IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-5, May 2018 E-ISSN: 2347-2693

Digital Image Watermarking in Discrete Fourier Transform domain

Ningombam Jimson[1*], Kattamanchi Hemachandran[2]

[1*, 2]Department of Computer Science, Assam University, Dorgakona, Silchar, Pin-788011, India

**Corresponding Author: jimson123@gmail.com, Tel.: +91-8011855859*

Available online at: www.ijcseonline.org

Accepted: 21/May/2018, Published: 21/May/20182018

Abstract—The rapid development of internet communication has increased the rate at which digital data is being shared wideley as the digital data can be flawlessly copied and distributed over the internet. A Digital watermarking is a process in which a bit of information is added to the digital data like image video and audio. A CDMA based image watermarking method in Discrete Fourier Transform (DFT) is proposed in this paper for protecting the copyright and authentication of the digital image. The original digital image is divided into a non-overlapping block of 8X8 and one bit of binary information is embedded in the block using two highly uncorrelated Pseudo-random sequences in the coefficient of the magnitude domain of DFT. For watermark extraction, the original image is not required. Based on the correlation values between magnitude coefficient and Pseudo-random sequences the watermark is extracted from the watermarked image. The scheme is tested using Stimark Benchmarking tools. The Experimental result suggested that the method is robust against numbers of digital watermarking attacks.

Keywords— Discrete Fourier Transform (DFT), CDMA Image Watermarking, Peak Signal to Noise Ratio (PSNR), Normalized Correlation (NC).

I. INTRODUCTION

Digital watermarking has attracted lots of interest in past decade due to fact that a digital data in the form of image video and audio can be duplicated in high quality and distributed which results in the violation of copyright and misperception of the data owners. Digital watermarking, which is a process of embedding a piece of information in the digital content, is considered one of the possible solution for the protection of the digital content. Cryptography can be considered as another mean for protecting the digital content from unauthorized access by making the content meaningless to the third party, only the valid consumer is provided with a key for deciphering the digital content. Once the content is deciphered, the content owner has no control over the distribution or duplication of the digital data.

The general framework of digital image watermarking consist of an encoder, a decoder and a comparator. An encoder (E) accept the cover image C, a watermark W and produce an output watermarked image C'. The decoder (D) process consist of two process – extracting the watermark and a comparator process. A watermark extractor takes an image (I) which can be a watermarked or a non-watermark image and resulting output as extracted watermark W^*. In the comparator process the extracted watermark W^* is compared with the original watermark W. The output of the comparator (O) can be 1 or 0 depending on the fact that the watermark is present or not. Figure 1 shows the general watermarking procedure [2]

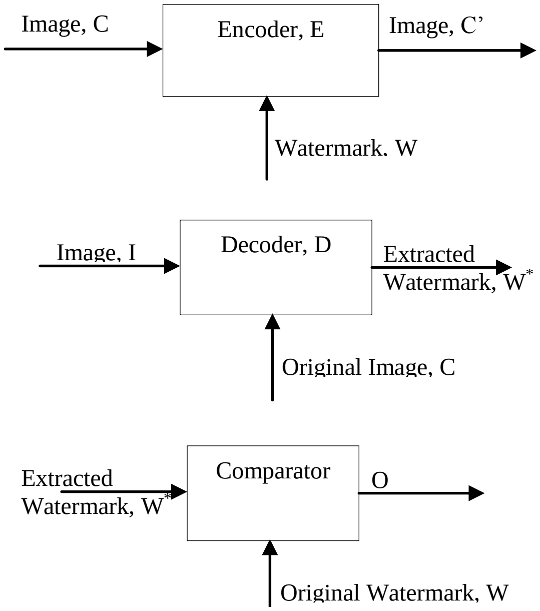


Figure 1. Digital Image Watermarking Processes

A watermark can be added in the pixel level that's spatial domain by modifying the pixels value. Some of the schemes used in the spatial watermarking are Least

Significant bit substitution(LSB), Patchwork based scheme. Watermark can also be embedded in the transform domain which is more robust compared to the spatial domain embedding. Discrete Cosine Transform (DCT), Discrete wavelet transform (DWT), Discrete Fourier transform (DFT) are some of the common transformation used for image watermarking. In the presented scheme DFT is used for watermarking

II. Discrete Fourier Transform

The DFT decompose an image into its sine and cosine component. DFT produce a complex numbered images and can be displayed into two images either with real and imaginary part or with the magnitude and phase. The number of frequencies in the Fourier domain corresponds to the number of pixels in the spatial domain i.e. the images in the spatial and Fourier domain are of the same size. The Fourier transform of an image of MXN is given by [3][4]

$$F(u,v) = \frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1} f(m,n)e^{-j2\pi\left(\frac{um}{M}+\frac{vn}{N}\right)} \qquad (1)$$

where f(m, n) is the image in the spatial domain and exponential term is the basis function corresponding to each point F(u, v) in the fourier space. The basis function are sine and cosine waves with increasing frequency. The inverse DFT is given by

$$f(m,n) = \frac{1}{MN}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} F(u,v)e^{j2\pi\left(\frac{um}{M}+\frac{vn}{N}\right)} \qquad (2)$$

The magnitude (M) and phase (P) of the DFT is given by

$$M(u, v) = |F(u, v)|$$

$$P(u, v) = \angle F(u, v)$$

In the presented scheme, the watermark is embedded in the magnitude component of the DFT. Comparing to the phase, the magnitude hold less image information than the phase of the DFT

III. Proposed scheme

A. Watermark embedding

The original cover image C_o is divided into a non-overlapping block of 8X8. The magnitude of the DFT is calculated for each block. Using a key, two highly uncorrelated PN sequence (eg. pn sequence one and pn sequence zero) are generated. If the watermark bit is one the value from the pn sequence one is embed as the watermark and if the watermark bit is 0, the pn sequence zero is embeded as watermark using the following equation.

$$C_w(u,v) = \begin{cases} C_o(u,v) + \alpha * W(u,v), & u,v \notin F_L \\ C_o(u,v), & u,v \in F_L \end{cases} \qquad 3$$

Where α is the watermarking strength, C_w is the resultant watermarked image where F_L is the lower frequency component. W is the binary watermark used. Performing the inverse DFT using the phase of the original image and modified magnitude component we get the watermarked cover image.

B. Watermark Detection

In the extraction process, the watermarked image is divided into the 8X8 blocks and DFT of the each block is found out. We generated higly uncorrelated pseudorandom noise (PN) sequences using the secret key viz. PN1 and PN0. The correlation between the two PN sequences with the magnitude coefficient of DFT of the watermarked image is found out. If the correlation of PN1 and magnitude component is higher then correlation of PN0, then 1 is encodes as watermark bit otherwise 0 is encoded as watermark bit. Thus we get a vector of watermarking bits, reshaping the resulting vector we get the extracted watermark.

IV. Expiremental Results

We use a 64X64 binary image as watermark, this is will be embedded onto a cover images which is of size 512X512 with 256 gray level. The watermark and cover image are shown in figure 1 and figure 2 repectivey.

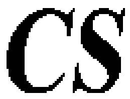


Figure 2. Binary watermark

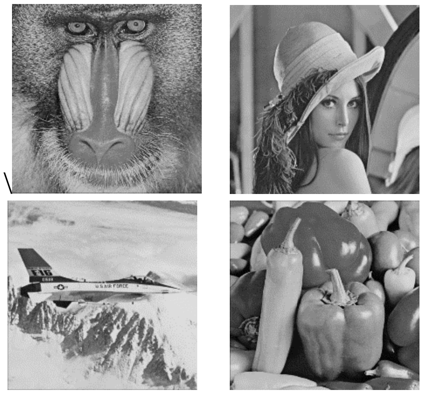


Figure 3. Cover Images used

We used Peak Signal to Noise Ratio (PSNR) to measure the invisibility of the watermark and Normalised Correlation (NC) to detect the similarity between the original and the extracted watermark. PSNR is define as [5]

$$\mathrm{PSNR} = 10\log\left(\frac{255^2}{\mathrm{MSE}}\right) \qquad 4$$

Where MSE is Mean Square error, the MSE betweern original image I and watermarked image I* which is of MXN, then

$$\mathrm{MSE} = \frac{1}{\mathrm{MXN}}\sum_{i=1}^{M}\sum_{j=1}^{N}[\mathrm{I}(i,j) - \mathrm{I}^*(i,j)]^2 \qquad 5$$

The Normalised correltion(NC) between MXN original watermark image W and extracted watermark W* can be calculated using the equation 6 [6]

$$\mathrm{NC}(W, W^*) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j).\, W^*(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j)^2}\ \sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} W^*(i,j)^2}} \qquad 6$$

NC value lies between 0 and 1, higher the NC value the better the similarity between the original and watermark image. According to [7].

Fig. 3 shows the original cover images, watermarked images and the extracted watermark without any attacks.

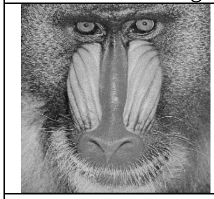
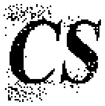
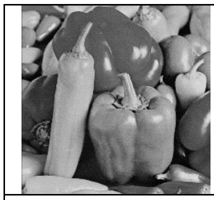
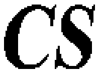
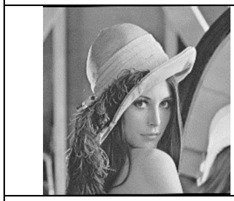
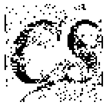
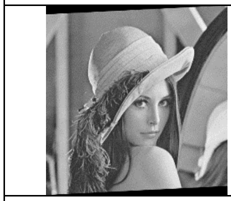
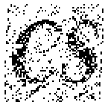
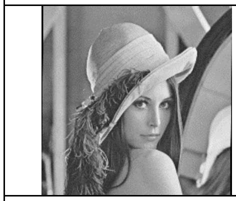
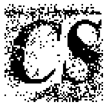
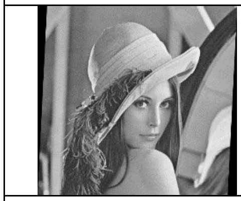
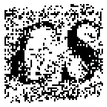
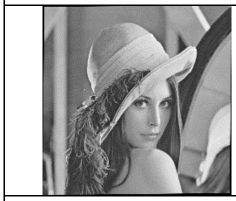
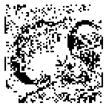
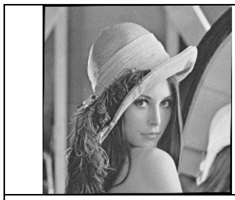
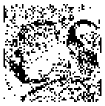
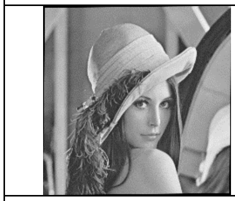
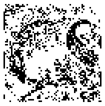
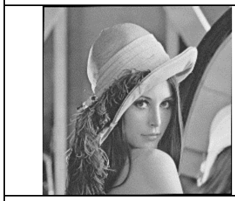
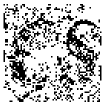
Watermarked image	Extracted Watermark
	
PSNR = 35.0964	NC = 0.9638
PSNR = 35.5679	NC = 0.99969
PSNR = 35.1323	NC = 0.99922
	
PSNR = 34.8433	NC = 1

Figure 4. Watermarked Image and Corresponding extracted Watermark

We tested our algorithm using Stirmark benchmarking tools [8] and common image processing attack to the watermarked Lena image keeping the value of α=100, result obtained are as follows

Table 1. Performance Against Affince Transformation

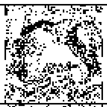
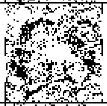
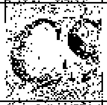
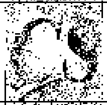
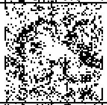
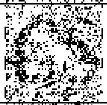
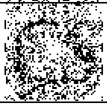
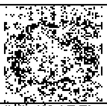
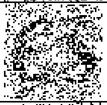
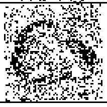
Affine Transformation	**NC of the Extracted watermark**
	
Affine transformation 1	NC = 0.9031
	
Affine Transformation 2	NC = 0.868
	
Affine Transformation 3	NC = 0.87062
	
Affine Transformation 4	NC = 0.82253
	
Affine Transformation 5	NC = 0.83352

	
Affine Transformation 6	NC = 0.82772
	
Affine Transformation 7	NC = 0.82738
	
Affine Transformation 8	NC = 0.83522

From Table 1 we got the NC > 8 for all the affine transformation simulated using StirMark benchmarking tools. From the result obtained we can say that the scheme is robust against such type of attacks

Table 2 shows the expiremental result of the scheme against small angular rotation of the watermarked Lena image with different angle.

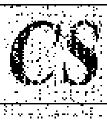
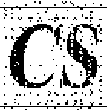
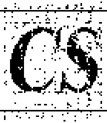
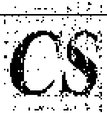
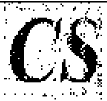
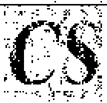
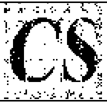
Table 2. Performance Against Rotation Attacks

Angle of rotation	Extracted Watermark	NC
0.5		0.81964
-.05		0.82315
0.25		0.86858
-0.25		0.86664
0.75		0.79766
-0.75		0.81374
1		0.79166
-1		0.80728
2		0.78955
-2		0.81374

The watermark extraction after the image is rotates with rotation angle >2, we got NC of the extracted and original watermark is greater then 7 but the watermark is not perceptible to the normal eyes.

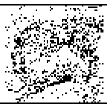
Table III shows the performance of the of the scheme against the random removal of line on the watermarked Lena image.

Table 3. Results Against Random Removal Of Line

No. of line removed	Extracted Watermark	NC
40		0.94128
50		0.954
60		0.95093
70		0.95628
80		0.96201
90		0.93829
100		0.95047

The Random removal of line in the watermarked cover image has no effect in the watermark extraction process. This shows that the scheme is robust against such type of attack from the result obtained.

Table 4. Result Obtained From Rescaling Watermark Lena Image

Rescaling %	Extracted watermark	NC
50		0.84151

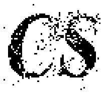
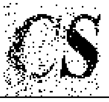
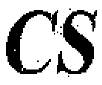
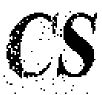
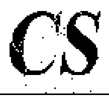
75		0.959
90		0.9402
110		0.99655
150		0.98127
200		0.99327

Table 5. Result From The Rotation And Cropping Attacks

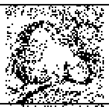
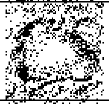
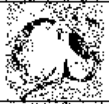
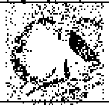
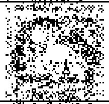
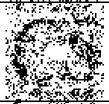
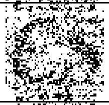
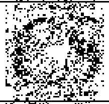
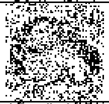
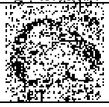
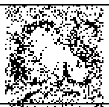
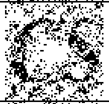
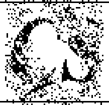
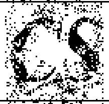
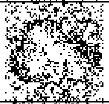
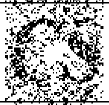
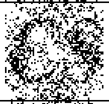
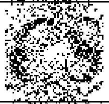
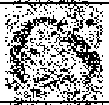
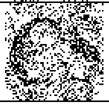
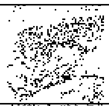
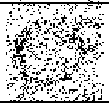
Angle of rotaion	Extracted Watermark	NC
0.5		0.82975
-0.5		0.82892
0.25		0.87446
-0.25		0.87109
0.75		0.81307
-0.75		0.81539
1		0.80297
-1		0.80792
2		0.78864
-2		0.79215

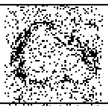
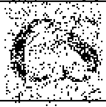
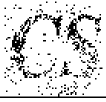
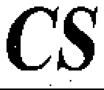
Table 6. Performance Against Rotation And Scaling

Rotation angle	**Extracted Watermark**	**NC**
0.5		0.82544
-0.5		0.83845
0.25		0.86687
-0.25		0.88271
0.75		0.80823
-0.75		0.82139
1		0.81255
-1		0.80761
2		0.79968
-2		0.78764

From the result obtained, we can conclude that the scheme is robust against most of the attacks simulated by Stirmark benchmarking tool. The scheme shows high robusteness toward scaling, geometrical crop or scaling as we got the NC value is almost 8 in most of the cases. Since the watermark is inserted in in high frequency component of the magnitude of the DFT. The scheme suffer from JPEG compression attacks when the Quality factor is less then 50. Table 7 showed the result obtained from JPEG Compression attack on the watermark lena image

Table 8. Performance Against Jpeg Compression

Quality factor	**Extracted Watermark**	**NC**
20		0.8301
40		0.8344

50		0.8507
60		0.8830
80		0.91251
100		0.99953

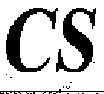
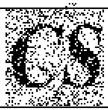
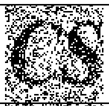
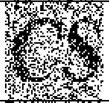
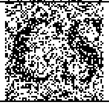
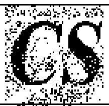
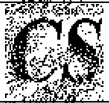
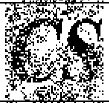
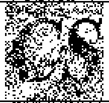
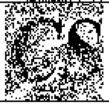
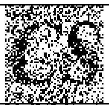
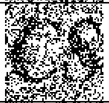
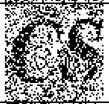
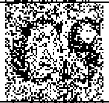
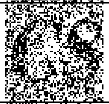
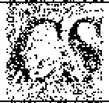
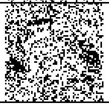
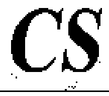
We tested our scheme on other image format like tiff, png and jpeg. The results obtained is shown in Table 8.

Table 8. Performance Against Different Image Format

Image type	Watermarked image	Extracted watermark	NC
JPEG			0.99969
TIFF			0.99984
PNG			0.99984

We also tested our scheme with common image processing attacks like noise addition(salt and pepper, speckle, guassian), filter like median, weiner and histogram equalization and the experimental results are shown in table 9

Table 9. Performance Against Different Types Of Image Processing Attacks

Salt and pepper noise addition	**Extracted watermark**	**NC**
0.01		0.92734
0.02		0.85094
0.03		0.81071
0.04		0.78782
0.05		0.75926
Speckle Noise addition	**Extracted watermark**	**NC**
0.01		0.89961
0.02		0.84361
0.03		0.81905
0.04		0.7953
0.05		0.77401
Gaussian Noise addition	**Extracted Watermark**	**NC**
0.01		0.76869
0.02		0.76791
0.03		0.78138
0.04		0.77486
0.05		0.75924
Weiner Filter		0.85694
Median Filter		0.75716
Histogram Equalization		0.99859

V. Conclusion

We proposed a block-based CDMA watermarking scheme in DFT domain using two highly uncorrelated pseudorandom noise sequence. The results is found to be robust against affine transformation, Rescaling, small angular rotation and JPEG compression. The scheme also surivive common image processing attacks like noise addition and filter. Future work will focused on increasing the robust against JPEG compression and angular rotation. We also tried our scheme in different image format like JPEG, PNG and TIFF images and the achieved a desirable results.

References

[1]. Chandramouli, R., Memon, N., & Rabbani, M. (2002). Digital watermarking. *Encyclopedia of Imaging Science and Technology*.

[2]. Mohanty, S. P., Sengupta, A., Guturu, P., & Kougianos, E. (2017). Everything You Want to Know About Watermarking: From Paper Marks to Hardware Protection: From paper marks to hardware protection. *IEEE Consumer Electronics Magazine*, *6*(3), 83-91.

[3]. Qidwai, U., & Chen, C. H. (2009). *Digital image processing: an algorithmic approach with MATLAB*. CRC press.

[4]. Ruanaidh, J. J. K. O., Dowling, W. J., & Boland, F. M. (1996, September). Phase watermarking of digital images. In *Image Processing, 1996. Proceedings., International Conference on*(Vol. 3, pp. 239-242). IEEE.

[5]. Voloshynovskiy, S., Pereira, S., Iquise, V., & Pun, T. (2001). Attack modelling: towards a second generation watermarking benchmark. *Signal processing*, *81*(6), 1177-1214.

[6]. Janthawongwilai, K., & Amornraksa, T. (2004, October). Improved performance of amplitude modulation based digital watermarking. In *Communications and Information Technology, 2004. ISCIT 2004. IEEE International Symposium on* (Vol. 1, pp. 318-323). IEEE.

[7]. Na, W., Yunjin, W., & Xia, L. (2009, December). A novel robust watermarking algorithm based on DWT and DCT. In *Computational Intelligence and Security, 2009. CIS'09. International Conference on* (Vol. 1, pp. 437-441). IEEE.

[8]. Fabien A. P. Petitcolas, Ross J. Anderson, Markus G. Kuhn. Attacks on copyright marking systems, in David Aucsmith (Ed), Information Hiding, Second International Workshop, IH’98, Portland, Oregon, U.S.A., April 15-17, 1998, Proceedings, LNCS 1525, Springer-Verlag, ISBN 3-540-65386-4, pp. 219-239.

[9]. Mazumder, J. A., & Hemachandran, K. (2014). Color Image Steganography Using Discrete Wavelet Transformation and Optimized Message Distribution Method. *International Journal of Computer Sciences and Engineering*, *2*(7), 90-100.

[10]. Dheeraj Sai D V L N, K N S Aneesh, (2015). Image Water Marking Using Cryptography. International Journal of Computer Sciences and Engineering, 3(7), 171-178.

Authors Profile

Mr. Ningombam Jimsonr received its Bachelor of Science from Mangalore University in 2005 and Master of Science from Mangalore University in the year 2007. He is currently pursuing Ph.D. in Assam University and his main research work focuses on Image processing, Information Hiding, Visual Cryptography, Digital Watermarking, Steganography, Data Security

Prof. Kattamanchi Hemachandran is currently serving as the Head in the Department of Computer Science, Assam University, Silchar and is associated with the Department since 1998. He obtained his Master Degree from Sri. Venkateswara Univerisity, Tirupati and M.Tech and Ph.D degree from Indian School of Mines, Dhanbad. His areas of research interest are Image Processing, Software Engineering and Distributed Computing.