IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

Digital Watermarking with DWT & DCT using Bit Plane Encryption

Ragini Sharma[1], Er. Surbhi Gupta[2]

Scholar at Rayat Bahra Institute of Engineering and Biotechnology Mohali, Punjab[1]

Associate Professor at Rayat Bahra Institute of Engineering and Biotechnology Mohali, Punjab[2]

Abstract: It is a process of hiding a message in a carrier signal (i.e. an image, song, and video) within the signal itself. This is done for the security, data integrity and ownership of data. Digital watermarking comprises various approaches for the hiding of information behind the cover image. In this process the cover image is divided into smaller regions by using various approaches and then the watermark is embedded to these different approaches by using an embedding algorithm. In this process big issue of digital watermarking is security and distortion occurred in different formats of the cover image. Due to distortion the predictions is easy and data at receiver end does not get properly. To overcome these issues in the previous approaches, the bit plane image encryption scheme is proposed for encryption of watermark and implements DWT at fourth level for hiding information using DCT on the cover image and secret image.

Keywords: Watermark, Watermarking, 4th Level DWT and DCT, Bit Plane Encryption, PSNR, MSE, Correlation, SSIM.

1. INTRODUCTION

It is a process of hiding a message in a carrier signal (i.e. an image, song, and video) within the signal itself. Traditional Watermarks may be connected to unmistakable media (like pictures or feature), though in advanced watermarking, the sign may be sound, pictures, feature, writings or 3d models [13]. A sign may convey a few diverse watermarks in the meantime. Dissimilar to metadata that is added to the transporter flag, a computerized watermark does not change the extent of the bearer signal. Watermarking tries to shroud a message identified with the genuine substance of the advanced sign, while in steganography the computerized sign has no connection to the message, and it is only utilized as a spread to conceal its presence. Watermarking has been around for a few hundreds of years, as watermarks found at first in plain paper and accordingly in paper bills. Nonetheless, the field of advanced watermarking was just created amid the most recent 15 years and it is currently being utilized for various applications [10]. The main watermarks showed up in Italy amid the thirteenth century, yet their utilization quickly spread crosswise over Europe.

2. TYPES OF WATERMARKING

There is various types of watermarking such as 'public watermarking', 'blind watermarking', 'semi-blind watermarking', 'private watermarking', 'non-blind watermarking' and 'asymmetric watermarking', 'Digital watermarking'.

Public watermarking and blind watermarking mean the same, but the wording was confusing with public-key watermarking. 'Signal processing people' took over the field, so only the later tends to remain. In these schemes, the cover signal (the original signal) is not needed during the detection process to detect the mark. Solely the key, which is typically used to generate some random sequence used during the embedding process, is required [7].

Private watermarking and non-blind-watermarking mean the same the original cover signal is required during the detection process.

Asymmetric watermarking or public-key watermarking refers to watermarking schemes with properties reminding asymmetric cryptosystem (or public key cryptosystem). No such system really exists yet although some possible suggestions have been made [10]. In this case, the detection process (and in particular the detection key) is fully known to anyone as opposed to blind watermarking where a secret key is required. So here, only a 'public key' is needed for verification and a 'private key' (secret) is used for the embedding. Knowledge of the public key does not help to compute the private key (at least in a reasonable time), it does not either allow removal of the mark nor it allows an attacker to forge a mark.

2.1 STRUCTURE OF A TYPICAL WATERMARKING SYSTEM

Every watermarking system consists at least of two different parts: watermark embedding unit and watermark detection and extraction unit. The unmarked image is passed through a perceptual analysis block that determines how much a certain pixel can be altered so that the resulting watermarked image is indistinguishable from the original. This takes into account the human eye sensitivity to changes in flat areas and its relatively high tolerance to small changes in edges. After this so-called perceptual-mask has been computed, the information to be hidden is shaped by this mask and spread all over the original image. This spreading technique is similar to the interleaving used in other applications involving coding, such as compact disc storage, to prevent damage of the information caused by scratches or dust. The main reason for this spreading is to ensure that the hidden information

DOI 10.17148/IJARCCE.2015.41297

survives cropping of the image.

2.2 DIGITAL WATERMARKING LIFE CYCLE PHASES

The data to be inserted in a sign is known as an advanced watermark, albeit in a few settings the expression computerized watermark implies the contrast between the watermarked sign and the spread sign. The sign where the watermark is to be implanted is known as the host signal [4]. A watermarking framework is typically isolated into three different steps, inserting, assault, and discovery. In inserting, a calculation acknowledges the host and the information to be installed, and produces a watermarked sign [6].

At that point the watermarked advanced sign is transmitted or put away, generally transmitted to someone else. On the off chance that this individual makes a change, this is called an assault. While the change may not be vindictive, the term assault emerges from copyright assurance application, where outsiders may endeavor to evacuate the advanced watermark through alteration [6]. There are numerous conceivable adjustments, for instance, lossy packing of the information (in which determination is decreased), editing a picture or feature, or purposefully including commotion [7].

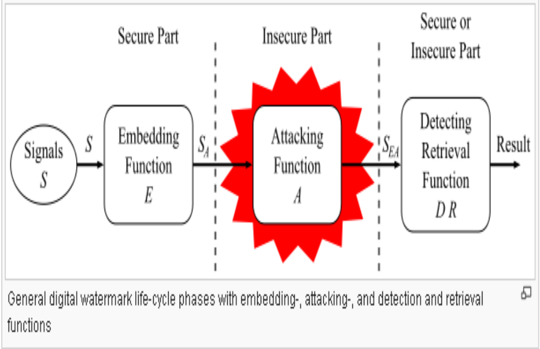
Secure Part
Insecure Part
Secure or Insecure Part
Signals S
S
Embedding Function E
S_A
Attacking Function A
S_{EA}
Detecting Retrieval Function D R
Result
General digital watermark life-cycle phases with embedding-, attacking-, and detection and retrieval functions

Fig.1 Digital watermarking life-cycle phases

Digital watermarking is the process of hiding the secret data behind any image or signal.

2.3 Digital Watermarking models

There are a few routes in which we can display a watermarking procedure. These can be comprehensively characterized in one of two gatherings. The main gathering contains models which are taking into account a correspondence based perspective of watermarking and the second gathering contains models focused around a geometric perspective of watermarking [4].

2.4 Communication-based models

Correspondence based models portray watermarking in a manner fundamentally the same to the conventional models of correspondence frameworks. Watermarking is truth be told a methodology of conveying a message from the watermarking embedded to the watermarking beneficiary. Subsequently, it bodes well for utilize the models of secure correspondence to model this methodology [6]. In a general secure correspondence model we would have the sender on one side, which would encode a message utilizing an encoding key to anticipate spies to interpret the message if the message was captured a mid-transmission. At that point the message would be transmitted on a correspondences channel, which would add some commotion to the clamor to the encoded message.

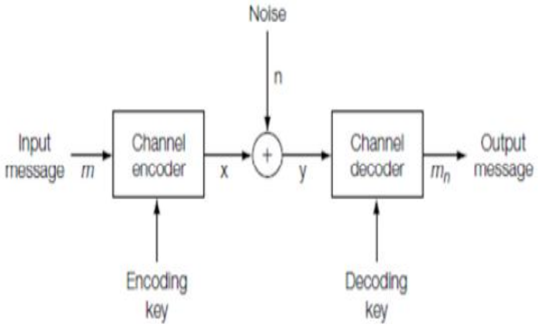

Fig.2 Standard model of a communications channel with key-based encoding

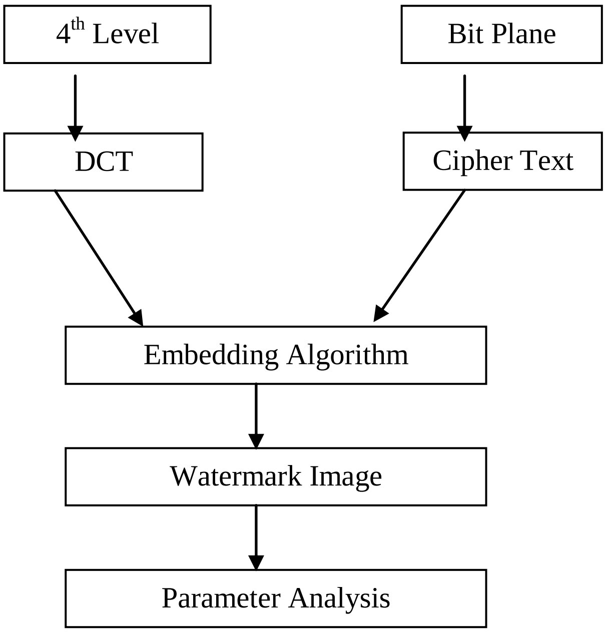

Fig. 3 Flow of work

Here embedding procedure is followed which is based on DCT and DWT. DWT can separate the host image in 4 levels of sub-band. There are LL (high scale low frequency components), HL (Horizontal low-scale, high-frequency components), LH (Vertical low-scale, high-frequency components), and HH (Diagonal low-scale, high-frequency components). The new embedding algorithm (NEA) uses up to 4 levels DWT and embeds image in HL and LH sub-band of host image data. For convenience to discuss firstly focus on 4 levels DWT and then on 3 level and 2 level respectively is done.

A 512×512 image is taken as host image and a 32×32 image is taken as mark image in case of 4 level of DWT. A 256×256, 64×64 and 128×128 image is taken as mark image in case of 3 levels and 2 level of DWT. The image embedding flowchart and its various operational steps are described as follows:

DOI 10.17148/IJARCCE.2015.41297

Step 1: Perform DWT on a 512×512 host image to decompose it into four non-overlapping multi resolution coefficient sets: LL1, HL1, LH1, and HH1.

Step 2: Perform DWT again on two HL1 and LH1 sub-bands to get eight smaller sub-bands and choose two coefficient sets: HL12, and LH22.

Step 3: Perform DWT again on two sub-bands: HL12 and LH22 to get eight smaller Sub-bands and choose two coefficient sets: HL13, LH23.

Step 4: Perform DWT again on two sub-bands:HL13 andLH23 to get eight smaller Sub-bands and choose two coefficient sets: HL14, LH24.

Step 5: Divide coefficient sets: HL14, LH24, into 4 × 4 blocks.

Step 6: Perform DCT to each block in the chosen coefficient sets (HLLL14; LHLL 24).

Step 7: Re-formulate the grey-scale watermark using a key scrambling the gray scale mark image.

Step 8: Transform the image into DCT.

Step 9: DCT Algorithm is used to divide the last block of 32*32 in to 4*4 sub-blocks.

Step 10: In last Bit Plane Encryption is used for the Encryption purpose.

The scrambling method based on bit-plane can combine the pixel exchanging and gray level changing handily to reach a good chaotic effect. The reference is an image scrambling based on bits exchange, which divides the bits of pixels into two groups. In every group, the high bit-plane exchanges with the low bit-plane. Because it's major rule is bits exchange of inner pixel, this method, therefore is described to pixel based scrambling.

In this, Image is decomposed into several bit-plane images firstly. Then the scrambling of positions exchange of pixels in each bit-plane separately by the method mentioned in the reference is done. Finally, reconstruct the shuffled bit-plane images into a scrambled image. The same positions in different bit-planes do not stay on the original positions when each bit plane being scrambled separately. For each pixel, it's all bits of gray level, therefore; may come from those pixels located at different positions. Consequently, the reconstructed gray levels of image are changed inevitably. It is obvious that this method can do both positions exchange scrambling and gray level change scrambling at the same time. So, it can reach a good scrambling effect.

3. THE TECHNIQUES IMPLEMENTED

3.1 4TH LEVEL DIGITAL WATERMARKING

With regard to a still image that consists of a two-dimensional signal, it is to be decomposed into DWT pyramid structure with various frequency bands such that low-low frequency band, low-high frequency band, high-lowfrequency band and high-high frequency band components. DWT based watermarking algorithm of color images is proposed (Guangmin, 2007). In his scheme the RGB color space is converted into YIQ color space and watermark is embedded in Y and Q components. This method dealt with JPEG Compression attack and achieved good result. Watermarking using multi-resolution wavelet decomposition is proposed (Kundur, 1998). He decomposed the cover image into non overlapping multi-resolution discrete wavelet decomposition and used the decomposed level for watermarking. His scheme proved increased robustness of watermarked images and resist to most image processing attacks. A robust logo image watermarking is proposed (Hien, 2004). He used a binary logo as the watermark image. Independent Component Analysis is done for the images and then embedded with the logo watermark which proved high imperceptibility of watermarked images.

3.2 BIT PLANE ENCRYPTION OF IMAGE

Along with the rapidly popularization of e-commerce ande-government, a lot of multimedia information transmits and exchanges in network every day. Due to media, data (such as digital image, video etc.) are very easy to be intercepted illegally when they are transmitted in the network. Therefore, there is a great hidden trouble in the information security andits validity [12]. At present, there are two principle types of techniques to solve this trouble [1, 2]: the first is to encrypt the information, the second is to embed watermark into the digital multimedia data. The image scrambling is the first technique, which can shuffle an image through exchanging the positions of pixels and changing their gray levels or colors to aim at image encryption.

Now, there are many methods that can do scrambling [1-7], and the majority of them are scrambling algorithms based on pixel exchanging, which cannot change the histogram of an image [12]. Hence, their security performances are not good. Also, there is no scrambling algorithm that can give attention to both the pixel exchanging and gray level changing simply.

3.3 DCT (DISCRETE COSINE TRANSFORM)

The DCT is a very popular transform function used in signal processing. It transforms a signal from spatial domain to frequency domain. Due to good performance, it has been used in JPEG standard for image compression. DCT has been applied in many fields such as data compression, pattern recognition, and image processing, and so on.As an image transformed by the DCT, it is usually divided into non-overlapped m * m block. In general, a block always consists of 8´8 components [4]. The left-top coefficient is the DC value while the others stand for AC components. The zigzag scanning permutation is implied the energy distribution from high to low as well as from low frequency to high frequency with the same manner. The human eyes are more sensitive to noise in lower-frequency band than higher frequency. The energy of natural image is concentrated in the lower frequency range.

4. RESULTS AND DISCUSSIONS

The DCT, DWT, SVD and the proposed algorithm were all implemented using MATLAB. In order to evaluate the

DOI 10.17148/IJARCCE.2015.41297

performance of the proposed algorithm, a variety of different images were processed. Ten images are used for demonstration and numerical evaluation.

1

2

3

4

5

6

7

8

9

10

The parameters sed are as follows:

4.1 PEAK SIGNAL-TO-NOISE RATIO

The term peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible value of a signal and the power of distorting noise that affects the quality of its representation. Because many signals have a very wide dynamic range, (ratio between the largest and smallest possible values of a changeable quantity) the PSNR is usually expressed in terms of the logarithmic decibel scale. Image enhancement or improving the visual quality of a digital image can be subjective. Saying that one method provides a better quality image could vary from person to person [13].

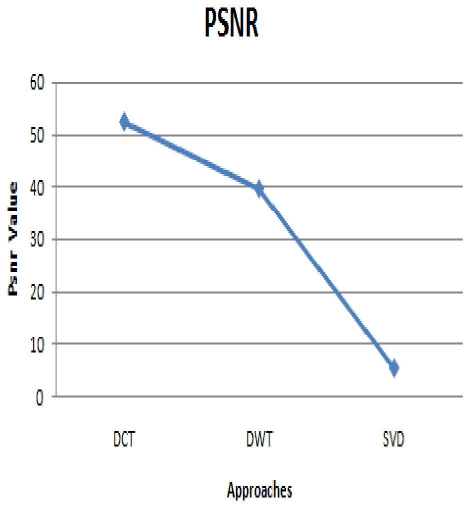

Fig 4.1 Graph for PSNR

This graph represents the average values of 10 images for PSNR between DCT, DWT, SVD and proposed work. Higher values will provide better results.

Image	DCT	DWT	SVD	Proposed
1	52.36	39.56	5.36	101.96
2	50.23	39.45	5.56	99.67
3	50.67	40.18	4.73	98.23
4	54.72	38.97	4.94	100.34
5	51.98	39.97	4.95	99.93
6	50.52	39.66	4.82	98.23
7	49.88	42.52	4.71	98.45
8	54.89	40.08	5.20	100.10
9	45.95	38.45	3.99	99.76
10	57.8	45.22	5.98	103.22

Table 4.1 Comparison table for peak signal-to-noise ratio (PSNR)

This table represents the value for PSNR using DCT, DWT and SVD watermarking approaches for various 10 images. Higher the values for PSNR better the performance of the watermarking technique.

4.2 MEAN SQUARE ERROR:

Mean square error (MSE) of an estimator measures the average of the squares of the "errors", that is, the difference between the estimator and what is estimated. MSE is a risk function, corresponding to the expected value of the squared error loss or quadratic loss. The difference occurs because of randomness or because the estimator doesn't account for information that could produce a more accurate estimate. The MSE is the second moment (about the origin) of the error, and thus incorporates both the variance of the estimator and its bias. For an unbiased estimator, the MSE is the variance of the estimator [3]. Like the variance, MSE has the same units of measurement as the square of the quantity being estimated. In an analogy to standard deviation, taking the square root of MSE yields the root-mean-square error or root-mean-square deviation (RMSE or RMSD), which has the same units as the quantity being estimated; for an unbiased estimator, the RMSE is the square root of the variance, known as the standard deviation.

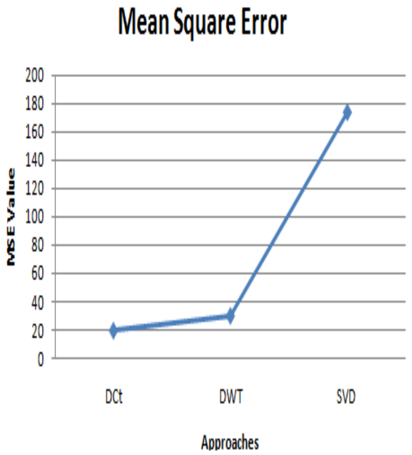

Fig 4.2 Graph for Mean Square Error

This graph represents the average values of 10 images for mean square error between DCT, DWT, SVD and proposed work. Lower values will provide better results.

Image	DCT	DWT	SVD	Proposed
1	19.8	30.25	173.4	8.82
2	18.27	30.49	178.56	5.3
3	19.99	32.83	181.25	4.82
4	19.54	30.94	178.88	4.73
5	19.87	30.77	180.39	4.26

DOI 10.17148/IJARCCE.2015.41297

6	17.99	31.84	170.36	3.67
7	17.95	32.09	172.99	3.98
8	18.67	31.88	170.78	5.02
9	18.49	32.69	174.24	4.4
10	17.01	30.99	180.25	3.01

Table 4.2 Comparison table for Mean Square Error (MSE)

This table represents the value for MSE using DCT, DWT and SVD watermarking approaches for various 10 images. Lower the value for MSE better the performance of the watermarking technique.

4.3 CORRELATION:

Degree and type of relationship between any two or more quantities (variables) in which they vary together over a period; for example variation in the level of expenditure or savings with variation in the level of income. A positive correlation exists where the high values of one variable are associated with the high values of the other variable. A negative correlation means association of high values of one with the low values of the other(s). Correlation can vary from +1 to -1. Values close to +1 indicate a high-degree of positive correlation, and values close to -1 indicate a high degree of negative correlation. Values close to zero indicate poor correlation of either kind, and 0 indicates no correlation at all.

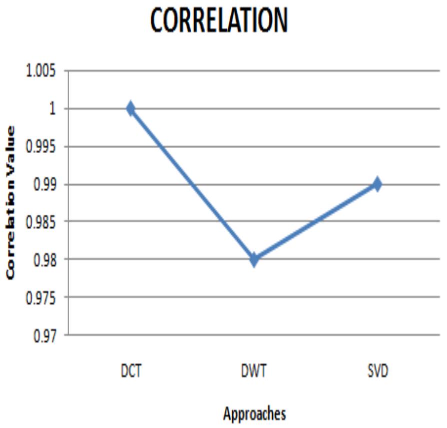

Fig 4.3 Graph for Correlation

This graph represents the average values of 10 images for Correlation between DCT, DWT, SVD and proposed work. . Values near to 1 will provide better results.

Image.	DCT	DWT	SVD	Proposed
1	1.00	0.98	0.99	0.99
2	0.99	0.98	0.97	0.99
3	0.98	0.99	0.98	0.99
4	0.99	0.98	0.98	0.99
5	0.99	0.98	0.98	0.99
6	0.99	0.99	0.97	0.99
7	1.00	0.98	0.98	0.98
8	0.99	0.99	0.98	0.99
9	0.99	0.98	0.97	0.99
10	1.00	0.99	0.99	0.98

Table 4.3 Comparison table for Correlation

This table represents the value for correlation using DCT, DWT and SVD watermarking approaches for various 10 images. Values near to 1 will provide better results.

4.4 SSIM:

The structural similarity (SSIM) index is a method for measuring the similarity between two images. The SSIM index is a full reference metric; in other words, the measuring of image quality based on an initial uncompressed or distortion-free image as reference. SSIM is designed to improve on traditional methods like peak signal-to-noise ratio (PSNR) and mean squared error (MSE), which have proven to be inconsistent with human eye perception.

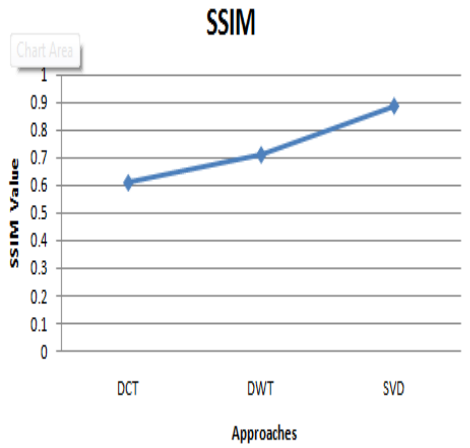

Fig 4.4 Graph for SSIM

This graph represents the average values of 10 images for SSIM between DCT, DWT, SVD and proposed work. . Values near to 1 will provide better results.

Image	DCT	DWT	SVD	Proposed
1	0.611	0.711	0.885	0.932
2	0.658	0.734	0.828	0.908
3	0.623	0.656	0.796	0.900
4	0.600	0.683	0.889	0.932
5	0.558	0.799	0.817	0.911
6	0.721	0.801	0.798	0.971
7	0.599	0.699	0.801	0.967
8	0.689	0.765	0.899	0.928
9	0.512	0.798	0.862	0.955
10	0.546	0.723	0.851	0.917

Table 4.4 Comparison table for structural similarity (SSIM) index

This table represents the value for SSIM using DCT, DWT and SVD watermarking approaches for various 10 images. Closer the value of SSIM to 1 better is the performance of the watermarking technique.

5. CONCLUSION

From the above discussions it is concluded that the proposed technique is less prone to errors and watermarks the image accurately. Digital watermarking is the process of hiding the secret data behind any image or signal. This paper comprises of the various phases that are explained in

DOI 10.17148/IJARCCE.2015.41297

this way. In first phase the cover image is reflected behind which data has to be hidden. After this discrete wavelet transformation is implemented to that image which divides the image into four different resolution regiments. This transformation is implemented up to fourth level. In the next phase secret image is reflected which has to be encrypted using bit phone encryption approach and that has to be embedded behind the cover image extracted region.

REFERENCES

[1] Tripathi S., Jain R.C. and Gayatri V.,"Novel DCT and DWT based watermarking techniques for digital images", 2006, IEEE.

[2] Song Y.J. and Jain T.N., "comparison of four different digital watermarking techniques", 2007, IEEE.

[3] Oueslati S., Cherif A. and Solaimane B.," Adaptive image watermarking scheme based on neural network ", Vol. 3 No. 1 Jan 2011, IJEST.

[4] Chiou-Ting H. and Ja-Ling W., "Hidden digital watermarks in image", vol.8, No 1, 1999, IEEE transactions on image processing.

[5] Potdar V.M., Han S. and Chang E., "A survey of digital watermarking techniques", 2005, IEEE International conference on industrial informatics

[6] Jianghua Cao "Study on multiple watermarking scheme for GIS vector data" 18th International Conference onGeoinformatics, 2010, pp. 1 – 6.

[7] Qing Liu, Jun Ying "Grayscale image digital watermarking technology based on wavelet analysis" Symposium onElectrical & Electronics Engineering (EEESYM), 2012, pp. 618 – 621.

[8] Zhang Fan, ZhangHongbin "Capacity and reliability of digital watermarking" International Conference onBusiness of Electronic Product Reliability and Liability, 2004, pp. 162 – 165.

[9] Fang Ma, JianPing Zhang, Wen Zhang "A Blind Watermarking Technology Based on DCT Domain" International Conference on Computer Science & Service System (CSSS), 2012, pp. 397 – 400.

[10] Jiang-bin Zheng, Sha Feng "A color image multi-channel dwt domain watermarking algorithm for resisting geometric attacks" International Conference on Machine Learning and Cybernetics, 2008, vol. 2,pp. 1046 – 1051.

[11] Jingbing Li, Fan Wu "Robust watermarking for text images based on Arnold Scrambling and DWT-DFT" International Conference onMechatronic Sciences, Electric Engineering and Computer (MEC), Proceedings 2013 ,pp. 1182 – 1186.

[12] Zhang Fan, Zhang Hongbin "Capacity and reliability of digital watermarking" International Conference onBusiness of Electronic Product Reliability and Liability, 2004, pp. 162 – 165.

[13] Tang Lei,GaoZhinian,Sun Peng "A Rotation Resistant Image Watermarking Algorithm via Circle" Eighth International Conference onComputational Intelligence and Security (CIS), 2012, pp. 461 – 463.

[14] Steinebach, M., Hauer, E., Wolf, P. "Efficient Watermarking Strategies" Third International Conference onAutomated Production of Cross Media Content for Multi-Channel Distribution, 2007, pp. 65 – 71.

[15] Fan Zhang, Hongbin Zhan "Digital watermarking capacity research" International Conference on Communications, Circuits and Systems, 2004, vol. 2. ,pp. 796 - 799.

[16] Afroja Akter, Nur-E-Tajnina, and Muhammad Ahsan Ullah" Digital Image Watermarking Based on DWT-DCT Evaluate for a New Embedding Algorithm", 3rd international conference on informatics, electronics & vision 2014.

[17] Qiudong Sun, Wenying Yan, Jiangwei Huang, Wenxin Ma," Image Encryption Based on Bit-plane Decompositionand Random Scrambling", Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference,pp 2630 – 2633

DOI 10.17148/IJARCCE.2015.41297