World Journal of Computer Application and Technology 1(2): 35-40, 2013 http://www.hrpub.org
DOI: 10.13189/wjcat.2013.010203

Comparative Analysis of Blind Digital Image Watermarking Utilising Dual Encryption Technique in Frequency Domains

Gursharanjeet Singh Kalra[1,*], Rajneesh Talwar[2], Harsh Sadawarti[3]

[1]Lovely Professional University, Punjab, India
[2]CGC- College of Engineering, Punjab Technical University, Jalandhar, Punjab, India
[3]RIMT Institute of Engg. & Technology, Punjab Technical University, Jalandhar, Punjab, India
*Corresponding Author: gursharanjeetkalra@yahoo.com

Abstract Piracy in the presence of internet and computers proves to be a biggest jolt to the concerned industry. To reduce the piracy and duplicity of the images, digital watermarking technique is having an edge over the other available techniques. In this paper, a blind digital watermarking algorithm is presented which is robust enough to resist the watermark against the attacks. The algorithm exploits the random sequence generated by Arnold and Chaos transformations. Discrete wavelet transformation of third level decomposition is used to convert the image into its frequency domain. In another transformation, the image is converted into frequency domain by using DCT and DWT combined. The binary watermark is embedded into its HL3 domain. The evaluation of the algorithm is calculated in terms of peak signal to noise ratio and non correlation. The results prove that the algorithm is robust enough to handle the attacks like JPEG, filtering, and different types of noise attacks.

Keywords Watermarking, Image, DWT, DCT, Frequency domain Robust, Blind

1. Introduction

Now days the growth of internet is so fast that it is penetrating in the remote areas. It is even present where the person needs hard work to reach such areas [1], the data can be easily transferred to the other person in just a single click, with the reducing time for outdoor entertainment.

Due to busy lifestyle, the only source of entertainment is television or computers. But, if someone is getting the entertainment on computer just like television then it will be great option for everyone. The digital representation of media files possesses advantages of portability, efficiency and accuracy of information content. This is the reason that piracy is in full swing. Everybody wants latest images, audio files or video files and they are getting it on the internet, free of cost. The original producer of the file even doesn't know that the file created by him/her is available for free through internet and even if knows, nothing can be done. Here is the point, when the need of some method comes in so that the actual producer can prove that the file belongs to him/her.

There are many solutions for this problem like Steganography cryptography and digital watermarking. Digital watermarking is intended to complement cryptographic process [2] and steganography. Later technique facilitates the access of encrypted data only to them who have valid key but fails to track any reproduction or retransmission of data after decryption. But, in digital watermarking, a specific code or mark is embedded permanently inside a cover multimedia file which remains within that cover invisibly or visibly even after decryption process. Digital watermarking is the process that embeds data, called a watermark, into a multimedia object in such a manner that the watermark can be detected or extracted later to make a decision about the copyright of the object. In digital watermarking, a specific code or mark is embedded permanently inside a cover multimedia file which remains within that cover invisibly or visibly even after decryption process.Watermark must have the following characteristics:

1) *Imperceptibility.* The watermark must not degrade the image or multimedia file but also retains in the file so that it must be invisible, until and unless required to be visible.

2) *Security.* The watermarking method should be in such a way that it uses some private key or encryption with keys.

3) *Robustness.* The embedded watermarks should not be removed or eliminated by unauthorized distributors using common processing techniques including; compression, filtering, cropping, quantization and others.

4) *Adjustability.* The algorithm should be tuneable to various degrees of robustness, quality, or embedding capacities to be suitable for diverse applications.

5) *Real-time processing.* Watermarks should be rapidly embedded into the host signals without much delay.

There are several methods of embedding the watermark. The watermark can be embedded in spatial or frequency domain. Generally, frequency domain watermarking is more robust than the spatial domain. DCT and DWT are the methods by which an image can be converted into frequency domain. In some of the techniques, watermark is embedded by using combined DCT and DWT methods. In this paper, we have implemented our watermarking algorithm using DCT and DWT combined to exploit the benefit of targeting the particular range of frequencies to embed the watermark.

This paper is organized as follows: section-II presents review of the literature survey on the algorithms using DCT, DWT and combined DCT-DWT technique. Section-III illustrates proposed scheme including techniques used in the paper, embedding procedure and extraction procedure. Section-IV presents the parameters to evaluate the watermarked image, the extracted watermark and the bit error rate. In section-V, Results are presented and thereafter a small discussion is presented. Section-VI is the conclusion on the paper.

2. Related Works

There are certain techniques which uses DWT to convert the cover image into its frequency domain. In paper [3], authors implemented their algorithm on contourlet transform as well as wavelet transform and found that their algorithm is robust in the former case. Authors of [4], uses lifting wavelet and Henon chaos for the encryption of watermark. Chaos has irregular movement which looks like random and occurs in a deterministic system. Although chaos is a deterministic describing system, its behaviour is uncertain. The method is invisible and robust against some usual attacks such as JPEG, cropping, adding noise and filtering. Based on DWT, DCT and SVD, authors [5] proposed a new watermarking algorithm for digital images. Their results show that the algorithm combines the advantages of these three transforms. It can satisfy the imperceptibility and robustness very well but for few attacks like jpeg. In [6], information of digital watermarking which has been discrete Cosine transformed, is put into the high frequency band of the image which has been wavelet transformed. Then, distils the digital watermarking with the help of the original image and the watermarking image. In [7], authors verified that the combination of the two transforms improved the watermarking performance considerably when compared to single watermarking techniques. In general, combining more than one digital watermarking technique; especially in transformed domain, highly improves both robustness and capacity of watermarking. In [8], authors proposed a watermarking algorithm for color image based DCT and DWT. A binary image as watermark was embedded into green component or blue component of color image. The algorithm can satisfy the transparence and robustness of the watermarking system very well. In [9], the proposed algorithm has been developed to take advantage of both spatial as well as frequency domain properties. This is due to the fact that spatial domain watermarking has advantage of less computational cost and frequency domain watermarking provides more robustness. Authors in [10] presented a blind low frequency watermarking scheme on gray level images, which is based on DCT transform and spread spectrum communications technique. In this method, they achieved higher because of embedding the watermark in low frequency. In addition, higher imperceptibility was gained by scattering the watermark's bit in different blocks. In [11], during the embedding of the watermarking, discrete wavelet transform is done firstly and extracted the low frequency part as the embedding field; then the chaotic sequence was used to encrypt the watermark and transform the encrypted part and extract the low frequency; finally, authors embedded the low frequency part into that of the original image. Authors extracted the watermark non-blindly. In [12], authors used a watermarking sequence encrypted by Arnold transformation with secret keys afterwards embedded into the DCT transform coefficients according to JND (Just Noticeable Difference) model. The watermark is extracted without the original image. The authors in [13], described an imperceptible and a robust combined DWT-DCT digital image watermarking algorithm. The algorithm watermarked a given digital image using a combination of the Discrete Wavelet Transform (DWT) and the Discrete Cosine Transform (DCT). Performance evaluation results show that combining the two transforms improved the performance of the watermarking algorithms that are based solely on the DWT transform. The authors in [14], proposed a perceptual image hashing scheme that they showed secure and robust to visually insignificant changes but fragile enough to detect and precisely locate malicious attacks. The proposed image hashing method was based on the outlines of one-dimensional signals re-arranged from the 8×8 DCT blocks. The final image hash was obtained by applying binary quantization to the DWT coefficients of the obtained 1-D signals.

The proposed scheme

In the proposed scheme, the watermark is embedded in DWT domain and combined DCT-DWT domain.

A Discrete CosineTransform

Discrete Cosine Transform (DCT) have the advantage over the other domains like, spatial and DWT. It is more robust against the attacks specifically jpeg lossy compression because of its energy compaction property. Two Dimensional Discrete Cosine Transform(2D-DCT) can be calculated as given in Eq. 1. After applyying Eq. 1-2-D image blocks of size 8X8 pixels, DC component will be aligned to one corner and rest of the AC components will be aligned to the rest of the block in the zig-zag fashion.

B. Wavelet Transform

Discrete wavelets transform is a method of signal analysis theory which has arisen in recent years. It is a frequency domain analysis method which can localize frequency domain and has widely used in many fields. The basic idea of DWT is the detailed frequency separation of signal, namely

multi-resolution decomposition. The host image is decomposed to four sub-images in size of one quarter: one low frequency approximating image and three medium and high frequency detail sub-images in horizontal, vertical and diagonal direction. The three level decomposition of discrete wavelet transform is shown in fig 1.

On the basis of discrete wavelets theory and human visual characteristics, we know that the embeddable watermarking capacity will decrease with the increase of layer numbers. The high frequency part of discrete wavelets represents the edge, outline and texture information and other detail information. Embedding watermark is difficult to be detected in these parts, but it is easy to be destroyed and has a poor stability after image processing. The low frequency part concentrates the most energy of image; the amplitude of coefficient is larger than the one of detail sub-graph.

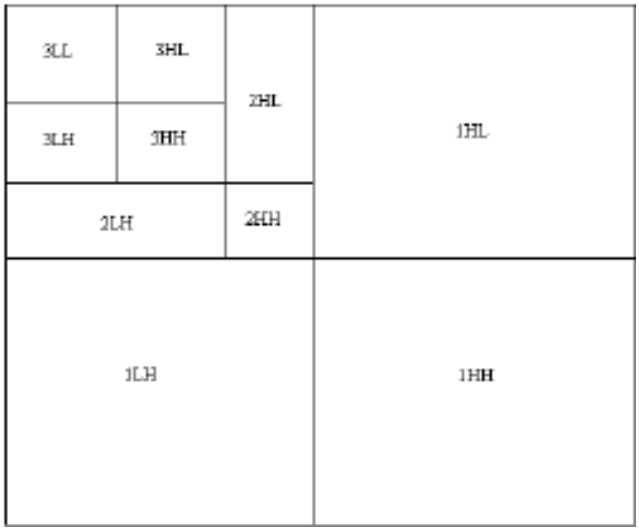

Figure 1. Three level wavelet decomposition

The brightness masking on human visual model shows that the larger the background brightness, the more the just noticeable difference of embeddable signal [10], which means low frequency approximate image can be embedded by more watermarking capacity, provided that embeddable watermarking capacity is lower than JND, as human eyes cannot suspect the existence of signal. Some common attacking to low frequency coefficients are almost invariant, even if some attacks have more effect on low frequency coefficients, the host image is also destroyed. So it is good to embed watermark in medium and low frequency.

B. Arnold Transform

Arnold transformation is posed in the research of Arnold theory. Assume that a cat face is drawn in a planar unit square and transformed by (1):

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \left[\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod1 \right] \quad (1)$$

Arnold transformation defined by (1) is a one-to-one transformation. From the view of sampling theory, digital images can be viewed as a matrix of 2D discrete points derived from sampling according to a certain interval and a certain method. Square matrix of digital images can be made discrete by Arnold transformation.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \left[\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} modN \right] \quad (x,y)\epsilon\ 0,1\ldots\ldots,N\text{-}1 (2)$$

Equation (2) is used to transform each and every pixel coordinates of the images. When all the coordinates are transformed, the image we obtain is scrambled images. In addition, when one digital image is transformed by Arnold transformation, the transforming process can be achieved continually. At a certain step of iteration, if the image we achieve reaches our anticipated target, we have achieved the scrambled image we need. The decryption of image relies on the transformation periods. The periods change in correspondence to the size of images. The iteration periods is 96 for a 128×128 image; 48 for a 64×64 image. Here the number that images are scrambled is used as an encryption key and modulated by binary pseudo random sequence, which further strengthens the security of watermark. Due to its pseudo random and the pseudo random of binary sequence, attackers can hardly detect the watermark without first knowing the pseudo random sequence.

C. Chaotic encryption

Chaos signals are a kind of pseudorandom, irreversible and dynamical signals, which process good characteristics of pseudorandom sequences. Chaotic systems are highly sensitive to initial parameters. The output sequence has good randomness, correlation, complexity and is similar to white noise. Chaotic sequence has high linear complexity and non predictability. The model [11] here is chaos 1-D Logistic and is shown in (3).

$$x(n+1) = \mu * x(n) * [1-x(n)] \quad (3)$$

Where $\mu \in (0,4)$; $x(n) \in (0,1)$. By initializing μ and x(0), we can get the required chaotic signal. In order to get chaotic sequences, the chaotic signal x(*n*) must be transformed into binary sequence *s*(*n*) . So quantized function *T*[x(*n*)] is used and can be given by (4).

$$T[x(n)] = \begin{cases} 0 & x(n)\epsilon \bigcup_{k=0}^{2^{m-1}} I_{2k}^{m} \\ 1 & x(n)\epsilon \bigcup_{k=0}^{2^{m-1}} I_{2k=1}^{m} \end{cases} \quad (4)$$

Where m is random integer and should be greater than 0. $(I_0^m, I_0^m, \ldots\ldots)$.is continuous equal interval in [0,1] and the interval is divided by 2^m . If the value is in the odd interval of the quantized function, the quantized value is 1, or else, the quantized value is 0. The binary sequences generated were of good pseudorandom sequence characteristics. Chaotic key sequence are XORed by binary image, generated the encrypted watermark image.

D. Watermarking Embedding algorithm

The flow diagram of embedding process is shown in fig.2. The steps in the process of embedding are follows:

1. Take the original image and resize it to 1024X1024 image. Make three-level wavelet decomposition of the original image and the frequency band HL3 as the embedded

domain, the wavelet coefficient of HL3 extracted as *CH*3. In case of combined DCT-DWT, first apply DWT, then take HL1 component of the resultant and the apply 8X8 DCT.

2. Take the watermark and resize it to 32X32 bit binary image.

3. Then apply the Arnold transformation to the watermark.

4. After the Arnold transformation, apply the Chaoss transformation to the output of Arnold transformed watermark.

5. Perform the embedding of the watermark in the original image as given in (5) below:

$$X_w = \begin{cases} \frac{+\sigma^2}{\alpha} & ,if\ wk = 1 \\ \frac{-\sigma^2}{\alpha} & ,if\ wk = 0 \end{cases} \quad (5)$$

Where, Xw is the watermarked image before inverse DWT/DCT-DWT. Wk is the watermark bit at k'th position and k=0,1,2,……..1023.

σ^2 is the standard deviation of the original image and α is the depth of the watermark to be embedded.

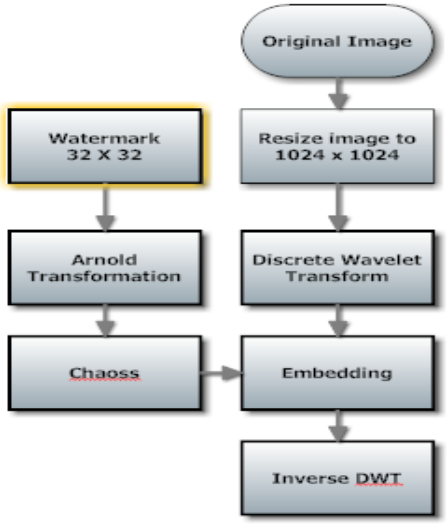

Figure 2. Embedding algorithm

6. Take the inverse DWT/DCT-DWT to get the watermarked image and resize it to 256 X 256 image.

E. Watermarking Extraction algorithm

The flow chart for watermarking extraction algorithm is shown in fig. 3. The steps involved in extraction algorithm are given below:

1. Take the watermarked image and resize it to 1024 X 1024 image.

2. Then take the DWT upto 3 level decomposition and mark the frequency band HL3 as CH3 to extract the watermark.

3. Extract the watermark from CH3 as given in (6) below:

$$w_k = \begin{cases} wk = 1 & ,if\ Xw(i+4, j+4) = \frac{+\sigma^2}{\alpha} \\ wk = 0 & ,if\ Xw(i+4, j+4) = \frac{-\sigma^2}{\alpha} \end{cases} \quad (6)$$

Where, Xw is the pixel where watermark was embedded.

wk is the extracted watermark bit.

4. Take the inverse Chaoss transformation of the extracted watermark.

5. Take the inverse Arnold transformation of the reverse Chaoss image to get the desired extracted watermark.

Performance Evaluation

The performance of the watermarked image can be evaluated on the basis of peak signal to noise ratio (PSNR) in decibels (dB). Higher the value of PSNR better is the quality of the watermarked image. PSNR more than 30 dBs is considered to be the acceptable quality image in which watermark is making no alteration to the quality of the image.

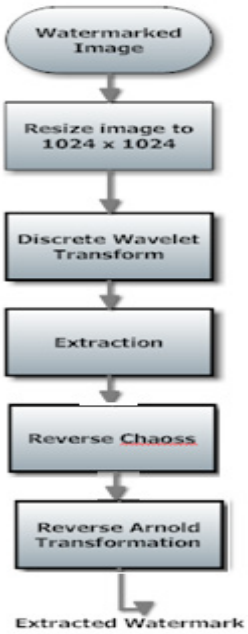

Figure 3. Extraction algorithm

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 \quad (7)$$

$$PSNR = 10 \log_{10} \left(\frac{R}{MSE}\right) \quad (8)$$

Where, MSE is the mean square error of the watermarked image and the original image and m, n are the number of rows and number of columns. I and K are the watermarked images.

The quality of the extracted watermark is evaluated using term Normalized cross-correlation (NC). The ideal value of the NC is 1 which means the original and the extracted watermarks are exactly the same which is given by the (9):

$$NC = \frac{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} W(i,j) * W'(i,j)}{\sqrt{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} W(i,j)^2} \sqrt{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} W'(i,j)^2}} \quad (9)$$

The bit error rate (BER) can be calculated as given in (10).

$$BER = \frac{\sum_{1}^{m*n} w(i) EXOR\ w'(i)}{m*n} \quad (10)$$

Where *W*(i,j) is the original watermark and *W'*(i,j) is the extracted watermark.

3. Results and Discussions

The image used is 256 X 256 Cameraman and the watermark image used is a 32 X 32 binary image shown in fig.4(a). Encrypted watermark after Arnold and Choss encryption is shown in fig. 4(b). The values of PSNR, NC and BER without attack are given in Table. I.

Figure 4. (a) Original Watermark (b) Encrypted Watermark

Table 1. PSNR (db)

Image	DWT	DCT-DWT [12]
Lena	40.44	43.03
Cameraman	40.43	40.92
Baboon	40.28	35.68
Peppers	40.47	42.70

Different types of attacks are performed and tabularized below in Table II. Watermarks extracted after attacks are shown in fig. 5 in case of DWT.

Table 2. Results in PSNR After Attacks on Lena Image

Attack	Depth	DWT	DCT-DWT [12]
JPEG (Quality)	50%	39.72	44.86
	80%	39.80	45.76
	90%	40.17	45.11
Gaussian Filter	3 X 3	41.06	42.97
	7 X 7	40.88	42.67
Median Filter	3 X 3	42.98	47.2
	5 X 5	41.75	44.39
Gaussian Noise (Mean =0.01)	Var=0.01	20.23	20
	Var=0.02	17.41	17.14
Salt & Pepper Noise	0.01	24.92	25.34
	0.02	22.01	22.43
	0.04	19.03	21.71
	0.05	18.07	18.43
Speckle Noise	0.01	25.48	25.62
	0.02	22.55	22.65
	0.04	19.57	19.75
	0.06	17.85	18.08

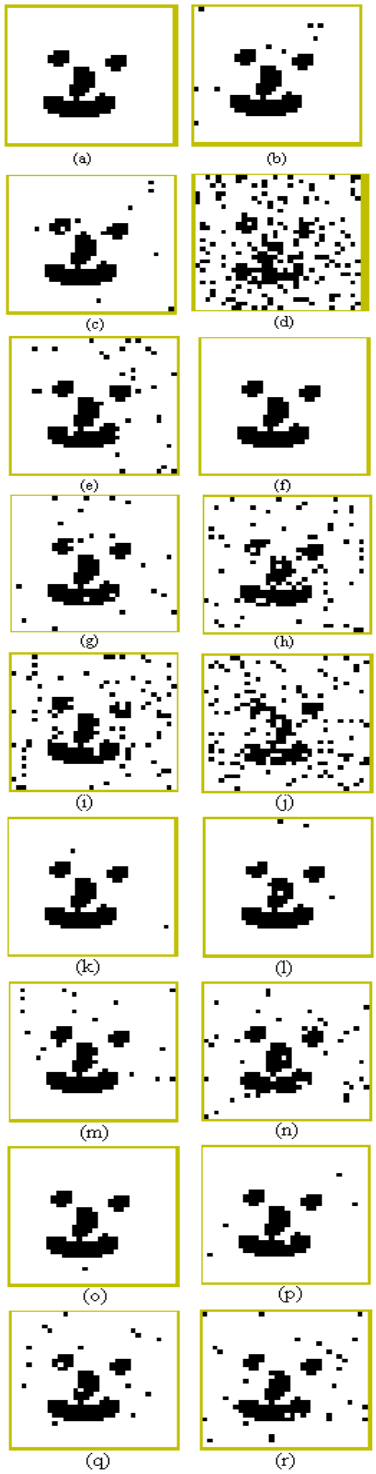

Figure 5. Extracted watermark after attack in DWT domain (a) JPEG (QF30%) (b) JPEG (QF=10%) (c) Median filter 3X3 (d) Median filter 5X5 (e) Median filter 7X7 (f) Gaussian noise Mean=0.01, Var=0.01 (g) Gaussian noise Mean=0.01, Var=0.01 (h) Gaussian noise Mean=0.01, Var= 0.02 (i) Gaussian noise Mean=0.01, Var=0.04 (j) Gaussian noise Mean=0.01, Var=006 (k) S & P noise 2% (l) S & P noise 4% (m) S & P noise 5% (n) S & P noise 10% (o) Speckle noise 2% (p) Speckle noise 4% (q) Speckle noise 6% (r) Speckle noise 8%

The PSNR values of the combbined DCT-DWT domain are quite more than the only DWT domain

4. Conclusions

In this paper, we analysed blind watermarking algorithm based on Arnold-Chaos encryption with discrete wavelet transform and combined discrete cosine transform-discrete wavelet transform. The pseudo-random sequence generated by Arnold and chaos system possesses feature of very high randomness, so the watermark become more secure. The parameter of embedding the watermark, α, is introduced with inverse property. Which means that lower the value of alpha, more will be the depth of the watermark and vice-versa. So the contradiction between transparency and robustness can be settled easily, which brings the algorithm higher application oriented. The watermark embedding algorithm can efficiently resist attacks like JPEG with quality factor as low as 10%, Gauss low pass filter, salt & Pepper noise, speckle noise and median filtering. But the ability of resistance of Gaussian noise and median filtering attack is weaker which shows that a further research is needed in this field.

REFERENCES

[1] "InternetUsers",http://data.worldbank.org/data-catalog/world-development-indicators?cid=GPD_WDI, 'internet users'.

[2] J.A. Bloom, U. Cox, T. Kalker, J.M.G. Linnartz, M.L. Miller, C.B.S. Traw, "Copy Protection for DVD Video" in Proceedings of the IEEE, vol. 87, pp 1267,1272-1275, July 1999.

[3] Shereen Ghannam, Fatma E. Z. Abou-Chadi, "Contourlet Versus Wavelet Transform: A Performance Study for a Robust Image Watermarking", icadiwt-09, UK, pp.545-550.

[4] Zheng-Wei Shen, Wei-Wei Liao, Ya-Nan Shen, "Blind Watermarking Algorithm Based On Henon Chaos System And Lifting Scheme Wavelet", International Conference on Wavelet Analysis and Pattern Recognition, Baoding, 12-15 July 2009, pp.308-313.

[5] Ben Wang, Jinkou Ding, Qiaoyan Wen, Xin Liao, Cuixiang Liu, "An Image Watermarking Algorithm Based on DWT DCT And SVD", IEEE International Conference on Network Infrastructure and Digital Content, China, 2009, pp.1034-1038.

[6] Mei Jiansheng, Li Sukang, Tan Xiaomei, "A Digital Watermarking Algorithm Based On DCT and DWT", International Symposium on Web Information Systems and Applications, 2009, China, pp.104-107.

[7] Mohamed A. Mohamed, Mohy EI-Din A, Abou-Soud, Mai S. Diab, "Fast Digital Watermarking Techniques for Still Images", 2009 International Conference on Networking and Media Convergence, Cairo, Egypt, 2009, pp.122-129.

[8] Fan Zhao, Guizhong Liu, Feifei Ren, "Adaptive Blind Watermarking for JPEG2000 Compression Domain", Image and Signal Processing, 2009, Hawaii, USA.

[9] Fang Wang-sheng, Chen Kang, "A wavelet watermarking based on HVS and watermarking capacity analysis", International Conference on Multimedia Information Networking and Security, China, 2009, pp.141-144.

[10] Li Yushen, Hao Yanling, Wang Chenye, "A Research on the Robust Digital Watermark of Color Radar Images", IEEE International Conference on Information and Automation, China, 2010, pp. 1091-1096.

[11] Qiang Wang, Qun Ding, Zhong Zhang, Lina Ding, "Digital Image Encryption Research Based on DWT and Chaos", Fourth International Conference on Natural Computation, 2008,pp.494-498

[12] Kalra G.S., R. Talwar and H. Sadawarti, 2012. Blind digital image watermarking robust against histogram equalization. J. Comput. Sci. 8: 1272-1280.