Research Journal of Applied Sciences, Engineering and Technology 6(18): 3365-3371, 2013
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: January 12, 2013 Accepted: February 18, 2013 Published: October 10, 2013

Digital Image Watermarking in Frequency Domain Using ECC and Dual Encryption Technique

[1]G.S. Kalra, [2]R. Talwar and [3]H. Sadawarti
[1]School Electrical and Electronics Engg., Lovely Professional University, Jalandhar, Punjab, India
[2]Principal, Swift College of Engg and Tech. (Affiliated to Punjab Technical University), Punjab, India
[3]Principal Cum Director, RIMTIET (Affiliated to Punjab Technical University), Punjab, India

Abstract: This study presented an algorithm to protect the copyright watermark by providing Hamming codes as error correcting technique. Watermark was embedded in frequency domain using discrete cosine transformation and discrete wavelet transformation, to enhance the susceptibility. Combinations of two techniques are used to target medium frequencies only. Randomness of the watermark is also created before embedding. Instead of embedding in the same place in every block, it is embedded adaptively which depends upon the row and column of that particular block. Results prove the effectiveness of the algorithm against various attacks like jpeg attack, filtering and addition of noises like Gaussian noise, salt and pepper noise and speckle noise. ECC proved to be effective to recover the watermark after certain attacks performed.

Keywords: DCT, DWT, frequency domain, image, watermarking

INTRODUCTION

The tremendous growth of internet resulted penetrating in the remote areas. It is even present where the person find hard to reach. People need latest images, audio files or video files and they are getting it free of cost on the internet. 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. Then the need arises for a method so that the actual producer can prove that the file belongs to him/her.

There are many solutions for this problem as far images are concerned like Steganography, cryptography and digital watermarking. 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. 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 watermarking. DCT and DWT are used to convert an image into frequency domain. Watermark can be embedded by using combined DCT and DWT transformations. In this study, we have implemented our watermarking algorithm using combined DCT and DWT. Also the embedding pixel coordinates are variable depending upon the block handled at that time. The value of the embedding pixel is also adaptive as it changes its percentage of embedding value depending upon its sensitivity to survive against the attacks. Watermark must have the characteristics like Imperceptibility, Security, Robustness and adjustability. Also watermarks should be rapidly embedded into the host signals without much delay.

LITERATURE REVIEW

Image can be converted by DWT into its frequency domain. In study (Shereen and Abou-Chadi, 2009), tested algorithm on CT as well as WT and found that their algorithm is robust in the former case. Authors (Zheng-Wei *et al*., 2009), uses LW and Henon chaos for the encryption of watermark. Chaos has a property of irregular movement which looks like random. Although chaos is a deterministic describing system, its behavior is uncertain. The method was robust against attacks such as JPEG, cropping, adding noise and filtering. Based on DWT, DCT and SVD, authors (Ben *et al*., 2009) and results show that the algorithm combines the advantages of these three transforms. It can satisfy the imperceptibility and robustness very well but was robust only for few attacks like jpeg. In another investigation (Mei *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 WT. Then extract the digital watermark with the help of the original image and the

Corresponding Author: G.S. Kalra, School Electrical and Electronics Engg., Lovely Professional University, Jalandhar, Punjab, India

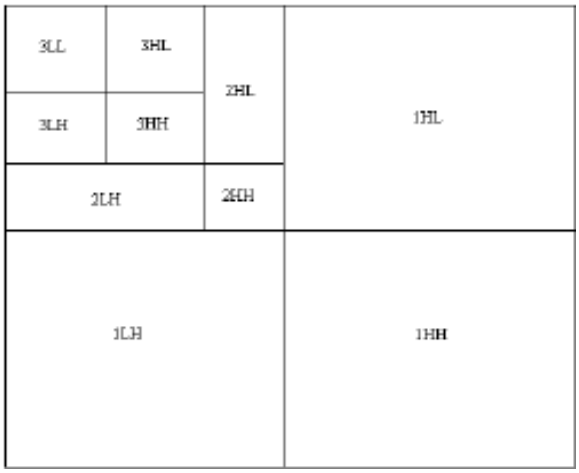


Fig. 1: Three level wavelet decomposition

watermarking image. (Hossein *et al*., 2010) Uses Dynamic Fuzzy Inference System (DFIS) is used along with the block wise DCT to identify the best place for watermark insertion by approximating the relationship established between the properties of HVS model. In the insertion phase, the DC coefficients of the original image were modified according to DC value of watermark and output of Fuzzy System. The algorithm was robust against attacks but the watermarking technique was non-blind. Another watermarking scheme was proposed (Chuan *et al*., 2010) which was capable of providing unequal protection levels to different regions by means of Error Correcting Codes. ECC are used extensively for better robustness, so that the watermark can be recovered with low bit error rates. Before insertion of the watermark, ECC was inserted and after extraction of the watermark on the receiver side, the same inverse ECC was applied and the original watermark recovered. Certain techniques were developed by using error correcting techniques such as hamming error correction, RS code and BCH (Yuan and Xiaozhi, 2011) codes. Some watermarking techniques also described RS codes (Wadood *et al*., 2009) for blind frequency domain watermarking schemes in the presence of attacks. It also shows good results especially for burst attacks. Another technique (Fang, 2009) analyzed the security of delivery images; at the same time, a method about error correcting code was implemented to prevent passive attacks based on bit modification. A watermarking technique (Zhang *et al*., 2009) was implemented on Y, Cb and Cr color spaces after performing DCT and Hamming error codes. ECC techniques also show good results while implementing in audio (Htay and Foo, 2009) and video watermarking. Hamming code was also proposed for medical images watermarking (Abadi *et al*., 2010). In another investigation (Mitekin and Timbay, 2012), hamming distance was used to generate watermarking sequence which shows the effectiveness of the algorithm using hamming. Thus we concluded to develop an algorithm which will be implemented in frequency domain to achieve the robustness and it will remain invisible. Watermark will be provided error correcting technique, so that it can be recovered after common signal processing attacks. To enhance the security of the watermark, we are going to implement two encryption techniques which are chaos and Arnold transformation.

METHODOLOGY

The proposed scheme is made up after concluding the literature survey. It utilizes the advantages of discrete cosine transformation, wavelet transform, Arnold Transform, Chaos and Hamming error codes. Two encryption techniques are used to enhance the security of the watermark. The image for watermarking is first applied by the discrete wavelet transform up to two levels as shown in Fig. 1. This is because depending upon the discrete wavelets theory and human visual characteristics; we know that the embeddable watermarking capacity will decrease with the increase of layer numbers. Then 2D-DCT will be applied on the middle frequency band which is HL2. 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.

As far as watermark is concerned, Hamming error codes are to be inserted row wise as well as column wise. Arnold and chaos encryption will be applied on the coded watermark. Arnold transformation defined by (1) is a one-to-one transformation:

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

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

Equation (2) 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. 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 and 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: Random integer and should be greater than 0
$(I_0^m, I_0^m, \ldots)$: Continuous equal interval in [0, 1] and the interval is divided by 2^m

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

- Take the original image and resize it to 1024×1024 images. Make two-level wavelet decomposition of the original image and the frequency band HL2 as the embedded domain, the wavelet coefficient of HL2 extracted as CH2
- Take the DCT of sub size 4×4
- Take the watermark and resize it to 32×32 bit binary image
- Apply hamming error codes horizontally and vertically and then apply the Arnold transformation to the watermark
- After the Arnold transformation, apply the Chaos's transformation to the output of Arnold transformed watermark
- Calculate the pixel to be embedded using the row number and column number of the starting of that block after DCT. Let the sum of row values and column values comes out to be xm and ym. Then the coordinates of pixel insertion in that particular block can be given as:

```
if (xm = 1) or (xm = 6) or (xm = 8)
x' = 3;
else if (xm = 0) or (xm = 2) or (xm = 3) or (xm = 5)
x' = 4;
else
x' = 5;
end
if (ym = 1) or (ym = 6) or (ym = 8)
y' = 3;
else if (ym = 0) or (ym = 2) or (ym = 3) or (ym = 5)
y' = 4;
else
y' = 5;
end
```

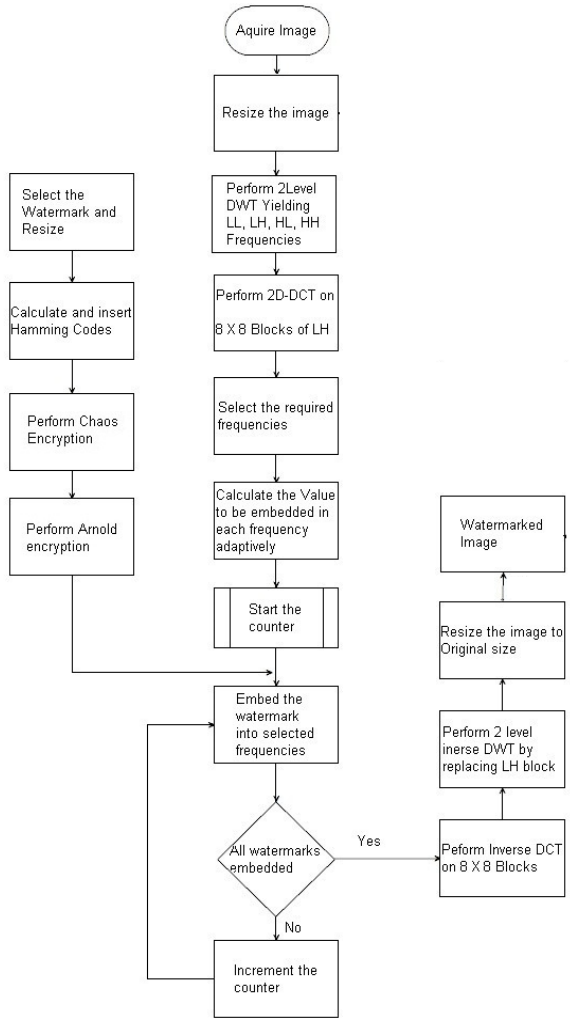


Fig. 2: Embedding algorithm

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

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

where,
Xw : The watermarked image before inverse DWT
Wk : The watermark bit at k'th position and k = 0, 1, 2,……..1023
σ^2 : The S.D. of the original image
α : 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

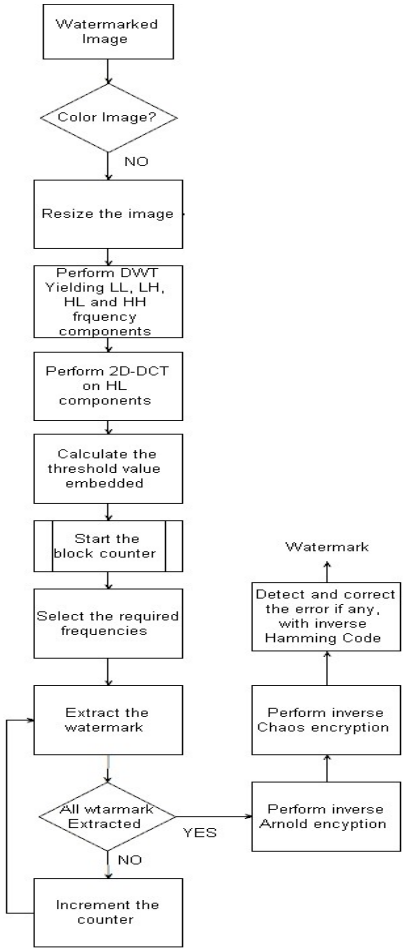


Fig. 3: Extraction algorithm

Watermarking extraction algorithm: The flow chart for watermarking extraction algorithm is shown in Fig. 3. 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 2 level decomposition and mark the frequency band HL2 as CH2 to extract the watermark
- Take the DCT of sub size 4×4
- Extract the watermark from CH3 from the location (x', y') calculated in the embedding procedure at step 6 as given in (6) below:

$$w_k = \begin{cases} wk = 1 \ , if\ Xw(x',y') \geq 0 \\ wk = 0 \ , if\ Xw(x',y') < 0 \end{cases} \quad (6)$$

where,
Xw = The pixel where watermark was embedded
wk = The extracted watermark bit

- Take the inverse Chaos transformation of the extracted watermark
- Take the inverse Arnold transformation of the reverse Chaos image to get the desired extracted watermark
- Calculate the error syndrome row wise and column wise, if any, then correct the errors and watermark will be extracted and corrected

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:

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

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

where,
MSE : The mean square error of the watermarked image and the original image
m, n : The number of rows and number of columns
I & K : 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):

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

The Bit Error Rate (BER) can be calculated as given in (10):

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

where,
W (i, j) : The original watermark
W' (i, j) : The extracted watermark

Table 1: PSNR, NC and BER without attack

Image	PSNR (dB)	NC	BER
Lena	44.69	1	0
Cameraman	42.63	1	0
Baboon	38.48	1	0
Peppers	45.19	1	0

Table 2: PSNR results after attacks on images

Attack	Depth	Lena	Camera man	Baboon	Peppers
JPEG (QF)	60%	44.86	42.98	36.10	46.40
	70%	45.76	43.75	36.28	47.24
	80%	45.11	42.79	36.07	46.96
Gaussian filter	3×3	42.97	41.54	35.54	48.59
	7×7	42.67	41.19	34.85	48.35
Median filter	3×3	47.20	44.21	33.94	48.38
	5×5	44.39	39.53	27.36	47.84
Gaussian noise (mean = 0.01)	Var = 0.01	20.00	20.26	19.92	20.01
	Var = 0.02	17.14	17.41	17.05	17.34
Salt and pepper noise	0.01	25.34	24.91	25.35	25.01
	0.02	22.43	22.01	22.51	21.98
	0.03	20.71	20.25	20.81	20.25
	0.05	18.43	18.07	18.54	18.02
Speckle noise	0.01	25.62	25.54	25.25	28.75
	0.02	22.65	22.59	22.35	25.81
	0.04	19.75	19.61	19.39	22.90
	0.06	18.08	17.87	17.70	21.19

Table 3: BER results after attacks on images

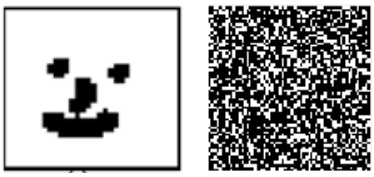
Attack	Depth	Lena	Camera man	Baboon	Peppers
JPEG (QF)	60%	0.335	0.052	0.006	0.352
	70%	0.045	0.005	0.002	0.081
	80%	0.000	0.000	0.000	0.005
Gaussian filter	3×3	0.000	0.002	0.004	0.000
	7×7	0.000	0.000	0.003	0.000
Median filter	3×3	0.359	0.403	0.508	0.340
	5×5	0.032	0.067	0.234	0.022
Gaussian noise (mean = 0.01)	Var = 0.01	0.081	0.037	0.000	0.102
	Var = 0.02	0.225	0.149	0.011	0.267
Salt and pepper noise	0.01	0.000	0.000	0.000	0.000
	0.02	0.006	0.008	0.000	0.044
	0.03	0.078	0.016	0.000	0.089
	0.05	0.222	0.092	0.001	0.230
Speckle noise	0.01	0.000	0.000	0.000	0.000
	0.02	0.008	0.000	0.000	0.000
	0.04	0.049	0.027	0.000	0.013
	0.06	0.138	0.050	0.003	0.021

Table 4: NC results after attacks on images

Attack	Depth	Lena	Camera man	Baboon	Peppers
JPEG (QF)	60%	0.791	0.971	0.997	0.7800
	70%	0.974	0.997	0.999	0.9540
	80%	1	1.000	1.000	0.9970
Gaussian filter	3×3	1	0.999	0.998	1.0000
	7×7	1	1.000	0.998	1.0000
Median filter	3×3	0.774	0.742	0.660	0.7880
	5×5	0.982	0.961	0.859	0.9870
Gaussian noise (mean = 0.01)	Var = 0.01	0.954	0.979	1.000	0.9410
	Var = 0.02	0.865	0.912	0.994	0.8380
Salt and pepper noise	0.01	1.000	1.000	1.000	1.0000
	0.02	0.997	0.995	1.000	0.0975
	0.03	0.955	0.991	1.000	0.9490
	0.05	0.867	0.946	0.999	0.8620
Speckle noise	0.01	1.000	1.000	1.000	1.0000
	0.02	0.995	1.000	1.000	1.0000
	0.04	0.972	0.984	1.000	0.9930
	0.06	0.919	0.971	0.998	0.9880

RESULTS AND DISCUSSION

The image used is 1024×1024 Cameraman and the watermark image used is a 32×32 binary image shown in Fig. 4a. Encrypted watermark after ECC, Arnold and Choss encryption is shown in Fig. 4b. The values of PSNR, NC and BER without attack are given in Table 1. The original and watermarked images of Lena, Cameraman, Baboon and Pepper with value of alpha = 1.5, are shown in Fig. 5a to 5h. Different types of attacks are performed and the values of PSNR, BER and NC are tabularized in Table 2, 3 and 4 respectively.

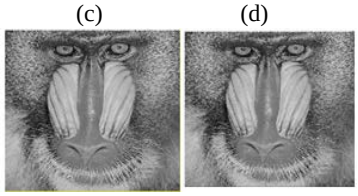


(a) (b)

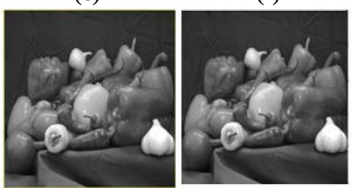
Fig. 4: (a) Original watermark, (b) encrypted watermark

(a) (b)

(c) (d)



(e) (f)

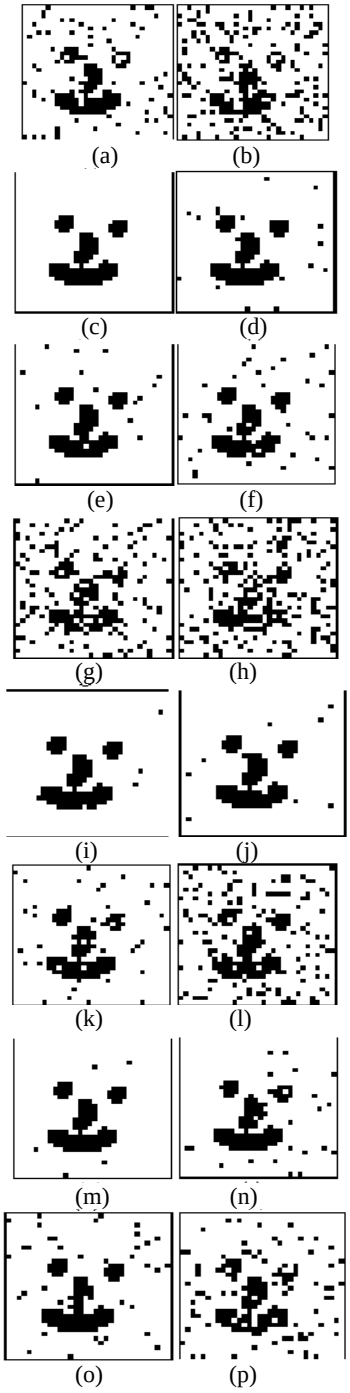


(g) (h)

Fig. 5: (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

Watermarks extracted after attacks on Lena watermarked image are shown in Fig. 6.

It is clear from the Table 2, 3 and 4 PSNR is in between 38 dB to 45dB depending upon the complexity of the image. This is due to the fact that the embedding quantity in the pixels is depending upon the variance of the original image. For jpeg compression, lena and peppers images can not handled the 40% compression because complexity of the images are less. However, in Lena and Cameraman images are able handle the 40% compression due to more complexity. Gaussian filtering attacks was not able to distort the watermark in both the



(a) (b)

(c) (d)

(e) (f)

(g) (h)

(i) (j)

(k) (l)

(m) (n)

(o) (p)

Fig. 6: Extracted watermark after attack, (a) JPEG (QF40%), (b) JPEG (QF = 30%), (c) median filter 3×3, (d) median filter 7×7, (e) Gaussian noise mean = 0.01, Var = 0.01, (f) Gaussian noise mean = 0.01, Var = 0.02, (g) Gaussian noise mean = 0.01, Var = 0.04, (h) Gaussian noise mean = 0.01, Var = 0.06, (i) S & P noise 2%, (j) S & P noise 4%, (k) S & P noise 5%, (l) S & P noise 10%, (m) speckle noise 2%, (n) speckle noise 4%, (o) speckle noise 6%, (p) speckle noise 10%

cases as 3×3 or 7×7 windows. While with median filter attack, watermark survived only for 5×5 window and not with 3×3 window. Also watermark survived after Gaussian noise, salt &pepper noise and speckle noise attacks.

CONCLUSION

In this study, we proposed a watermarking algorithm based on Hamming error codes and dual encryption combined with DWT-DCT. The randomness generated by Arnold and chaos system possesses the watermark to become more secure. The watermark embedding algorithm can efficiently resist attacks like JPEG with quality factor as low as 60% for the image of Baboon having large information, Gauss low pass filter, salt & Pepper noise, speckle noise and median filtering. Further the algorithm can be made enhanced to handle the lower quality factor of the compression and median filtering for less informative images.

REFERENCES

Abadi, M., H. Danyali and M. Dehnavi, 2010. Medical image authentication based on fragile watermarking using hamming code. ICBME2010, Nov. 2010, Iran.

Ben, W., D. Jinkou, W. Qiaoyan, L. Xin and L. Cuixiang, 2009. An image watermarking algorithm based on DWT DCT and SVD. Proceeding of the IEEE International Conference on Network Infrastructure and Digital Content, China, pp: 1034-1038.

Chuan, Q., M. Qian and Z. Xinpeng, 2010. Image watermarking scheme with unequal protection capability based on error correcting codes. J. Multimed., 5(5): 427-433.

Fang, Z., 2009. Digital image of restoring image based on (7, 4) hamming code. Proceeding of the International Conference on Multimedia Information Networking and Security.

Hossein, R., M. Reza and E.M. Mohsen, 2010. A new robustwatermarking scheme to increase image security. EURASIP J. Adv. Signal Proc., 2010: 1-30.

Htay, H.Y. and S.W. Foo, 2009. Audio watermarking with error-correcting code. TENCON 2009, Singapore.

Mei, J., S. Li and X. Tan, 2009. A digital watermarking algorithm based on DCT and DWT. Proceeding of the International Symposium on Web Information Systems and Applications, China, pp: 104-107.

Mitekin, V.A. and E.I. Timbay, 2012. A new watermarking sequence generation algorithm for collision-free digital watermarking. Proceeding of the 8th International Conference on Intelligent Information Hiding and Multimedia Signal (IIH-MSP), July 18-20, pp: 256-260.

Shereen, G. and F. Abou-Chadi, 2009. Contourlet versus wavelet transform: A performance study for a robust image watermarking. Proceeding of the 2nd International Conference on the Applications of Digital Information and Web Technologies (ICADIWT), Electron and Commun. Dept., Mansoura Univ., Egypt, pp: 545-550.

Wadood, A., C. Philippe and G. Philippe, 2009. List decoding of reed solomon codes forwavelet based colour image watermarking scheme. Proceeding of the 16th IEEE International Conference on Image Processing (ICIP), Lab. SIC-XLIM, Univ. of Poitiers, Chasseneuil, France, pp: 3637-3640.

Yuan, L. and H. Xiaozhi, 2011. A blind watermarking algorithm based on image scrambling and error correct coding preprocessing. Proceeding of the International Conference on Electrical and Control Engineering (ICECE), Sept. 16-18, pp: 4231-4233.

Zhang, Y., L. Li-Cai, L. Qi-Shen and J. Ze-Tao, 2009. A blind watermarking algorithm based on block DCT for dual color images. Proceeding of the International Symposium on Electronic Commerce and Security, China.

Zheng-Wei, S., L. Wei-Wei and S. Ya-Nan, 2009. Blind watermarking algorithm based on henon chaos system and lifting scheme wavelet. Proceeding of the International Conference on Wavelet Analysis and Pattern Recognition, Baoding, July 12-15, pp: 308-313.