Journal of Computer Science 8 (8): 1272-1280, 2012
ISSN 1549-3636

Blind Digital Image Watermarking Robust Against Histogram Equalization

[1]Kalra, G.S., [2]R. Talwar and [3]H. Sadawarti
[1]Lovely Faculty of Technology and Sciences,
Lovely Professional University Punjab, India
[2]Department of Electronics and Communication,
[3]Department of Computer Science,
RIMT, Punjab Technical University, Punjab, India

Abstract: Problem statement: Piracy in the presence of internet and computers proves to be a biggest damage to the industry. Easy editing and copying of images yields a great damage to the owner as original images can be distributed through internet very easily. To reduce the piracy and duplicity of the digital multimedia files, digital watermarking technique is dominating over the other available techniques. There are certain methods or attacks which are used to damage the watermark. One of the major attacks is histogram equalization and reducing the number of histogram equalized levels. Thus, there is a need to develop a method so that the watermark can be protected after histogram equalization. **Approach:** A blind digital watermarking algorithm is presented which embed the watermark in frequency domain. Firstly, DWT is applied on the original image and then DCT on the 4×4 blocks to target the particular frequencies of the image for embedding the watermark which does not have more effect after histogram equalization. Also, to enhance the security of the watermark dual encryption technique is deployed. **Results:** Algorithm applied to four images which are Lena, Cameraman, Baboon and Peppers. 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 to histogram equalization attack up to 2 grey levels. **Conclusion/Recommendations:** The developed algorithm proved its performance against histogram equalization but the algorithm can also be checked for the other attacks which can be addition of white noise, Gaussian noise, filtering.

Key words: Watermarking, image, dwt, frequency domain robust, blind, histogram equalization

INTRODUCTION

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 penetration of internet in the wolrd population is shown in Fig. 1. 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.

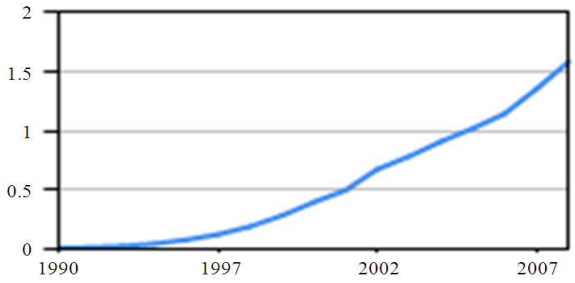


Fig. 1: Internet Users (in billions)

Digital watermarking is intended to complement cryptographic process (Bloom, 1999) and Steganography. 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 characteristics like Imperceptibility, Security, Robustness, Adjustability and Real-time processing.

Corresponding Author: Kalra, G.S., Lovely Faculty of Technology and Sciences, Lovely Professional University Punjab, India

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.

Related works: There are certain techniques which uses DWT to convert the cover image into its frequency domain. In paper (Ghannam and Abou-Chadi, 2009), 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 (Shen *et al*., 2009), 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 (Wang *et al*., 2009) 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 another paper (Jiansheng *et al*., 2009), 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 the study (Mohamed *et al*., 2009), 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 another paper (Yang and Jin, 2009), authors proposed a watermarking algorithm for colour image based DCT and DWT. A binary image as watermark was embedded into green component or blue component of colour image. The algorithm can satisfy the transparency and robustness of the watermarking system very well. In the study (Joshi and Darji, 2009), 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 (Taherinia and Jamzad, 2009) 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 the study (Wang *et al*., 2008), 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 study (Na *et al*., 2009), authors used a watermarking sequence encrypted by Arnold transformation with secret keys afterwards embedded into the DCT transform coefficients according to Just Noticeable Difference (JND) model. The watermark is extracted without the original image. The authors in (Al-Haj, 2007), 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 (Zhan *et al*., 2008), 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.

MATERIALS AND METHODS

The proposed scheme is made up after concluding the literature survey. It utilizes the advantages of wavelet transform, Arnold Transform and Chaoss. Two encryption techniques are used to enhance the security of the watermark.

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 (Yushen *et al*., 2010). 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:

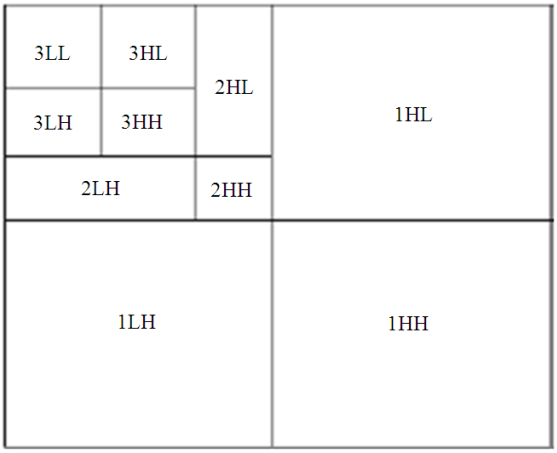


Fig. 2: Three level wavelet decomposition

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. 2.

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 (Yushen *et al*., 2010). 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.

The brightness masking on human visual model shows that the larger the background brightness, the more the just noticeable difference of embeddable signal (Yushen *et al*., 2010), 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.

Discrete cosine transform: 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 (Rao and Yip, 1990). 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 alligned to one corner and rest of the AC components will be alligned to the rest of the block in the zig-zag fashion:

$$F(jk) = a(j)a(k)\sum_{m=0}^{N-1}\sum_{n=0}^{N-1} f(mn)\cos\left[\frac{(2m+1)j\pi}{2N}\right]\cos\left[\frac{(2m+1)k\pi}{2N}\right] \quad (1)$$

Arnold transform: Arnold transform is commonly known as cat face transform. Arnold transformation defined by Eq. 2 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:

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

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \left[\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} \bmod N\right] (x,y) \in 0,1.....,N-1 \quad (3)$$

Equation 3 is used to transform each and every pixel coordinates of the images. Where (x, y) is the location coordinates of the original image pixels and (x', y') is the location coordinates of image pixels that after transform 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.

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.

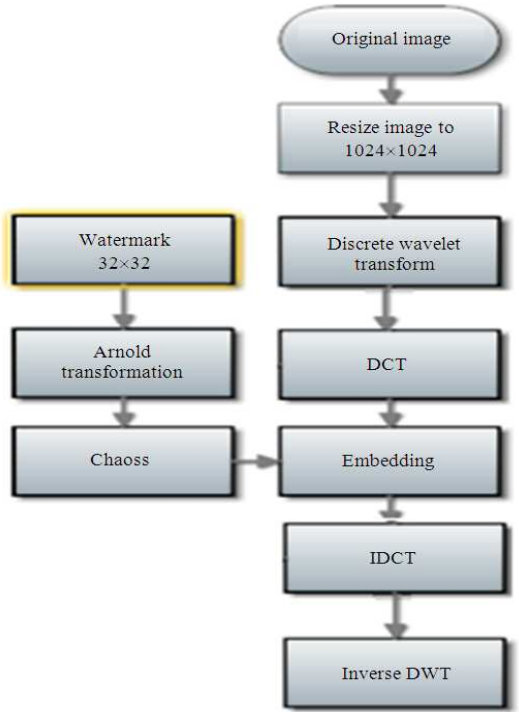


Fig. 3: Embedding algorithm

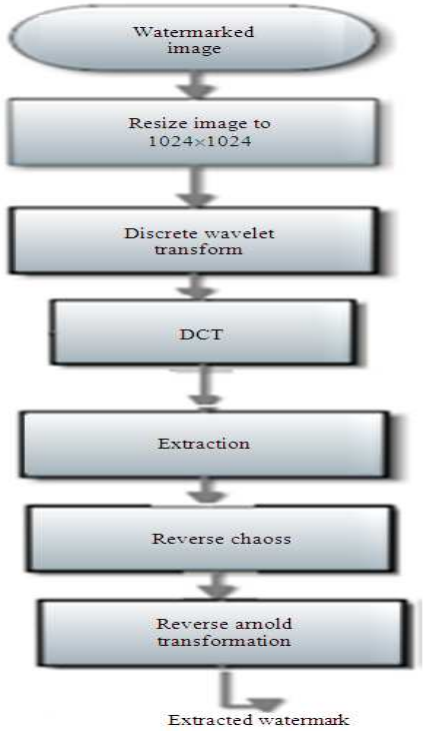


Fig. 4: Extraction algorithm

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 (Wang *et al*., 2008) here is chaos 1-D Logistic and is shown in Eq. 4:

$$x(n+1) = \mu * x(n) * [1-x(n)] \quad (4)$$

where $\mu \in (0, 4)$; $x(n) \in (0, 1)$. By initializing μ and $x(0)$, we can get the required chaotic signal. Randomness will be maximum with values of μ between 3.7 to 3.99. 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 Eq 5.

$$T[x(n)] = \begin{cases} 0 & x(n) \in \bigcup_{k=0}^{2^{m-1}} I_{2k}^{m} \\ 1 & x(n) \in \bigcup_{k=0}^{2^{m-1}} I_{2k=1}^{m} \end{cases} \quad (5)$$

Where m is random integer and should be greater than $0.(I_0^m, I_0^m, ...)$. 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.

Watermarking embedding algorithm: The flow diagram of embedding process is shown in Fig. 3. The steps in the process of embedding are follows:

- Take the original image and resize it to 1024×1024 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 CH3
- Take the DCT of sub size 4×4
- Take the watermark and resize it to 32×32 bit binary image
- Then apply the Arnold transformation to the watermark
- After the Arnold transformation, apply the Chaoss transformation to the output of Arnold transformed watermark
- Perform the embedding of the watermark in the original image as given in Eq. 6.

$$X_W = \begin{cases} \frac{+\sigma^2}{\alpha} & ,\text{if } wk = 1 \\ \frac{-\sigma^2}{\alpha} & ,\text{if } wk = 0 \end{cases} \quad (6)$$

Where, Xw is the watermarked image before inverse 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.

Take the inverse DCT and then take the inverse DWT to get the watermarked image and resize it to 256×256 image.

Watermarking extraction algorithm: The flow chart for watermarking extraction algorithm is shown in Fig. 4. The steps involved in extraction algorithm are given below:

- Take the watermarked image and resize it to 1024×1024 image
- Then take the DWT up to 3 level decomposition and mark the frequency band HL3 as CH3 to extract the watermark
- Take the DCT of sub size 4×4
- Extract the watermark from CH3 as given in Eq. 7 below:

$$W_k = \begin{cases} Wk = 1 & \text{,if } Xw(i+4, j+4) \geq 0 \\ Wk = 0 & \text{,if } Xw(i+4, j+4) < 0 \end{cases} \quad (7)$$

where, Xw is the pixel where watermark was embedded. wk is the extracted watermark bit:

- Take the inverse Chaoss transformation of the extracted watermark
- 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) as given in Eq. 9. 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:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[I(i,j) - K(i,j)\right]^2 \quad (8)$$

$$PSNR = 10\log_{10}\left(\frac{R}{MSE}\right) \quad (9)$$

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. It can be given as in Eq. 8. If vlues of the pixels are 8-bit binary then R will be 255 and if pixels values are having range 0-1 then value of R will be 1.

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 Eq. 10:

$$NC = \frac{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} W(i,j) * W'(i,j)}{\sqrt{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} W(i,j)^2}\sqrt{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} W'(i,j)^2}} \quad (10)$$

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

RESULTS AND DISCUSSION

The image used is 1024×1024 Lena, Cameraman, Baboon, Peppers and the watermark image used is a 32×32 binary image shown in Fig. 5a. Encrypted watermark after Arnold and Chaoss encryption is shown in Fig. 5b.

(a)

(b)

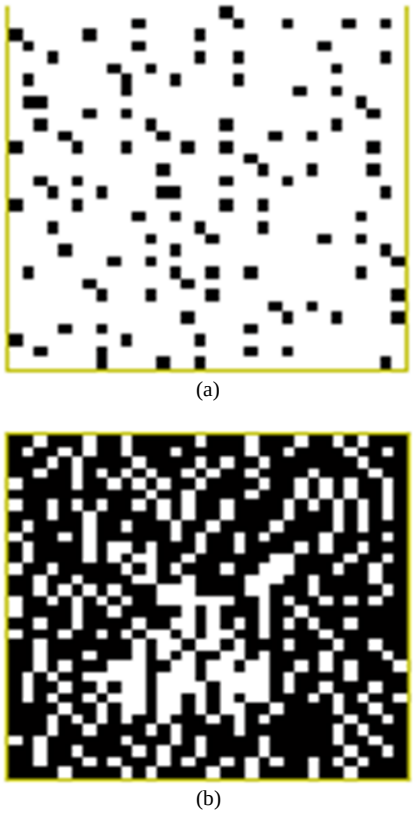
Fig. 5: (a) Original Watermark (b) Encrypted Watermark

Table 1: PSNR and NC without attack

Image	PSNR (dB)	NC
Lena	43.03	0
Cameraman	40.92	0
Baboon	35.68	0
Peppers	42.70	0

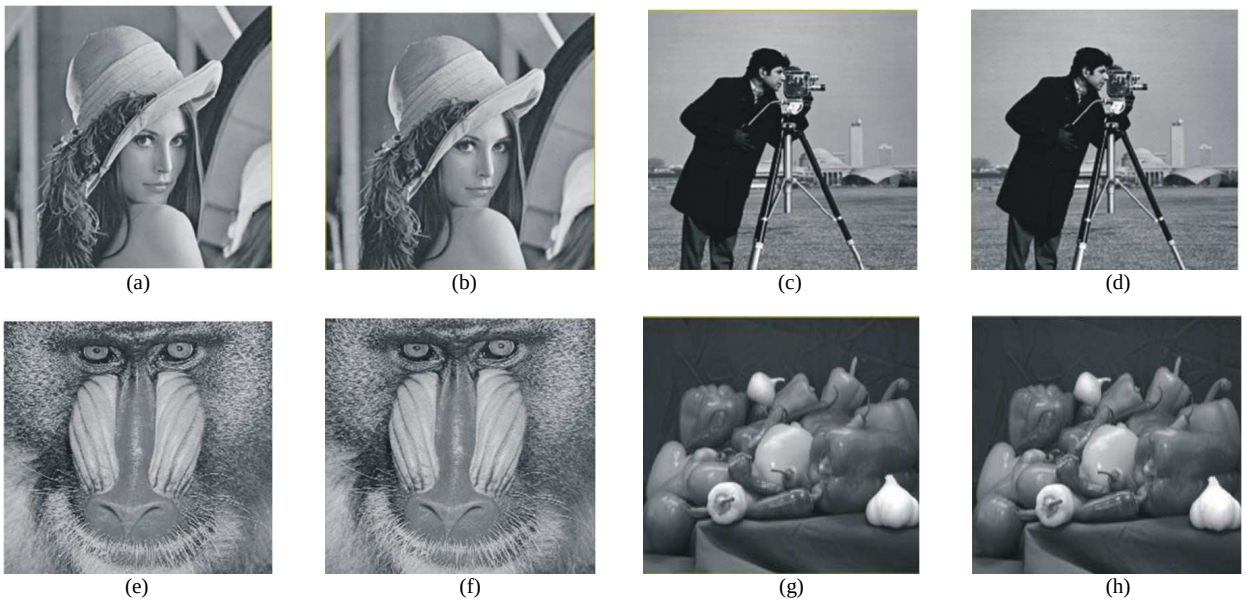
Table 2: PSNR and NC values for Lena image

Gray levels	PSNR	NC
256	19.26	1.000
128	19.19	1.000
64	19.01	1.000
32	18.65	1.000
25	18.45	0.999
20	18.25	0.999
16	17.97	0.999
15	17.86	0.998
14	17.72	0.997
13	17.60	0.998
12	17.48	0.993
11	17.22	0.993
10	17.10	0.992
9	16.85	0.981
8	16.54	0.972
7	16.14	0.972
6	15.62	0.957
5	14.88	0.931
4	13.84	0.930
3	12.10	0.894
2	8.82	0.894



(a) (b)

Fig. 6: (a) Arnold Encrypted Watermark (b) Chaoss Encrypted Watermark



(a) (b) (c) (d) (e) (f) (g) (h)

Fig. 7: (a) Original Lena image (b) Watermarked Lena image (c) Original Cameraman image (d) Watermarked Cameraman image (e) Original Baboon image (f) Watermarked Baboon image (g) Original Peppers image (h) Watermarked Peppers image

We can have only Arnold or only chaoss encryption as shown in Fig. 6a and b. The values of PSNR and NC without attack are given in Table. 1. The original and watermarked images of Lena, Cameraman, Baboon and Pepper with value of alpha = 0.5, are shown in Fig. 7 a-h. Many attacks which can be performed on watermarked image so that the watermark can be extracted from the image. But after attacks, the image becomes useless as the noise can be visually seen. One more specific attack is there which cannot be visually seen in the initial stage but becomes visible when deepen further and that attack is histogram equalization. It is the process in which intensity of the pixels are reassigned in such a way so that all the values available for assigning a gray level are utilized. This technique is generally used to enhance the image, so it can be a attack for the image watermark. We performed the histogram equalization attack on our watermarked image of Lena. We used to restrict the gray levels from 128-2 levels which were initially 256 levels. The result for Lena is shown in Table 2 in terms of PSNR and NC values. The original histogram of the watermarked Lena image is shown in Fig. 8. The Lena image after histogram equalization, extracted watermark and modified histogram are shown in Fig. 9. It is visible seen that as we go on reducing the grey levels, the quality of the Lena image is much reduced. After such a great reduction in quality, the watermark is still present in the image.

Figure 9 a-h Histogram equalized image of the watermarked Lena image with specified grey levels, histogram of the histogram equalized image and extracted watermark from histogram equalized Lena image.

The results after histogram equalization attack are represented in Fig. 10 and 11 as PSNR and NC values.

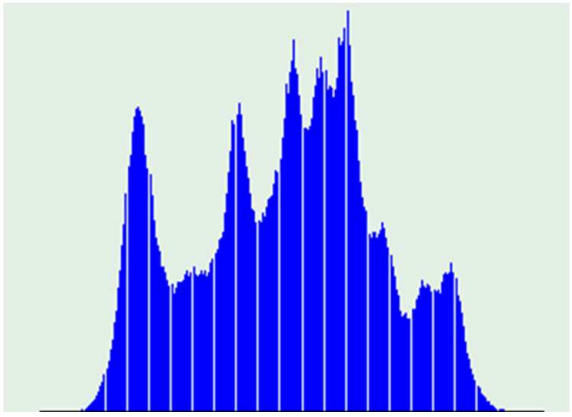


Fig. 8: Histogram of the watermarked Lena image with 256 grey levels

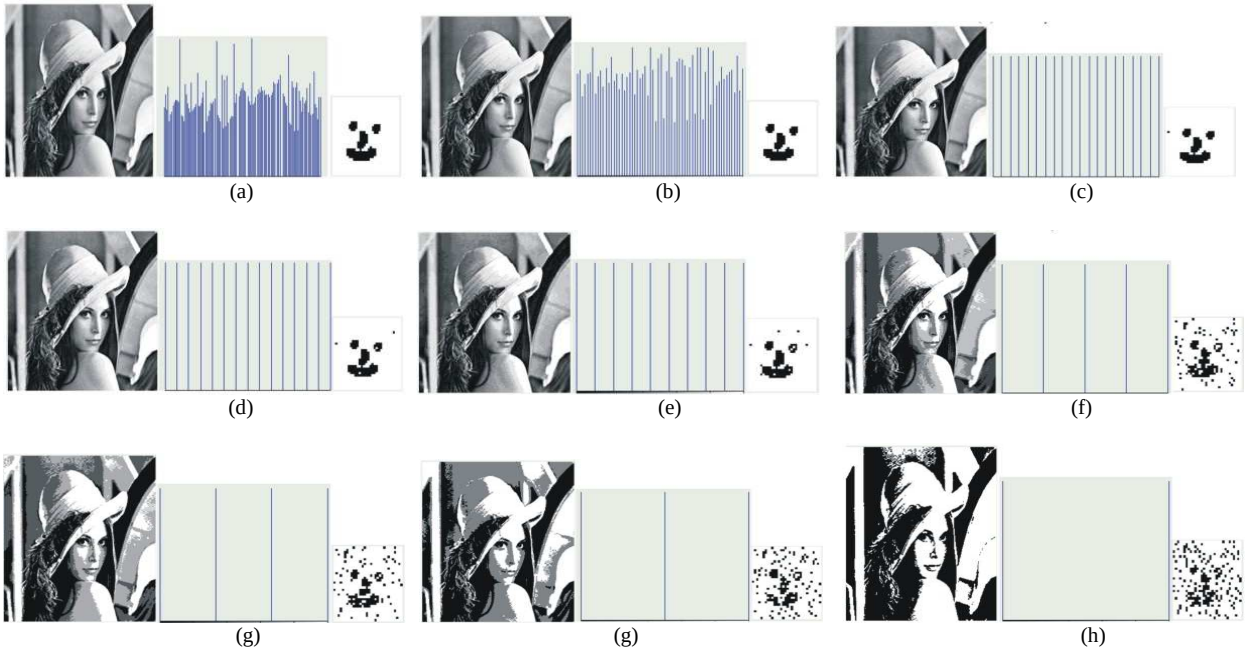


Fig. 9: Histogram equalized image of the watermarked Lena image with specified grey levels, histogram of the histogram equalized image and extracted watermark from histogram equalized Lena image. (a) 128 Grey levels (b) 64 Grey levels (c) 20 Grey levels (d) 10 Grey levels (e) 5 Grey levels (f) 4 Grey levels (g) 3 Grey levels (h) 2 Grey levels

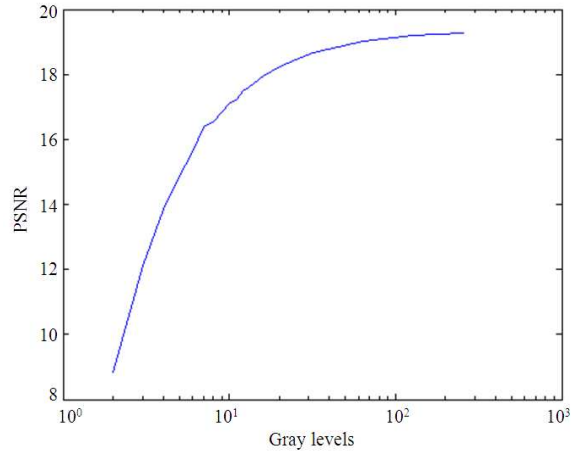


Fig. 10: Values of PSNR with histogram equalization

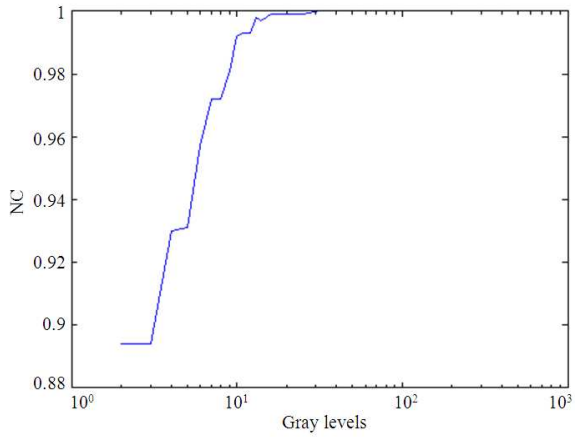


Fig. 11: Values of NC with histogram equalization

CONCLUSION

In this study, we proposed a robust blind watermarking algorithm based on Arnold-Chaoss encryption and combined discrete wavelet transform-discrete cosine transformation. 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 the histogram equalization attack up to quantization of grey level to 2.

REFERENCES

Al-Haj, A., 2007. Combined DWT-DCT digital image watermarking. J. Comput. Sci., 3: 740-746. DOI: 10.3844/jcssp.2007.740.746

Bloom, J.A., I.J. Cox, T. Kalker, J.P.M.G. Linnartz and M.L. Miller *et al*., 1999. Copy protection for DVD video. Proc. IEEE, 87: 1267-1276. DOI: 10.1109/5.771077

Ghannam, S. and F. Abou-Chadi, 2009. Contourlet versus wavelet transform: A performance study for a robust image watermarking. Proceedings of the 2nd International Conference on Applications of Digital Information and Web Technologies, Aug. 4-6, IEEE Xplore Press, London, pp: 545-550. DOI: 10.1109/ICADIWT.2009.5273921

Jiansheng, M., L. Sukang and T. Xiaomei, 2009. A digital watermarking algorithm based on DCT and DWT. Proceedings of the 2nd International Symposium on Web Information Systems and Applications, May 22-24, Academy Publisher, Nanchang, P.R.China, pp: 104-107.

Joshi, A.M. and A. Darji, 2009. Efficient dual domain watermarking scheme for secure images. Proceedings of the International Conference on Advances in Recent Technologies in Communication and Computing, Oct. 27-28, IEEE Xplore Press, Kottayam, Kerala, pp: 909-914. DOI: 10.1109/ARTCom.2009.215

Mohamed, M.A., M.E.D.A. Abou-Soud and M.S. Diab, 2009. Fast digital watermarking techniques for still images. Proceedings of the International Conference on Networking and Media Convergence, Mar. 24-25, IEEE Xplore Press, Cairo, pp: 122-129. DOI: 10.1109/ICNM.2009.4907202

Na, W., W. Yunjin and L. Xia, 2009. A novel robust watermarking algorithm based on DWT and DCT. Proceedings of the International Conference on Computational Intelligence and Security, Dec. 11-14, IEEE Xplore Press, Beijing, pp: 437-441. DOI: 10.1109/CIS.2009.135

Rao, K.R. and P. Yip, 1990. Discrete Cosine Transform: Algorithms, Advantages, Applications. 1st Edn., Academic Press, Boston, ISBN-10: 012580203X, pp: 490.

Shen, Z.W., W.W. Liao and Y.N. Shen, 2009. Blind watermarking algorithm based on henon chaos system and lifting scheme wavelet. Proceedings of the International Conference on Wavelet Analysis and Pattern Recognition, Jul. 12-15, IEEE Xplore Press, Baoding, pp: 308-301. DOI: 10.1109/ICWAPR.2009.5207447

Taherinia, A.H. and M. Jamzad, 2009. A robust image watermarking using two level DCT and wavelet packets denoising. Proceedings of the International Conference on Availability, Reliability and Security, Mar. 16-19, IEEE Xplore Press, Fukuoka, pp: 150-157. DOI: 10.1109/ARES.2009.132

Wang, B., J. Ding, Q. Wen, X. Liao and C. Liu, 2009. An image watermarking algorithm based on DWT DCT and SVD. Proceedings of the International Conference on Network Infrastructure and Digital Content, Nov. 6-8, IEEE Xplore Press, Beijing, pp: 1034-1038. DOI: 10.1109/ICNIDC.2009.5360866

Wang, Q., Q. Ding, Z. Zhang and L. Ding, 2008. Digital image encryption research based on DWT and chaos. Proceedings of the 4th International Conference on Natural Computation, Oct. 18-20, IEEE Xplore Press, Jinan, pp: 494-498. DOI: 10.1109/ICNC.2008.105

Yang, W.M. and Z. Jin, 2009. A watermarking algorithm based on wavelet and cosine transform for color image. Proceedingss of the 1st International Workshop on Education Technology and Computer Science, Mar. 7-8, IEEE Xplore Press, Wuhan, Hubei, pp: 899-903. DOI: 10.1109/ETCS.2009.464

Yushen, L., H. Yanling and W. Chenye, 2010. A research on the robust digital watermark of color radar images. Proceedings of the IEEE International Conference on Information and Automation, June 20-23, IEEE Xplore Press, China, pp: 1091-1096. DOI: 10.1109/ICINFA.2010.5512166

Zhan, R.X., K.Y. Chau, Z.M. Lu, B.B. Liu and W.H. Ip, 2008. Robust image hashing for image authentication based on DCT-DWT composite domain. Proceedings of the 8th International Conference on Intelligent Systems Design and Applications, Nov. 26-28, IEEE Xplore Press, Kaohsiung, pp: 119-122. DOI: 10.1109/ISDA.2008.66