Combined Operation of Secret Image Fusion, DCT based Compression and Visual Cryptography based Encryption

Prasanna Kumar H.R
Dept. of Computer Science and Engineering
NMAM Institute of Technology, Nitte

Niranjan N. Chiplunkar, Ph.D.
Dept. of Computer Science and Engineering
NMAM Institute of Technology, Nitte

Archana R Priyadarshini
Dept. of Computer Science and Engineering
NMAM Institute of Technology, Nitte

ABSTRACT

In recent years, there has been a rapid growth on information technology for people to communicate on the Internet. Since Internet is public, anyone can easily read the information and perform successful transmissions without protection. In the present era of computers and fast communication, one needs to protect the communicated information from unauthorized users. For this purpose, Visual Cryptography is introduced to provide confidentiality and security when visual data are transmitted through unsecured communication channels. In this paper, we depict the security of image encryption by the concept of Visual Cryptography Scheme(VCS) . The concept of image fusion helps us to extract features from feature set of different sources and also in applications like remote sensing. Techniques such as DCT based image compression and decompression are used mainly to have high data rates. Further this paper also aims to reduce storage requirements and also our scheme is much more effective for multimedia image compression(energy compaction) and decorrelation by the application of DCT.

General Terms

Confidentiality, security.

Keywords

Visual Cryptography Scheme, DCT, energy compaction, Quantization, Fast Fourier Transform.

1. INTRODUCTION

Security has become an inseparable issue as information technology is ruling the world now. Cryptography is the study of mathematical techniques related aspects of information security such as confidentiality, data security, entity authentication and data origin authentication. But it is not the only means of providing information security, rather one of the techniques. Visual Cryptography[4],[5],[6] is a new technique which provides information security using simple algorithm unlike the complex, computationally intensive algorithms used in techniques like traditional cryptography. This technique allows visual information(pictures, text etc) to be encrypted in such a way that decryption can be performed by human visual system without any complex cryptographic algorithms. This technique encrypts a secret image into shares such that the original secret image is revealed only upon stacking sufficient number of shares. Such a technique purely requires no previous knowledge or experience of cryptography on the part of the person decoding the message. Visual Cryptography uses the algorithm described as the one described here:- The images on the crypto-sheet and key-sheet must be prepared using a computer, but this is a fairly straightforward process. Each pixel in the image is described by a 2-by-2 grid, containing six patterns—horizontal, vertical or diagonal black lines at random. The crypto-sheet also contains 2-by-2 grid for each pixel, but the grids are set to be identical or complementary to those of key-sheet, so that black and white pixels of the original image are reproduced when the sheets are overlapped. In this paper, we depict the security and confidentiality of Visual Cryptography Scheme together with image fusion based and DCT based compression techniques.

2. EXISTING SYSTEM

In the Existing System, the dealer creates two shares(binary images),S_1 and S_2 , consisting of exactly two pixels for each pixel in the secret image. If the pixel is white, the dealer randomly chooses one row from the first two rows of the table shown below in Table 2. Similarly if the pixel is black, the dealer randomly chooses one row from the last two rows of the table as shown below.

Table 2 Pixel pattern for 2-out-of-2 VCS

Original Pixel	Pixel Value	Share1	Share2	Share1+ Share2
□	0	□■	□■	□■
□	0	■□	■□	■□
■	1	■□	□■	■■
■	1	□■	■□	■■

To analyze the security of 2-out-of-2 Visual Cryptography Scheme(VCS)[3],[5],[9],[11], the dealer randomly chooses one of the two pixel patterns say black or white for both of the shares S_1 and S_2.. The pixel selection is done randomly so that each of these shares contain equal number of both black and white pixels. Therefore if an intruder gets a single share, it is not possible to determine that the chosen secret pixel was black or white. This method provides perfect security. On receiving both the shares by the participants and upon superimposing of the two shared subpixels, the secret pixel can be recovered. The results obtained were as shown in Figure 2(a),2(b),2(c),2(d).

Fig 2(a) Original Secret Image

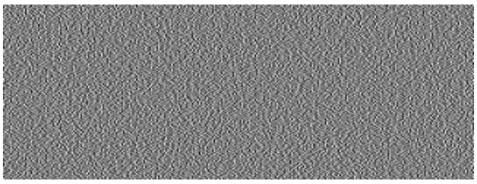

Fig 2(b) Share1 of the secret image

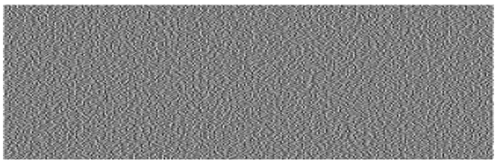

Fig 2(c) Share2 of the secret image

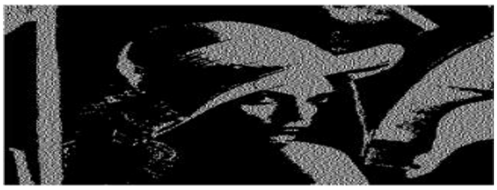

Fig 2(d) Overlapped Share

3. PROPOSED SYSTEM

3.1 Design Approach1

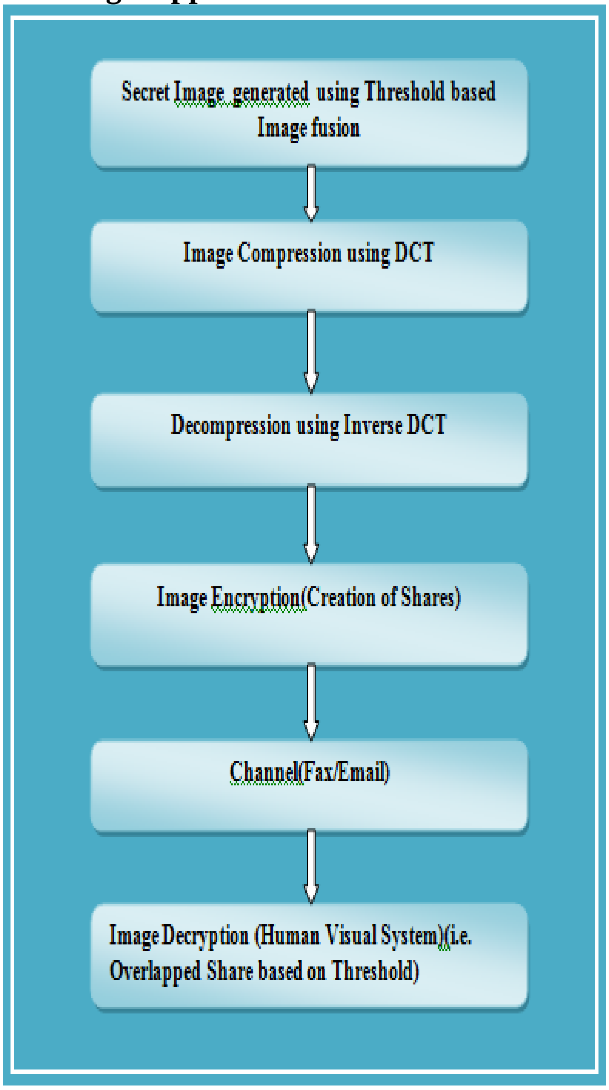
Secret Image generated using Threshold based Image fusion
Image Compression using DCT
Decompression using Inverse DCT
Image Encryption(Creation of Shares)
Channel(Fax/Email)
Image Decryption (Human Visual System)(i.e. Overlapped Share based on Threshold)

Fig 3.1

3.2 Design Approach2

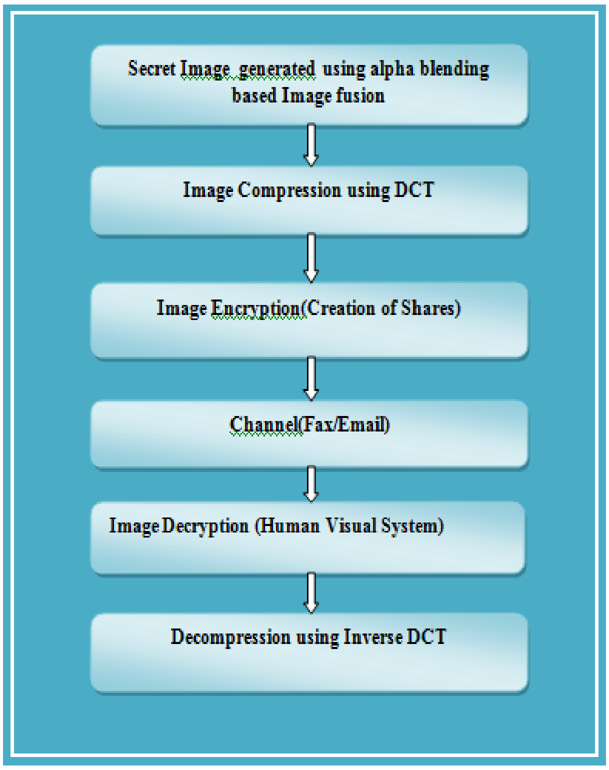
Secret Image generated using alpha blending based Image fusion
Image Compression using DCT
Image Encryption(Creation of Shares)
Channel(Fax/Email)
Image Decryption (Human Visual System)
Decompression using Inverse DCT

Fig 3.2

3.3 Design Approach1: Threshold based Image Fusion, Jpeg Compression and Decompression using DCT Matrix and Image Encryption

The design flowchart of this entire approach is depicted in Figure 3.1. In this approach, the secret image is got by image fusion(combination of two images into a single image on threshold basis). The fused image is then compressed using DCT matrix(also called Discrete Cosine Transform matrix). DCT[4],[12],[13] represents an image as the sum of sinusoids of varying magnitudes and frequencies. For a two dimensional DCT of a M-by-M matrix A, DCT can be computed as B= T *A*T'. DCT converts the information contained in block(8x8) of pixels from spatial domain to frequency domain. Here our original secret image which is based on threshold based fusion technique is divided into 8-by-8 blocks and two dimensional DCT is computed for each block. DCT coefficients are quantized, coded and transmitted. Image decompression is done using inverse two dimensional DCT which is given by T '*B*T. Decompression of an image is done by the Jpeg receiver where it decodes the Quantized DCT coefficients. The decompressed image is then subjected to encryption by the creation of required number of shares which are given to the participants. In Image Decryption, the 1st share is chosen as a master key where the secret image can be generated upon stacking of any shares with the first share chosen as a master key.

Jpeg Standard makes use of DCT for compression and the process is depicted as shown in Figure 3.3(a) .

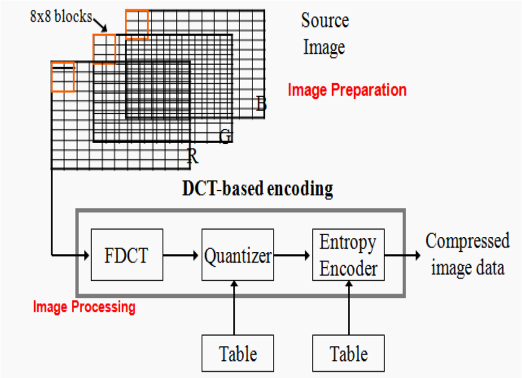

Fig 3.3(a) Jpeg Image compression using DCT

The overall process of Image compression and Decompression using DCT is as shown in Figure 3.3(b).

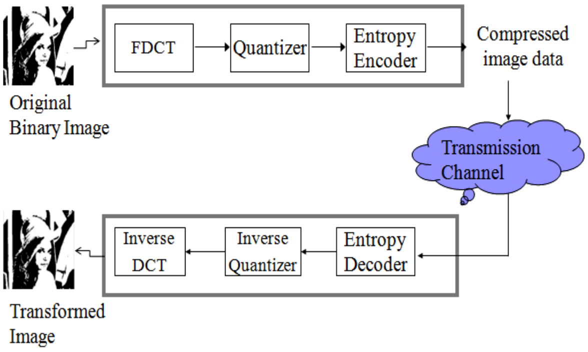

Fig 3.3(b) Image compression and Decompression Process

The process of Quantization is used to compress each block. Quantization takes place by dividing each element in the transformed image matrix B by the corresponding element in the quantization matrix and then rounding off to the nearest integer value. Thus the resultant quantized matrix has coefficients situated at the upper-left corner which correspond to lower frequencies to which human eye is most sensitive to the image block. During the process of Quantization, less important frequencies are discarded, thus giving rise to a lossy part of compression. Thus the reconstructed image consists of non-zero coefficients. Thus Decompression process retrieves the most significant information.

3.4 Design Approach2: Image Fusion, Jpeg Compression, Image Encryption and Jpeg Decompression using DCT Matrix

The design flowchart of this entire approach is depicted in Figure 3.2. In approach2, the image fusion is got not by threshold basis but by the concept of alpha blending and also by scaling the intensities of two images at a time (say A and B) jointly as a single dataset and thus we are able to make the composition of any number of gray-scaled images. Alpha blending allows us to add visual objects to a background image. Image compression uses Jpeg Standard similar to the previous approach as in 3.3. DCT is actually a cut-down version of Fast Fourier Transform(FFT). Here our blended fused image is subjected to image compression using DCT matrix. Quantization step, where the actual image compression takes place cannot be reversed when decompressing the data, thus the overall compression is ‘lossy’ or ‘irreversible’. This is due to the fact that, during Compression, redundant information are discarded. Compression has the advantage that it is read-only and cannot be modified or manipulated. Further this compressed image is subjected to image encryption. The 1st share is chosen as the master key from which on overlap of any share with the master key reveals the secret image during Image Decryption. Finally the Decrypted Image is subjected to Jpeg based Image Decompression technique based on Inverse-DCT. Since DCT is used, which is basically a ‘lossy’ image compression technique, our reconstructed decompressed image will not be identical to that of original, but there will be certain distortion in the image.

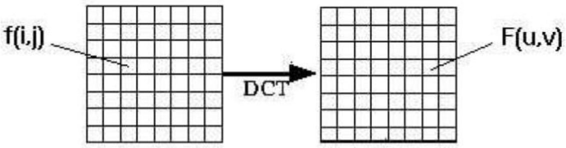

Fig 3.4(a) Applying DCT

Here in this Figure 3.4(a) , we observe how the transformation of a signal(or image) takes place from spatial domain to frequency domain. f(i,j) represents the intensity of pixel in row i and column j. F(u.v) represents DCT coefficient in row ui and column vj of DCT matrix. F(0,0) includes the lowest frequency termed as DC coefficient whereas F(0,1) to F(7,7) are termed AC coefficient. A DCT based transformation matrix is especially useful JPEG image compression. An 8x8 DCT matrix is applied to non-overlapping block throughout the image and only the subblock on the top-left corner of the each block is kept. During restoration process, the remainder of the block is filled with zeros and inverse transformation is applied to the block. The definition of DCT entries are shown in Figure 3.4(b).

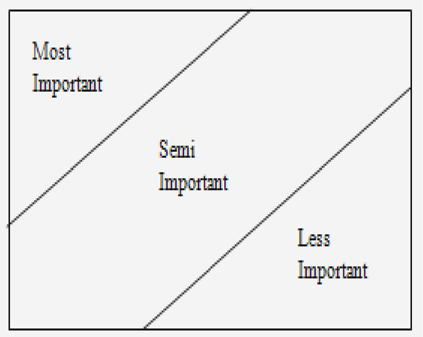

Fig 3.4(b)

We find that the most important values are placed at the top upper left corner of the DCT matrix and less important information are placed at the lower right corner of the matrix.

4. RESULTS

4.1 Results based on Proposed Approach1

In threshold based image fusion, given two gray-scaled images one of them considered to be a foreground image and the other background image, fusion takes place based on certain threshold criteria that is predefined. The result is that any one of the images say foreground or background is highlighted. In case the threshold is halved, the half of the pixel sets from both of the images are displayed. Fused images are compressed using DCT and decompressed using IDCT(Inverse DCT). Images are further encrypted and decrypted by stacking sufficient number of shares. Here we have considered two BMP images.

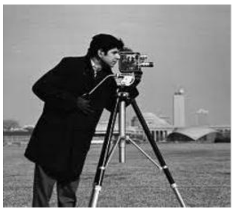

Fig 4.1(a) Background Image

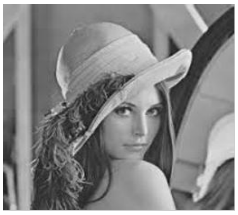

Fig 4.1(b) Foreground Image

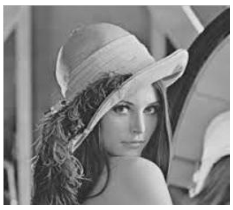

Fig 4.1(c) Original Fused Image

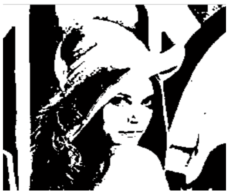

Fig 4.1(d) Binary fused Image

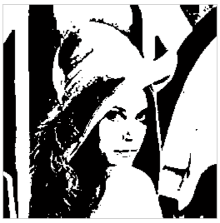

Fig 4.1(e) DCT compressed image

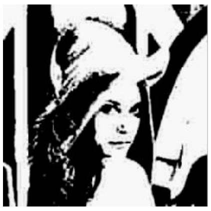

Fig 4.1(f) IDCT Decompressed Image

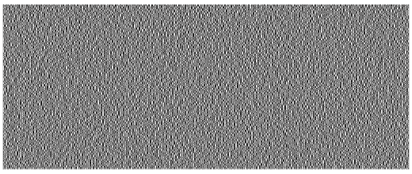

Fig 4.1(g) Share1

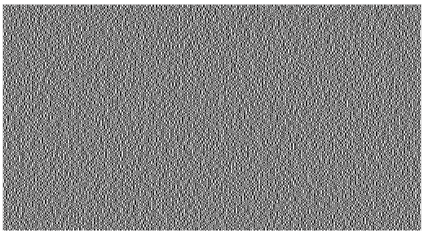

Fig 4.1(h) Share2

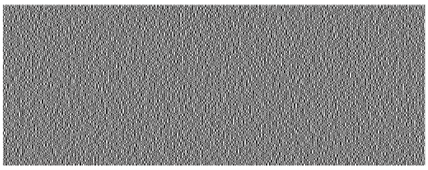

Fig 4.1(i) Share3

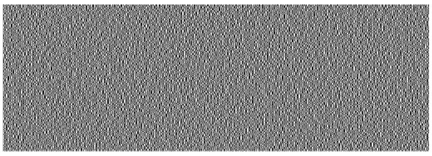

Fig 4.1(j) Share4

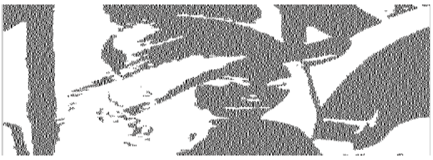

Fig 4.1(k) Overlap of Share1&2

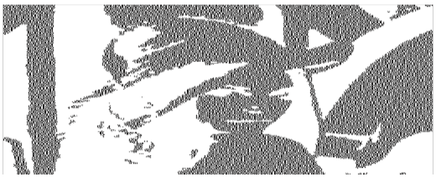

Fig 4.1(l) Overlap of Share 1&3

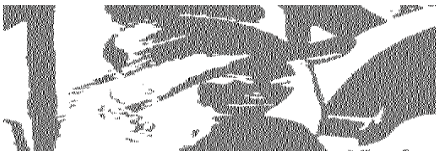

Fig 4.1(m) Overlap of Share 1&4

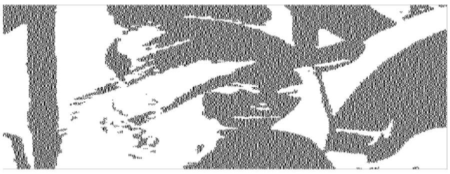

Fig 4.1(n) Overlap of Share 1,2,3

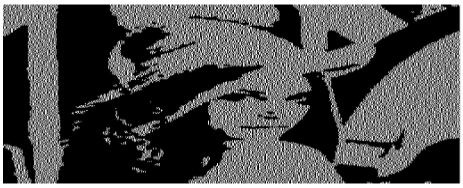

Fig 4.1(o)Overlap of all 4 shares

4.2 Results based on Proposed Approach2

In this approach, Image fusion is performed by alpha blending i.e. by the composition of any number of gray-scaled images. The fused image is then subjected to DCT based Jpeg compression technique. Compressed Image is then encrypted to create sufficient number of shares. Finally the decrypted image is decompressed using Inverse-DCT. But there is degradation in Image quality. Here we have considered two BMP images and a jpeg image.

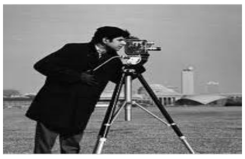

Fig 4.2(a) Original Image

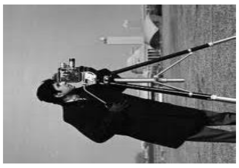

Fig 4.2(b) Rotated Image

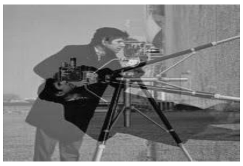

Fig 4.2(c) Fused Image of Fig 4.2(a)&(b)

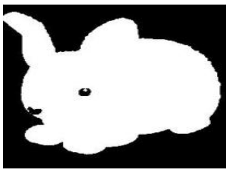

Fig 4.2(d) Third Image

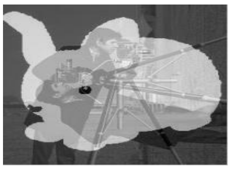

Fig 4.2(e) Fusion of Fig 4.2(c) &(d)

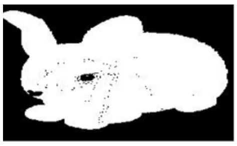

Fig 4.2(f) Binary Fused Image

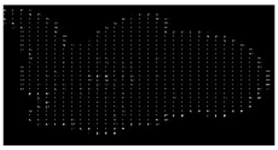

Fig 4.2(g) DCT Compressed Image

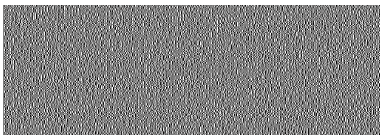

Fig 4.2(h) Share1

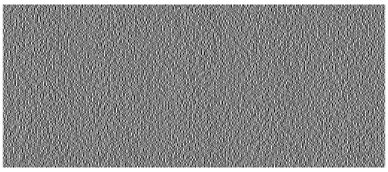

Fig 4.2(i) Share2

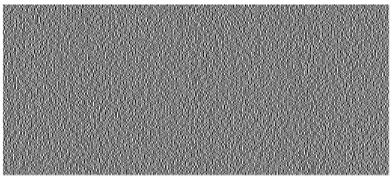

Fig 4.2(j) Share3

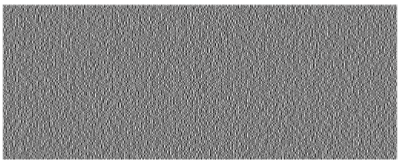

Fig 4.2(k) Share4

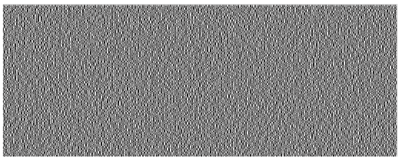

Fig 4.2(l) Share5

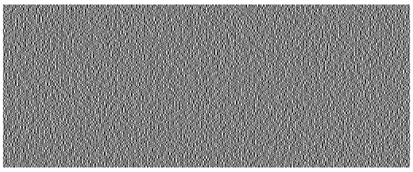

Fig 4.2(m) Share6

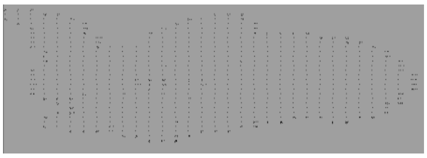

Fig 4.2(n) Overlap of share1&2

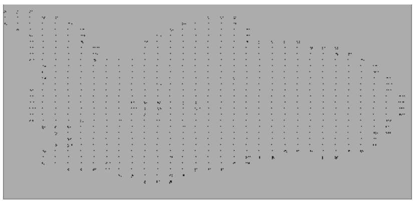

Fig 4.2(o) Overlap of share1&6

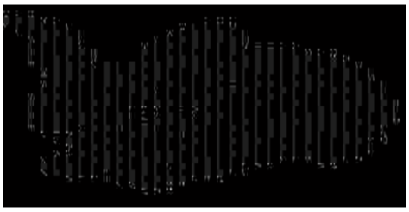

Fig 4.2(p) Overlap of all 6 Shares

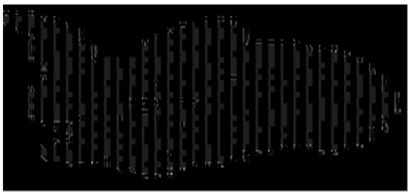

Fig 4.2(q) Inverse DCT Decompressed Image

5. COMPARISON OF EXISTING SYSTEM WITH THE PROPOSED APPROACHES

In the existing system, the secret image was encrypted using 2-out-of-2 Visual Cryptography. The original image was got by overlapping of these 2 shares. But our proposed system is very efficient. Our Proposed Approach in Section 3.3 is very much efficient in terms of Image quality than the Proposed Approach in Section 3.4. The Proposed Approach of Section 3.4 can make the composition of any number of images and has its applications in remote sensing but it is very much efficient in terms of security since compressed image which cannot be manipulated is further encrypted using Visual Cryptography rather than the approach proposed in Section 3.3 where the decompressed image is encrypted using Visual Cryptography. Moreover our Proposed approaches has benefits such as Confidentiality(i.e. by Visual Cryptography technique), High data rates, Secure from intruders, High Bandwidth(i.e. by DCT technique), extracting lot of features from feature sets in a single data set(i.e. by Composition technique).Our Proposed Approaches which makes use of DCT based Compression has lot of advantages over DFT since DCT has higher compression efficiency than DFT and also it avoids generation of spurious spectral components.DCT also exhibits good decorrelation and energy compaction characteristics[3].

6. CONCLUSION

This paper combines technologies such as Visual Cryptography , Image fusion, DCT compression and IDCT Image Decompression. The property that VCS(Visual Cryptography Scheme)relies purely on human visual system, leads to a lot of interesting applications in public and private sectors of our society. Visual Cryptography has the benefits that the person who decodes the message need not have any knowledge of cryptography and it can be used in lot of data hiding techniques such as steganography, watermarking. DCT based techniques have very good decorrelation i.e. removal of redundancies between neighboring pixels as well as energy compaction properties and also faster implementations are possible. Compression techniques are also able to reduce the storage requirements. Composition based image fusion helps to retrieve all features from different feature sets in a single data set and has its applications in remote sensing.

7. REFERENCES

[1] Prakash Chandra Jena1, Nikunja Kanta Das2, A Survey on Visual Cryptography using Image Encryption and Decryption, International Journal of Emerging Technology and Advanced Engineering ,ISSN 2250-2459l, Volume 3, Issue 8, August 2013.

[2] Pravin B. Pokle, N. G. Bawane, Lossy Image Compression using Discrete Cosine Transform, National Conference on Innovative Paradigms in Engineering & Technology (NCIPET-2012) , Proceedings published by International Journal of Computer Application IJCA.

[3] Jagdeep Verma, Dr.Vineeta Khemchandani ,A Visual Cryptographic Technique to Secure Image Shares, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Vol. 2, Issue 1, pp.1121-1125, Jan-Feb 2012 .

[4] S.Manimurugan, Dr.K.Porkumaran, New Fast and Efficient Visual Cryptography Scheme for Medical Images with Forgery Detection, Proceedings of ICETECT 2011.

[5] Er. Supriya Kinger, Efficient Visual Cryptography, Journal of Emerging Technologies in Web Intelligence, VOL. 2, NO. 2, pp. 137-141,MAY 2010

[6]P.S.Revenkar, Anisa Anjum, W .Z.Gandhare, Survey of Visual Cryptography Schemes, International Journal of Security and Its Applications, Vol. 4, No. 2, pp.49-56,April- 2010

[7] Z. Zhou, G. R. Arce, and G. Di Crescenzo, “Halftone Visual Cryptography,” IEEE Trans on Image Processing to appear in 2006

[8] R. C. Gonzalez and R. E. Woods, "Digital Image Processing", 2nd Ed., Prentice Hall, 2004.

[9] G.Ateniese, C.Blundo, A.DeSantis, D.R.Stinson, Visual Cryptography for general Access structures, Proc.ICALP96, Springer,Berlin,1996,pp.416-428.

[10] M. Naor and A. Shamir, “Visual cryptography,” Adv. Cryptol.: EUROCRYPT, Lecture Notes Comput. Sci., vol. 950, pp. 1-12, 1995.

[11] Naor, M., and Shamir, A. (1995), Visual cryptography, in ‘‘Advances in Cryptogoly Eurocrypt ’94’’ (A. DeSantis, Ed.), Lecture Notes in Computer Science, Vol. 950, pp. 112, Springer-Verlag, Berlin

[12]Andrew B. Watson, Image Compression Using the Discrete Cosine Transform ,Mathematica Journal, 4(1), 1994, p. 81-88

[13]www.ee.ic.ac.uk/hp/staff/dmb/courses/DSPDF/00300_Transforms.pdf

[14]www.fe.infn.it/u/filimanto/scienza/webkrypto/visualdecryption.pdf

[15] R. L. Rivest and A. Shamir, “How to expose an eavesdropper”, Communications of the Association for Computing Machinery, vol. 27, no. 4, pp. 393-395, 1984.