2015 17th UKSIM-AMSS International Conference on Modelling and Simulation

A Novel hybrid Discrete Cosine Transformation and Visual Cryptographic Technique for securing digital images

Quist-Aphetsi Kester[124], Laurent Nana[2], Anca Christine Pascu[3], Sophie Gire[2],Jojo M. Eghan[4], Nii Narku Quaynor[4]
[1]Faculty of Informatics, Ghana Technology University College, Accra, Ghana
Kester.quist-aphetsi@univ-brest.fr / kquist@ieee.org
[2]Lab-STICC (UMR CNRS 6285), European University of Brittany, University of Brest, France
[3]UFR Sc. et Tech and Lab-STICC (UMR CNRS 6285) European University of Brittany, UBO, France
[4]Department of Computer Science and Information Technology, University of Cape Coast, Cape Coast, Ghana

Abstract— **Security of digital images in today's cyber is a major concern. Transmission of compressed and uncompressed multimedia data is necessary for communication between different devices. Devices of different screen features and resolution need very efficient and fast compression techniques in order to maintain visual features of transmitted media. Robustness is of a key consideration and importance in image compression techniques. Full recovery of images after compression is a challenge for image compression algorithms. It is practically closely impossible for most encrypted-compressed-images or compressed-encrypted-images to be efficiently and fully reconstructed. In this paper we proposed a robust, efficient and fully recoverable encrypted-compressed image based on hybrid discrete cosine transformation and visual cryptographic technique for securing digital images. We first encrypted the image without pixel loss and then compressed the image which resulted into pixel loss during the compression phase. We decrypted the compressed image by obtaining perfect visuals but losses in pixel values. The analysis of the process proved to be an efficient way of encrypting images and compressing them for other channels with less data capacity without the worry of visual loss as well as ensuring security of the data during transmission. The programming and implementation was done using MATLAB.**

Keywords- visual cryptography; image compression; discrete cosine transformation; pixel transposition

I. INTRODUCTION

Security and privacy in transmission of digital signal play a vital role in image security. Image-data transmission from one site to another through public network is usually characterized in term of privacy, authenticity, and integrity [1]. Cryptographic approaches have been the bedrock for the transmission of data through secured and unsecured channels. These channels are normally confronted with a lot of issues such as capacity and speed.

The enormous amount of visual information available in digital format and in digital space has grown exponentially recently due to the wide range availability of digital equipments, spread use of the Internet in all types of personal and business activities, pay-after-trial services of digital multimedia and developments in high speed transmission of digital images[2].

Resources dedicated for transmission of data in streaming can be very huge based on different kinds of devices used [3]. There are significant challenges when working with more demanding data flows where multimedia streams are required for such devices with focus on service quality [4] as well as dedicated to resource [5]. For most applications, hybrid cryptographic approaches alongside with data compression techniques can produce a high cost in the transmission of data. That means that there have to be provisions at the transmitter side to take care of disparate applications or devices. This puts a lot of load on the server side and can lead to delays in transmission and can make real-time applications slower in transmission of live footage to disparate applications in a distributed environment. This can create a lot of problems such as in intelligence missions for Unmanned Ariel Vehicles where the security strength of footages and real-time videos are of paramount importance because a joint force operation on a distributed battle field will be using disparate applications of different size and resolutions can pose a lot of challenges. For such applications, robust and strong encryption techniques are required as well as speed for data transmission. Hence an efficient cryptographic scheme is needed to provide the following:

- high level data security
- high speed data transmission rates
- fast and robust encryption technique/schemes
- easy access to one source of data stream by desperate devices
- high visuals in decrypted data

The ability to satisfy the above conditions will provide visual cyber physical warfare superiority and dominance to ones drones and other UAVs in the warfare of the engagement of machines. The above is a very critical issue that faces the cyber warfare and cyber arms race in today's world.

In 2009, Iran-backed Shiite militants in Iraq were found to have downloaded live, unencrypted video streams from American Predator drones with inexpensive, off-the-shelf software. This was confirmed to be possible due to the challenge or lack of fast data transfer capability of highly secured encrypted data via space [6].

This paper proposed a robust, efficient and fully recoverable encrypted-compressed image technique or

978-1-4799-8713-9/15 $31.00 © 2015 IEEE
DOI 10.1109/UKSim.2015.101

approach based on a hybrid discrete cosine transformation and visual cryptographic technique for securing digital images. The image was first encrypted without pixel expansion, making it difficult for an adversary to visually read the content. The ciphered image was then compressed and this resulted into pixel loss during the compression phase. The compressed but loss in pixel value ciphered image was then decrypted successfully by obtaining perfect visuals but losses in pixel values. The analysis of the process proved to be an efficient the work is explained as in the followings. The paper has the following structure: section II Related works, section III Methodology, section IV The explanation of the procedure used, section V results and analysis, and section VI concluded the paper.

II. Related Works

Majority of video coding standards adopt a hybrid structure of macroblock-based motion compensation and block DCT, the blocking artifacts occurs at both the block boundary and block interior, and the degradation process due to quantization is generated on differential images. Junghoon et al worked on restoration of differential images for enhancement of compressed video. In their work, a modified regularization algorithm was used to enhance compressed video by restoring predictive-coded pictures. And their proposed method was more suitable for implementations in the decoding processes for enhancing the compressed video, such as digital VCR and digital HDTV systems [7]. Discrete cosine transform (DCT) is one the most lossy/lossless transform coding techniques used for image compression widely used technique. Prabhu et al proposed a 3-D warped discrete cosine transform for MRI image compression. In their work, they extended this concept and develop the 3-D warped discrete cosine transform (WDCT), a transform that has not been previously investigated and proposed a complete image coding scheme for volumetric data sets based on the 3-D WDCT scheme. Their results showed that the 3-D WDCT-based compression scheme performs better than a similar 3-D DCT scheme for volumetric data sets at high bit-rates [8]. The JPEG [9] compression standard is widely adopted in still image coding. The process consists of three stages: the block discrete cosine transform (DCT), uniform quantization with a quantization table, and the Huffman (used in the baseline system) or the arithmetic (used in the extended system) entropy coding [10]. Discrete Cosine Transform (DCT) is very important in image compression. Classical 1-D DCT and 2-D DCT has time complexity O(NlogN) and O(N&sup2;logN) respectively [11]. Nacer et al. proposed lossy image compression technique based on an orthogonal transformation global discrete cosine transform, GDCT, using an optimal data truncation combined with entropy coding [12]. There have also been some works in digital watermarking Encryption image for safe transmission and DCT [13]. And also digital watermarking approaches of Color Image based on Visual Cryptography and Discrete Cosine Transform was carried out by Yanyan Han et al [14].

A robust, efficient and fully recoverable encrypted-compressed image based on hybrid discrete cosine transformation and visual cryptographic technique for securing digital images was proposed in this paper.

III. Methodology

The method of implementation consists of the image visual cryptographic image process. The visual cryptographic approach was achieved by separating image into its RGB channels as n shares. The channels were then transposed; pixel values displaced, interchanged with the other channels positions and shuffled based on the algorithm. The Discrete Cosine Transform was then used to compress the image. The reverse processes from bottom to the up then yielded back the plain image but with loss pixel values. The following section then showed the detailed of the processes engaged.

IV. The Techniques Engaged

The explanations for the approaches used consisted of the image encryption and the process.

A) The Image Encryption Process

Step1. Start

Step2. Extraction of data from a plain image,

Let *I*= an image=*f (R, G, B)*

Were *R, G, B* are the channels

I is a color image of *m x n x 3* arrays

$$\left(\begin{array}{ccc} R & G & B \\ r_{i1} & g_{i2} & b_{i3} \\ \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \\ r_{n1} & g_{n2} & b_{n3} \end{array}\right) \qquad (1)$$

Let m= row size and n = column size

(R, G, B) = m x n

Where *R, G, B ∈ I*

(R o G) i j = (R) ij. (G) ij

Where *r_11* = first value of *R*

r= [ri1] (i=1, 2… m)

x ∈r_i1 : [a, b]= {x ∈I: a ≤ x ≥ b}

a=0 and *b=255*

R= r= I (m, n, 1)

Where *g_12* = first value of *G*

g= [gi2] (i=1, 2… m)

x ∈g : [a, b]= {x ∈I: a ≤ x ≥ b}

a=0 and *b=255*

G= g= I (m, n, 1)

And *b_13* = first value of *B*

b= [bi3] (i=1, 2… m)

x ∈b_i1 : [a, b]= {x ∈I: a ≤ x ≥ b}

a=0 and *b=255*

B=b= I (m, n, 1)

Such that *R= r= I (m, n, 1)*

Step3. Extraction of the red component as '*r*'

Let size of *R* be *m x n* *[row, column] = size (R) = R (m x n)*

$$rij= r= I\ (m, n, 1) = \begin{pmatrix} R \\ r_{i1} \\ \vdots \\ \vdots \\ r_{in} \end{pmatrix} \qquad (2)$$

Step4. Extraction of the green component as *'g'*

Let size of *G* be *m x n* *[row, column] = size (G)*

$$gij= g= I\ (m, n, 1) = \begin{pmatrix} G \\ g_{i2} \\ \vdots \\ \vdots \\ g_{n2} \end{pmatrix} \qquad (3)$$

Step5. Extraction of the blue component as *'b'*

Let size of *B* be *m x n* *[row, column] = size (B) = B (m x n)*

$$bij= b= I\ (m, n, 1) = \begin{pmatrix} B \\ b_{i3} \\ \vdots \\ \vdots \\ b_{n3} \end{pmatrix} \qquad (4)$$

Step6. Getting the size of r as *[c, p] = size (r)*

Let size of *R* be

$$[row, column] = size\ (r) = r\ (c\ x\ p) \qquad (5)$$

Step7. The key k is then engaged to iterate the step 8 to 14.

$$k = [c\ x\ p]^{(c+p)} \text{mod}256 \qquad (6)$$

Step8. Let *r* =Transpose of rij

$$r = \begin{pmatrix} & & R & & \\ r_{i1} & \cdots & \cdots & \cdots & r_{n1} \end{pmatrix} \qquad (7)$$

Step9. Let g =Transpose of *gij*

$$g = \begin{pmatrix} & & G & & \\ g_{i2} & \cdots & \cdots & \cdots & g_{n2} \end{pmatrix} \qquad (8)$$

Step10. Let b =Transpose of bij

$$b= \begin{pmatrix} & & B & & \\ b_{i2} & \cdots & \cdots & \cdots & b_{n2} \end{pmatrix} \qquad (9)$$

Step11. Reshaping of *r* into *(r, c, p)*

$$r= reshape\ (r, c, p) = \begin{pmatrix} R \\ r_{i1} \\ \vdots \\ \vdots \\ r_{in} \end{pmatrix} \qquad (10)$$

Step12. Reshaping of g into *(g, c, p)*

$$g= reshape\ (g, c, p) = \begin{pmatrix} R \\ r_{i1} \\ \vdots \\ \vdots \\ r_{in} \end{pmatrix} \qquad (11)$$

Step13. Reshaping of *b* into *(b, c, p)*

$$b= reshape\ (b, c, p) = \begin{pmatrix} R \\ r_{i1} \\ \vdots \\ \vdots \\ r_{in} \end{pmatrix} \qquad (12)$$

Step14. Concatenation of the arrays *r, g, b* into the same dimension of '*r*' or *'g'* or *'b'* of the original image

$$= \begin{pmatrix} R & G & B \\ r_{i1} & g_{i2} & b_{i3} \\ \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \\ r_{m1} & g_{m2} & b_{n3} \end{pmatrix} \qquad (13)$$

The inverse of the process will yield the deciphering phase. The engagement of this process was used for the image encryption for the results in section V below.

B) Implementation of the Dicrete cosine Transform

Discrete Cosine Transform transforms a time domain signal into its frequency components but it does that by the use of the real parts of the Discrete Fourier Transform (DFT) coefficients only [15]. Discrete cosine transform (DCT) turn over the image edge to make the image transformed into the form of even function with the character of discrete Fourier transform (DFT). It its applications spa across fields such as data compression, pattern recognition, image processing, etc. The DCT transform and its inverse manner can be expressed as follows [16]:

The DCT transform

$$F(u,v)=\frac{4C(u)C(v)}{n^2}\sum_{j=0}^{n-1}\sum_{k=0}^{n-1}f(j,k)\cos[\frac{(2j+1)u\pi}{2n}]\cos[\frac{(2k+1)v\pi}{2n}], \quad (14)$$

The DCT transform inverse

$$f(j,k)=\sum_{u=0}^{n-1}\sum_{v=0}^{n-1}C(u)C(v)F(u,v)\cos[\frac{(2j+1)u\pi}{2n}]\cos[\frac{(2k+1)v\pi}{2n}], \quad (15)$$

Where C(w) = 1/ 2 and when w =0 C(w) = 1 also when w =1,2,3,… n -1

For digital image concept for N-by-N image matrix of real numbers we will have [17, 18]

$$F=\begin{bmatrix} f_{00} & f_{01} & \cdots & f_{0(N-1)} \\ f_{10} & f_{11} & \cdots & f_{1(N-1)} \\ \vdots & \vdots & \vdots & \vdots \\ f_{(N-1)0} & f_{(N-1)1} & \cdots & f_{(N-1)(N-1)} \end{bmatrix} \quad (16)$$

The engagement of this process was used to compressed the image in figure 1 below after it was encrypted using the image encryption technique.

V. SIMULATED RESULTS AND ANALYSIS

The image below was encrypted, compressed and analyzed using the proposed approach and this was implemented in MATLAB. The recovery of the plain image from the compressed ciphered image was achieved successfully.

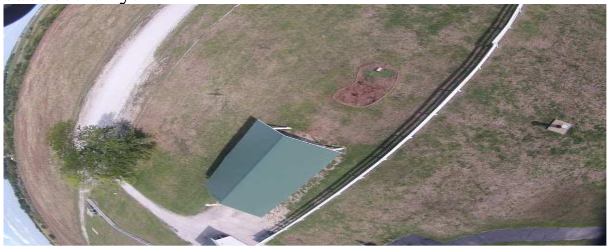

Figure 1. The plain image obtained from a UAV drone.

Figure 2. The ciphered and watermarked image of figure 1.

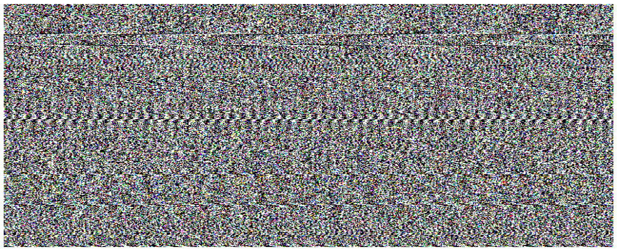

Figure 3. The DCT of figure 2.

Figure 4. The loss pixel imave values of fig 3.

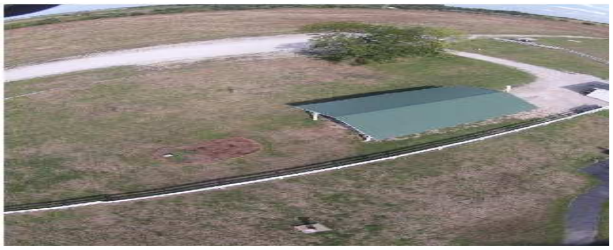

Figure 5. The recovered image from fig 3 .

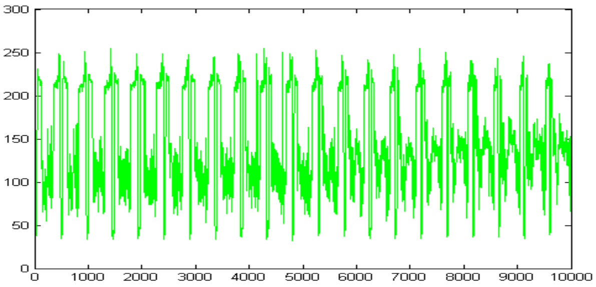

Figure 6. The graph of the first 10000 pixel G value of figure 1 .

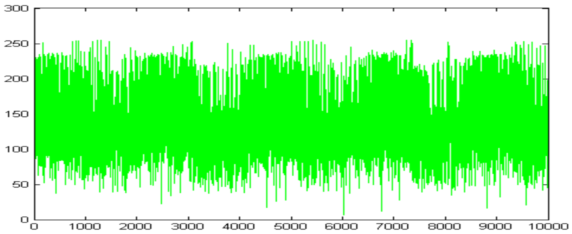

Figure 7. The graph of the first 10000 pixel of G value of figure 3 .

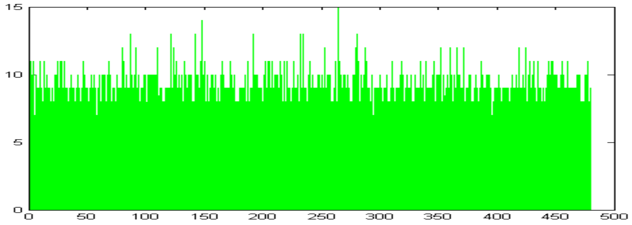

Figure 8. The graph of the pixel G values of figure 4 .

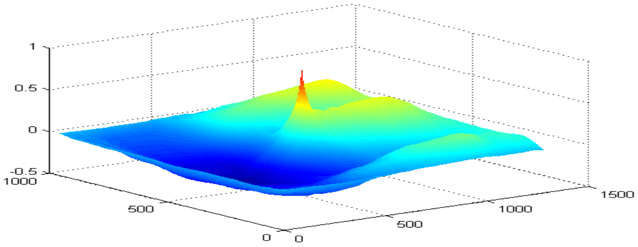

Figure 9. The graph of the normalized cross-correlation of the matrices of the plain image.

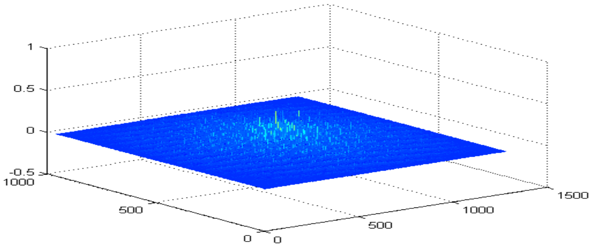

Figure 10. The graph of the normalized cross-correlation of the matrices of the ciphered image.

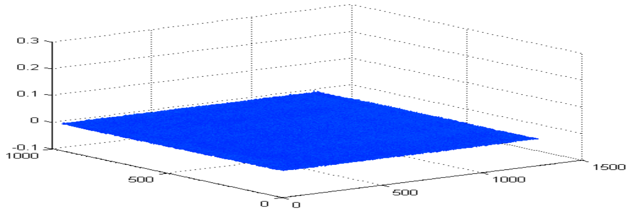

Figure 11. The graph of the normalized cross-correlation of the matrices of figure 4.

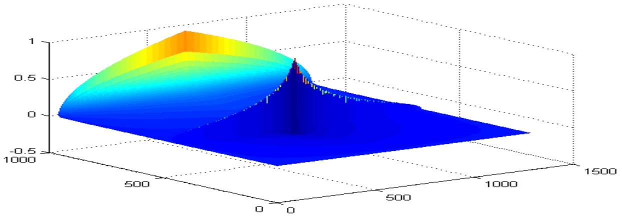

Figure 12. The graph of the normalized cross-correlation of the matrices of the recovered image.

The normalized cross-correlation of the matrices of is

$$\gamma(u,v)=\frac{\sum_{x,y}\left[f(x,y)-\bar{f}_{u,v}\right]\left[t(x-u,y-v)-\bar{t}\right]}{\left\{\sum_{x,y}\left[f(x,y)-\bar{f}_{u,v}\right]^2\sum_{x,y}\left[t(x-u,y-v)-\bar{t}\right]^2\right\}^{0.5}} \qquad (17)$$

f is the mean of the template, $\bar{t}$ is the mean of in the region under the template. $\bar{f}_{u,v}$ is the mean of $f(u,v)$ in the region under the template. The recovered but compressed and decryped image still have visual characteristics that makes it not to be visually different from its original one.

It can clearly be observed in the graphs that there has been transformation and figure 8 shows the graph of G channel pixel values loss during the discrete cosine transformation.

TABLE 1: ANALYSIS OF PLAIN, CIPHERD, COMPRESSED, DECOMPRESSED AND DECRIPTED IMAGE.

	Entropy(p)	*Arithmetic mean(m)*
PI	7.1726	125.8161
EI	7.1726	125.8161
CI	1.1960	5.7262
ICI	7.1753	125.8147
LI	2.0720	1.1645
DI	7.1753	125.8147

PI=plain image, EI= Enrypted Image, CI=Compressed Image, ICI=Decompressed Image, LI= Image Loss due to compression, DI=Decrypted Compressed Image

VI. CONCLUSION

From the table, there was no pixel loss in the ciphered image and the values remain the same for both the plain and the ciphered image. The decompressed image have the same characteristics as the decrypted image due to no pixel loss in that process but there was an increase in entropy in the decrypted image compared with the encrypted image.

With the implementation, we used DCT which has time complexity O(NlogN) with the visual cryptographic algorithm . We decrypted the compressed image by obtaining perfect visuals but losses in pixel values. The analysis of the proposed process proved to be an efficient for encrypting images and compressing them for other channels with less data capacity without the worry of visual loss as well as ensuring security of the data during transmission.

ACKNOWLEDGMENT

This work was supported by Lab-STICC (UMR CNRS 6285) at UBO France, AWBC Canada, Ambassade de France-Institut Français-Ghana and the DCSIT-UCC, and also Dominique Sotteau (formerly directeur de recherche, Centre national de la recherche scientifique (CNRS) in

France and head of international relations, Institut national de recherche en informatique et automatique, INRIA) and currently the Scientific counselor of AWBC, Canada.

REFERENCES

[1] Jianguo Zhang; Fenghai Yu; Jianyong Sun; Yuanyuan Yang; Chenwen Liang, "DICOM Image Secure Communications With Internet Protocols IPv6 and IPv4," Information Technology in Biomedicine, IEEE Transactions on , vol.11, no.1, pp.70,80, Jan. 2007doi: 10.1109/TITB.2006.879606

[2] Ranmuthugala, M.H.P.; Chandana Gamage, "Chaos theory based cryptography in digital image distribution," Advances in ICT for Emerging Regions (ICTer), 2010 International Conference on , vol., no., pp.32,39, Sept. 29 2010-Oct. 1 2010 doi: 10.1109/ICTER.2010.5643275

[3] Asaduzzaman, S.; Maheswaran, M., "Using Dedicated and Opportunistic Networks in Synergy for a Cost-Effective Distributed Stream Processing Platform," Parallel and Distributed Systems, 2008. ICPADS '08. 14th IEEE International Conference on , vol., no., pp.56,63, 8-10 Dec. 2008 doi: 10.1109/ICPADS.2008.116

[4] Lubonski, M.; Gay, V.; Simmonds, A., "An adaptation architecture to improve QoS of multimedia services for enterprise remote desktop protocols," Next Generation Internet Networks, 2005 , vol., no., pp.149,156, 18-20 April 2005 doi: 10.1109/NGI.2005.1431660

[5] Vella, J.; Zammit, S., "A Survey of Multicasting over Wireless Access Networks," Communications Surveys & Tutorials, IEEE , vol.15, no.2, pp.718,753, Second Quarter 2013 doi: 10.1109/SURV.2012.050412.00095

[6] Disarmament and International Security Committee.(2014) The Use of Drones and Autonomous Robots. Bucharest international model united nation congress.

[7] Jung, J., Joung, S., Shin, J., & Paik, J. (2004). Restoration of differential images for enhancement of compressed video. Journal of Visual Communication and Image Representation, 15(1), 91-109.

[8] Prabhu, K. M. M., Sridhar, K., Mischi, M., & Bharath, H. N. (2013). 3-D warped discrete cosine transform for MRI image compression. Biomedical Signal Processing and Control, 8(1), 50-58.

[9] H. G. Musmann and P. Pirsch, “Advances in picture coding,” Proc. IEEE, vol. 73, no. 4, pp. 523–548, Apr. 1985.

[10] Jiankun Li; Jin Li; Kuo, C.-C.J., "Layered DCT still image compression," Circuits and Systems for Video Technology, IEEE Transactions on , vol.7, no.2, pp.440,443, Apr 1997 doi: 10.1109/76.564125

[11] Pang, C. Y., Zhou, Z. W., & Guo, G. C. (2006). Quantum discrete cosine transform for image compression. arXiv preprint quant-ph/0601043.

[12] Nacer, F.-Z.N.; Zergainoh, A.; Merigot, A., "Global discrete cosine transform for image compression," Signal Processing and its Applications, Sixth International, Symposium on. 2001 , vol.2, no., pp.545,548 vol.2, 2001 doi: 10.1109/ISSPA.2001.950201

[13] Ajili, S.; Hajjaji, M.A.; Bouallegue, B.; Mtibaa, A., "Joint WatermarkingEncryption image for safe transmission: Application on medical imaging," Computer & Information Technology (GSCIT), 2014 Global Summit on , vol., no., pp.1,6, 14-16 June 2014doi: 10.1109/GSCIT.2014.6970110

[14] Yanyan Han; Wencai He; Shuai Ji; Qing Luo, "A Digital Watermarking Algorithm of Color Image based on Visual Cryptography and Discrete Cosine Transform," P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference on , vol., no., pp.525,530, 8-10 Nov. 2014doi: 10.1109/3PGCIC.2014.103

[15] Ram, B. (2013). Digital Image Watermarking Technique Using Discrete Wavelet Transform And Discrete Cosine Transform. International Journal of Advancements in Research & Technology, 2.

[16] Wen Yuan Chen and Shih Yuan Huang “Digital Watermarking Using DCT Transformation” Department of Electronic Engineering National ChinYi Institute of Technology.

[17] Rafael C. Gonzalez, Richard E. Woods, ”Digital Image Processing,” Publishing House of Electronics Industry ; Prentice Hall (Beijin, 2002)

[18] Wen Gao, 1994, ”Technique of Multimedia Data Compression,” Publishing House of Electron-ics Industry (Beijin: 1994)