International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 7 2078 – 2080

Image Authentication Resilient To Geometric Attacks Using DFT

Mr. Bhalchandra D. Dhokale
Electronics and Telecommunication
Dhole Patil College of Engg.
Pune, India
bhalchandradd@gmail.com

Prof. Ramesh Y. Mali
Electronics and Telecommunication
Maharashtra Institute of Technology
Pune, India.
Ramesh.mali@mitcoeedu.in

***Abstract*—**Strengthening the ownership rights on outsourced relational database is very important in today's internet environment. Especially where sensitive, valuable content is to be outsourced. Let us take an example of university database, weather data, stock market data, power consumption consumer behavior data, and medical and scientific data. Digital watermarking technique provides solution to the problem. Watermarking is the process in which an informal data is incorporated in original data to protect the owner's copyright over that content. Watermarking for relational data is made possible by fact that real data can very often tolerate a small amount of errors without any significant degradation with respect to their usability. Traditional watermarking schemes are sensitive to geometric distortions, in which synchronization for recovering embedded information is a challenging task because of the disorder caused by rotation, scaling or translation (RST). The existing RST-resistant watermarking methods still have limitations with respect to robustness, capacity or fidelity. Among these discrete Fourier transform (DFT) based watermarking algorithms have attracted researchers due to its simplicity and some attractive mathematical properties of DFT. Experimental results have been compared with existing algorithm which seems to be promising.

Keywords*-Image authentication, Reversible Watermarking, Geometric Attacks, DFT, RST*

*****

I. INTRODUCTION

More than 700 years ago, watermarks are used in Italy to indicate the paper brand and the mill that produced it [7]. By the 18th century watermarks began to be used as anticounterfeiting measures on money and other documents. The term watermark was introduced near the end of the 18th century. It was probably given because the marks resemble the effect of water on paper. The first example of technology similar to digital watermarking is a patent filled in 1954 by email hembrooke for identifying music works. In 1988, komastu and tominaga appear to be the first to use the term digital watermarking. About 1985, interest in digital watermarking began to mushroom [8]. The main aim of watermarking is to protect a certain data from unauthorized duplication and distribution by enabling provable ownership over the content [5]. More recently the focus of watermarking digital rights protection is shifting towards different data such as text, video, audio, software and relational data [10]. Watermarking embedding for relational data is made possible by the fact that real data can very often tolerate small amount of error without any significant degradation with respect to their usability. Detecting the watermark neither requires access the original data nor the watermark and the watermarking can be easily and efficiently maintained in the presence of insertion, updating and deletion. Secure watermarking embedding requires that the embedded watermark must not be easily tampered with, forged or removed from the watermarked data.

The watermark should also be imperceptible and should not degrade the quality of the image. In order to attain this, the watermark can be embedded in a domain such as the Discrete Fourier Transform (DFT), using the mid frequencies which do not contain visually important features of the image and hence largely unaffected by filtering and noise attacks. The DFT is sufficiently robust to signal processing attacks but very fragile to geometric attacks [1], [2]. There are a few geometric-distortion focused watermarking schemes; they can be roughly grouped into: moment-based, template-based, invariant domain-based and [2]. In this paper, we propose a novel watermarking technique for digital image that is invariant to rotation and translation, and resilient to scaling. The watermarking pattern of this technique is created from complex exponential function with random phase as spreading code. Embedding and detection are performed in frequency domain, i.e. discrete Fourier transform (DFT).

To obtain better imperceptibility as well as robustness, watermarking is done in frequency Domain. The frequency domain watermarking techniques are also called multiplicative watermarking techniques. Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) are most popular transforms operating in the frequency domain.[4] The mathematical description of each transform is given as under:

A. Discrete Fourier Transform (DFT):

For a length-M 1-D DFT, the relationship between the spatial/temporal domain signals, f[n], and their corresponding transform in the frequency domain, F[k],is

$$F[k] = \sum_{n=0}^{M-1} f[n] W_M^{kn} \tag{1}$$

Where $W_M^{kn} = e^{-2\pi r/M}$

For transform domain watermarking, three steps are generally followed:

- Image trans-formation
- Watermarking embedding
- Watermark recovery

Depending on application, image transform can be applied either on whole image or to block by block manner. Algorithms for achieving frequency domain watermarking would modify the selected coefficients in the transformed domain [5].

II. PROPOSED METHOD

In this paper an algorithm which combines DFT and Spread- Spectrum in the watermark embedding process. The embedding procedure can be summarized as follows. The LGB algorithm is used to design and obtain the codebook of the encoded image, the codebook again decomposed into *8-by-8* pixel blocks [7- 9] and the DFT coeffients of each block obtained. The DFT coeffients of the watermarks are then embedded into the coefficients of the codebook in the spread – spectrum format.

A. Embedding Procedure

- The LGB algorithm to construct a code book of the image with a codeword size of 8-by-8.
- Decomposed the image into 8-by-8 blocks of the codebook and compute a block-based DFT of the codebook and select the coefficients of the mid-frquency sub-band.
- Generate a pseudo-random sequence and select the value of β which controls the embedding strength.Embed the Watermarked into the selected mid-frequency sub-band using the pseudo-random(PN) sequence to determine the coefficients where the watermarked is embedded as follows:

$$I_i^{'} = I_i + \beta . I_i . W \tag{2}$$

- Where, I' and I represents the original and watermarked images respectively, W denotes the watermark and I represents the position to be embedded and is the watermark strength factor.
- Compute the inverse DFT of the watermarked codebook and then performed decoding to obtain the watermarked image.

B. Watermarked Recovery Procedure

For detection or verification, the receiver needs to verify if a specific watermarking pattern exists or not. A correlator is often used for full extraction of watermark. The correlation $C(I_0;W)$ between the possible attacked image I_0 and watermark W, can be calculated by

$$C_{(I',W)} = \frac{1}{L}\sum_{i=0}^{L-1} I_i^{'} . W_i \tag{3}$$

Given a pre-determined threshold T, it can be compared with the correlation given in ***Eq. 3*** for deciding the presence of the watermark. Therefore, the decision rule for presence of the watermark can be expressed by

$$C_{(I',W)} = \begin{cases} \geq T & watermark\ \ is\ \ present \\ < T & watermark\ \ is\ \ not\ \ present \end{cases} \tag{4}$$

The watermarked extraction process can be summarized as follows. Resynchronization, the codebook is obtained and the DFT coeffients obtain and the watermark extracted from the embedded positions. The process of watermark recovery from the image is given in this subsection as follow

- Obtain the codebook of resynchronized image and compute its DFT.
- Select mid-band frequencies and using the same PN sequence used in the embedding process check for the presence or absence of the embedded watermark using correlating the coeffients of the mid-band frequencies and PN sequence.
- Reconstruct the watermark using the extracted watermark bits.

Compute the correlation coefficient, between and the input watermark vector, as

$$D = \frac{w.v}{\sqrt{(w.w)(v.v)}} \tag{5}$$

If D is greater than a threshold, then indicate that the watermark is present. Otherwise, indicate that it is absent.

III. EXPERIMENTAL RESULTS

To evaluate the performance scheme, several experiments were performed to determine the visual perceptibility and robustness of the embedded watermark.

A. Visual Perceptibility

The watermark images were assessed for visual distortion and then Peak-signal-to Noise Ratio (PSNR) used to determine quality degradation as a of embedded watermark. For example, for the lena test image there is no visible degradation in quality at a PSNR value of 40.2 db. Similar observations were noted for other test images.

B. Resilient to Attack

The watermarked image is subjected to the variety of attacks, including signal processing attacks and geometric distortion attacks. The watermark was then extracted after restorations where necessary and the quality of the watermark computer using a Normalized cross-correlation (NC) factor.

The first attack to be stimulated was the rotation attack. Several rotation attack angles were simulated and then a reversal was done for each angle and the watermark extracted. Fig. 1 illustrates the probe and target triangle with an RF of 10 . The embedded watermark and the watermark that was recovered after restoring the attacked image to its original position are shown in fig. The recovered message has an NC of 0.71.

Figure 1. Attack Image (Lena) with 100 Rotational Attack.

Figure 2. Orignal Image and Recovered Image.

The second attack to be simulated was the scaling attack. The image was scaled from 25% to 125% of the original image size. At 25% of the original image size the recovered watermark was unsatisfactory, while scaling levels above 50% the watermark is recovered successfully after restoration. Fig. 3 shows the tessellation, probe triangle and the watermark recovered from the attacked image at an NC of 0.84.

Figure 3. Scaling Attack on Attack Image (Lena)

Figure 4. Scaling Orignal Image and Recovered Image

Figure 5. Various Images Used for DFT.

TABLE I. RESULT TABLE

Different Attacks	Lena				Barbara			
	PSI	***PSW***	***PNSR***	***NC***	***PSI***	***PSW***	***PNSR***	***NC***
Translational attack	60.9	67.6	44.9	0.81	86.9	67.6	41.0	0.82
Rotational Attacks	60.9	53.0	44.9	0.73	86.9	50.5	41.0	0.63
Scaling Attacks	60.9	67.3	44.9	0.72	86.9	58.2	41.0	0.62

Where,

PSI=Pixel similarity between original image and recovered image.

PSW=Pixel similarity between original watermark and extracted watermark.

PSNR = Peak Signal to Noise Ratio.

NC = Normalized Correlation.

CONCLUSION

In this paper we have demonstrated that a watermark can be recovered after RST attacks on an image by employing DFT techniques. In situations where RST attacks lead to formation of large dark regions, our proposed scheme of averaging has been shown to be effective in recovering the watermark at high NC factors. The scheme has been tested with success on various test images on a MATLAB Simulation platform

ACKNOWLEDGMENT

The author would like to thank Mr. Navnath S. Narawade (ME) Research Scholar, Dept of electronics Engg. Sant Gadgebaba, Amravati University, Amravati. For helpful discussion on DFT based algorithm watermarking.

REFERENCES

[1] S. Katzenbeisser, and F.A.P. Peti itcolas, Information HidingTechniques for Steganography and Digital Watermarking, MA,USA: Artech House Inc. 2000.

[2] R. Gonzalez, R.E. Woods, S.L. Eddins, Digital Image Processing, 3rd Edition, New Delhi, India: Prentice Hall of India Learning Pvt. Ltd, 2008.

[3] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Attacks on copyright marking systems," in Proc. Workshop Information Hiding, Portland, OR, Apr. 15–17, 1998.

[4] R. N. Bracewell, The Fourier Transform and Its Applications. NewYork: McGraw-Hill, 1986.

[5] Zheng, D., Zhao, J., Saddik, A.E.: 'RST-invariant digital image watermarking based on log-polar mapping and phase correlation', IEEE Trans. Circuit Syst. Video Technol., 2003, 13, (8), pp. 753–765

[6] Felix O. Owalla, Student Member," A Robust Image Watermarking Scheme Invariant to Rotation,Scaling and Translation Attacks" IEEE and Elijah Mwangi, Member, IEEE,2012

[7] IEEE Trans." Image Process". :Vol. 20, No. 12, pp.3524-3533, 2011.

[8] Ó Ruanaidh et al., "Rotation, Scale and Translation Invariant Digital Image Watermarking," Proc. IEEE Int. Conf. on Image Processing, Oct. 1997, pp. 536-539.*

[9] H.C. Huang, S.C. Chu "VQ-Based Watermarking Techniques", Journal of Comput., Vol.17, No.2,pp.37-50, July 2006.

[10] Wilson Wai Lun FUNG and Akiomi KUNISA," rotation, scaling, and translation-invariant multi-bit watermarking based on log-polar mapping and discrete fourier transform" 0-7803-9332-5/05 ©2005,IEEE.

[11] I. Cox, M. Miller, and J. Bloom, Digital Watermarking. New York:Morgan Kaufmann, 2002.

[12] I. J. Cox, M. L. Miller, and J. A. Bloom," Digital Watermarking", SanFrancisco, CA: Morgan, Kaufman, 2001.

[13] S. Katzenbeisser, and F.A.P. Petiitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, MA, USA: Artech house Inc. 2000.

[14] C.-H. Tang and H.-M. Hang. "A Feature-Based Robust Image Digital Image Watermarking Scheme," IEEE Trans. Signal Process., Vol. 51, No. 4, pp. 950-959, 2003.