56bit_16key2, 56bit_16key3:
//by applying the formula
Cipherimg64bits=Decrypt (64bitimglst, i)
Cipherimg64bits=Encrypt (64bitimglst,j)
Cipherimg64bits=Decrypt (64bitimglst, k)
//finalpermuation
img64bits =Inverse (Finalpermutation (img64bits))
For img in img64bits:
Imgr = imgr + img
Output:
[Decrypted image]=imgr

V. IMPLEMENTATION DETAILS

The system allows the user to login and upload an image with limited size and in-different types in the image format. Once the image has been uploaded, the image was redirected to the compressor. The compressor which is resized the image as 8x8 pixels and those 64 points were processed by the DCT Algorithm.

Once the DCT algorithm, compresses the 64 points of the image. It returns the points and moved towards the Encryptor.

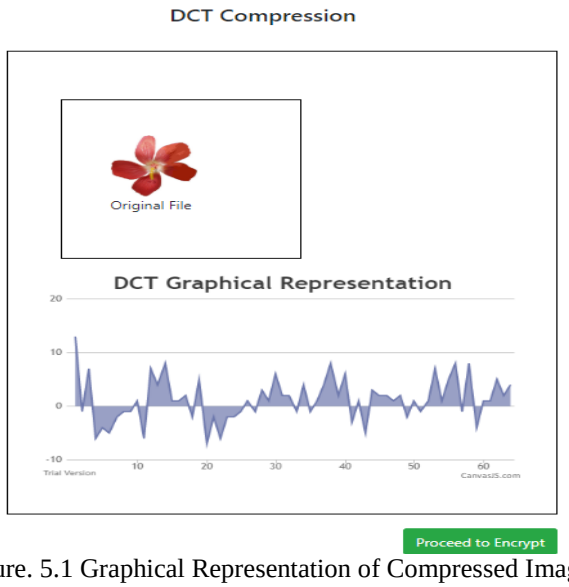

Figure. 5.1 Graphical Representation of Compressed Image

The Encryptor takes the input from DCT points and encrypt using the Triple DES Algorithm with the help of Private Key. The Private Key which is used to encrypt the DCT 64 points. The System finally generates the encrypted file for the user.

In the Decryptor end, the user uploads the encrypted file using the system. The file has been decrypted by the same private key which is used to encrypt the same. It returns the points which is compressed by DCT.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

||Volume 8, Issue 4, April 2020||

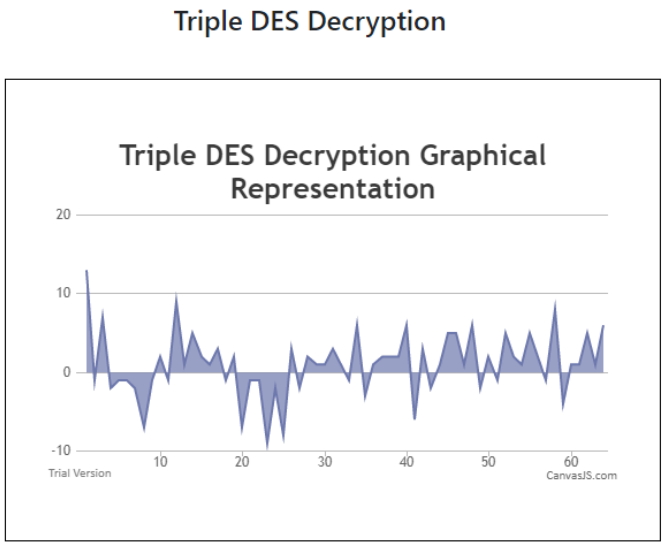

Figure 5.2 Graphical Representation of Decrypted File

VI. RESULTS

Time complexity played a vital role in image encryption and compared to text Encryption process. The DCT Compression and Triple DES Encryption security wise results are better performance and more secured encrypted file which is very difficult to crack when we use 64 bit three different encryption method.

VII. FUTURE WORK

In the future compress and encrypt more than one images at a time and also it's tries to improve no one should crack the encrypted file.

VIII. CONCLUSIONS

In the paper results and discussions prove that the image has been transferred through internet using Discrete Cosine Transform (DCT) and Triple DES Encryption and Decryption (Triple DES). Triple DES gives the better assurance and performance of the process.

REFERENCES

1. T. Koya, S. Chandran and K. Vijayalakshmi, "Analysis of application of arithmetic coding on dct and dct-dwt hybrid transforms of images for compression," 2017 International Conference on Networks & Advances in Computational Technologies (NetACT), Thiruvanthapuram, 2017, pp. 288-293.
2. D. Coppersmith, D. B. Johnson and S. M. Matyas, "A proposed mode for triple-DES encryption," in IBM Journal of Research and Development, vol. 40, no. 2, pp. 253-262, March 1996.doi: 10.1147/rd.402.0253.
3. R. T. Haweel, W. S. El-Kilani and H. H. Ramadan, "A fast modified signed Discrete Cosine Transform for image compression," 2014 9th International Conference on Computer Engineering & Systems (ICCES), Cairo, 2014, pp. 56-61.
4. Wallace, Gregory K. The JPEG Still Picture Compression Standard. Paper submitted in December 1991 for publication in IEEE Transactions on Consumer Electronics.
5. W.B. Pennebaker and J.L. Mitchel, "JPEG Still Image Data Compression Standards", New York: Van Nostrand Reinhold. (1993).
6. G. K .Wallace: "The JPEG Still Picture Compression Standard," Communication of the ACM, Vol.34, No.4, pp .30-44, (Apr 1991).
7. A. B. Waston Mathematica Journal, vol. 4, no. 1, pp. 81-88, 1994. http://vision.arc.nasa.gov/ Image Compression Using Discrete Cosine Transform, Andrew B. Waston publications/mathjournal94.pdf.