A Robust Image Watermarking Scheme Invariant to Rotation, Scaling and Translation Attack using DFT

Bhalchandra D. Dhokale, Ramesh Y. Mali

Abstract— Rapid development of digital technology has improved the ease of access to digital information copied, processed, stored and distributed among unauthorized users using freely available software. It also leads to the consequence of making the illegal production and redistribution of digital media easy and undetectable. Hence, the risk of copyright violation of multimedia data has increased due to the enormous growth of computer networks So, 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... Traditional watermarking schemes are sensitive to geometric distortions, in which synchronisation 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 and fidelity. Several types of watermarking algorithms have been developed so far each of which has its own advantage and limitations. 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.

Index Terms— Rotation, RST, DFT, scale, translation, watermarking.

I. INTRODUCTION

There has been much emphasis on the robustness of watermarks to common signal processing operations such as compression and signal filtering. However, recently it has become clear that even very small geometric distortions can prevent the detection of a watermark. If the original image is available to the detector, then the watermarked image can often be registered to the original and the geometric distortion thereby inverted. Blind detection requires that detection of the watermark be performed without access to the original unwatermarked image [7, 8]. As such, it is not possible to invert the geometric distortion based on registration of the watermarked and original images. Before proceeding further, it is important define what we mean by the geometric distortions of rotation, scale and translation. Specifically, we are interested interested in the situation in watermarked image undergoes an unknown rotation, scale, and translation prior to the detection of the watermark [2,3].

Manuscript Received on June 2014.

Mr. Bhalchandra D. Dhokale, Electronics and Telecommunication University of Pune, Dhole Patil College of Engineering, Pune, India.

Mr. Ramesh Y. Mali, Electronics and Telecommunication University of Pune, Maharashtra Institute of Technology College of Engineering, Pune, India.

The detector should detect the watermark if it is present. This definition is somewhat obvious, so it may be more useful to describe what we are not interested in particular, some watermark algorithms. Claim robustness to scale changes by first embedding a watermark at a canonical scale, then changing the size of the image, and finally, at the detector, scaling the image back to the canonical size prior to correlation. In our opinion, that detector does not see a scale change. Rather, the process is more closely approximated by a low pass filtering operation that occurs when the image is reduced in size. In the scaling degradation with which we are concerned, the detector is unaware of the scaling and cannot rescale or pad to the original size. Similarly, tests that rotate an image by some number of degrees and subsequently rotate the image by the same amount in the opposite direction are not adequate tests of robustness to rotation. The same is true for translation. The common situation we are concerned with when a watermarked image is printed and then cropped or padded and scanned back into the digital domain. In these circumstances, the image dimensions have changed both because of cropping and possibly scaling [2,3]. There is also likely to be an associated translational shift. We assume that the detector is not informed of the rotation, scale, and translation parameters. In this example, scaling to a canonical size does not undo the scaling. In this project, we propose a new watermarking system using discrete Fourier transform (DFT) to achieve robustness against RST distortions. This system embeds the watermark in a rotation and translation (RT) invariant domain, and handles scaling via a simple search along the log-radius axis. The original cover image is not required during watermark extraction. This proposed system is a multi-bit watermarking system, which has considerably broader applications than other RST-resilient zero-bit watermarking techniques [6]. In this project we shall review the material which is related to our research problems: the copyright protection and authentication of medical images. The state-of-art in the literature will be reviewed to provide a foundation for the evaluation of the proposed approaches. This chapter is divided into two main parts. In first part the background knowledge and requirements of watermarking are reviewed and in second part, the state-of-art medical image watermarking systems are reviewed. 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:

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

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 digital image 2D DFT can be define as,

$$Y(u,v)=\sum_{i=0}^{M-1}\sum_{i=0}^{N-1} X(i,\mathrm{j}).\mathrm{W}_M^{iu}.\mathrm{W}_N^{ju} \tag{2}$$

The DFT of an image is always

$$M(u,v)=|Y(u,v)|$$
$$\phi(u,v)=\angle Y(u,v) \tag{3}$$

For transform domain watermarking, three steps are generally followed:

i. Image trans-formation
ii. Watermarking embedding
iii. 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]. Generally the following formula is use

$$I_i^{'} = I_i + \alpha.I_i.W \tag{4}$$

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. 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

$$C_{(I',W)}=\frac{1}{L}\sum_{i=0}^{L-1} I_i^{'}.W_i \tag{5}$$

Given a pre-determined threshold T, it can be compared with the correlation given in Eq. 5 for deciding the presence of the watermark. Therefore, the decision rule for presence of the watermark can be expressed by

$$C_{(I',W)}=\begin{cases}\geq T & \text{watermark is present}\\ <T & \text{watermark is not present}\end{cases} \tag{6}$$

II. Styles of Robust Watermark

The different styles of robust watermark are reported in literature. Few of them are described here.

A. *Noise Watermark*

Noise watermark is most commonly used type of robust watermark. For the reason of security and statistical undetectivity, it is demonstrated that the watermark is most secure, if it is in the form of Gaussian random sequence. To measure the similarity between original and extracted sequence, the correlation value is used to indicate the similarity.

B. *Logo Watermark*

Logo is another form of robust watermark. The logo is small image pattern in binary form. It can be company logo used in commercial applications. The quality of logo image is measured by human perception. That is, it is subjective measure of verifying authenticity of the digital content. We have used the AGA Khan Hospital logo for authentication of CT scan medical images [3].

C. *Message Watermark*

Message watermark is comprised of text. Message watermark has the advantage of easy to use in comparison with noise-type watermark or logo watermark. However, the message watermark require bit error rate approaching to zero, because any bit error will cause major fault in the final result. In most cases it is required that information with at least 64 bit (or 8 ASCII character can be carried by multimedia) [6].

III. Algorithm

Consider an image i(x,y) and a RST version of the image i'(x.y):

$$i^{'}(x,y)=i(\sigma(x\cos\alpha+y\sin\alpha)-x_0,\ \sigma(-x\sin\alpha+y\cos\alpha)-y_0) \tag{7}$$

The Fourier Transform is I'(fx , fy):

$$|I^{'}(f_x,f_y)|=|\sigma|^{-2}|I(\sigma^{-1}(f_x\cos\alpha+f_y\sin\alpha),\ \alpha^{-1}(-f_x\sin\alpha+f_y\cos\alpha))| \tag{8}$$

For find more invariant value, we define:

$$g(\theta)=\sum_j \log(|I(\rho_j,\theta)|) \tag{9}$$

It would be more better to compute the value below

$$g_1(\theta^{'})=g(\theta^{'})+g(\theta^{'}+90^{\circ}) \tag{10}$$

It is invariant to both translation and scaling. Rotation result in a shift of its values. So by using this algorithm we are able to remove RST attacks.[1]

A. *Watermark Embedding Process:*

Once a method for detecting watermarks has been defined, we can construct a watermark embedding algorithm according to the methodology described in. In that paper, watermarking is cast as a case of communications with side information at the transmitter, which is a configuration studied by Shannon. The difference between this view of watermarking, and a more common view, is as follows. Most public watermarking

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

methods found in the literature use blind embedding in that the original image is considered to be noise. The embedder adds a small-amplitude signal to this noise, and the detector must be sensitive enough to work with the small signal-to-noise ratio those results [7, 8]. However, this common approach ignores the fact that the embedder has complete knowledge of the "noise" caused by the original image. If we view the embedder as a transmitter and the cover image as a communications channel, then this knowledge amounts to side-information about the behavior of that channel. When the transmitter knows ahead of time what noise will be added to the signal, its optimal strategy is to subtract that noise from the signal before transmission. The noise then gets added back by the communications channel, and the receiver receives a perfect reconstruction of the intended signal. In the case of watermarking, it is unacceptable for the embedder to subtract the original image from the watermark before embedding the watermark, because it would result in unacceptable fidelity loss. In fact, if the watermark is expressed as a pattern that is the same size as the image, then this strategy simply replaces the image with the watermark pattern, which is clearly too drastic. However, when the watermark is expressed as a signal in a lower-dimensional space, as is the case with the present system, the results need not be so drastic, since a wide variety of full-resolution images project into the same extracted signal and the embedded may choose the one that most resembles the original. But even in the case of lower-dimensional watermarks, it is not always possible to completely replace the extracted signal with the watermark signal while maintaining acceptable fidelity. To make maximal use of the side-information at the embedder, while maintaining acceptable fidelity [1].

The basic approach for embedding described in consists of three steps:-

i. Apply the same signal-extraction process to the unwatermarked image as will be applied by the detector, thus obtaining an extracted vector. In our case, this means computing.
ii. Use the mixing function, to obtain a mixture between v and the desired watermark vector. At present, our mixing function simply computes a weighted average w of v and u, which is a highly sub-optimal approach.
iii. Modify the original image so that, when the signal-extraction process is applied to it, the result will be instead of v .

This process is implemented as follows:

a. Modify all the values in column of the log-polar Fourier transform so that their logs sum to instead of this could be done, for example, by adding to each of K the values in column [6]. Care must be taken to preserve the symmetry of DFT coefficients.
b. Invert the log-polar resembling of the Fourier magnitudes, thus obtaining a modified, Cartesian Fourier magnitude.
c. The complex terms of the original Fourier transform are scaled to have the new magnitudes found in the modified Fourier transform.
d. The inverse Fourier transform is applied to obtain the watermarked image.

Unfortunately, there is inherent instability in inverting the log-polar resampling of the Fourier magnitude (Step b) [6]. We therefore approximate this step with an iterative method in which a local inversion of the interpolation function is used for the resampling [1].

B. Watermark Detection Process

The basic algorithm for watermark detection proceeds as follows.

i. Compute a discrete log-polar Fourier transform of the input image as described in Section III-A [6]. This can be thought of as an array K of rows N by columns, in which each row corresponds to a value of, and each column corresponds to a value of .
ii. Sum the logs of all the values in each column, and add the result of summing column to the result of summing column

$$j = N/2\,(j = 0 \cdots ((n/2) - 1) \tag{11}$$

to obtain an invariant descriptor , in which

$$v_j = g_1(\theta_j) \tag{12}$$

Where, θ_j, is the angle that corresponds to column in the discrete log-polar Fourier transform matrix [6].

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

$$D = \frac{w.v}{\sqrt{(w.w)(v.v)}} \tag{13}$$

iv. If D is greater than a threshold , then indicate that the watermark is present. Otherwise, indicate that it is absent [1]

IV. RESULT

The watermarked image was subjected to a 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 simulated was the rotation attack several rotation attack angles were simulated and then a reversal was done for each angle and the watermark extracted. illustrates the probe and target triangle with an *RF* of 10 degree. The embedded watermark and the watermark that was recovered after restoring the attacked image to its original position are shown in fig. 3 The recovered message has an NC of 0.63

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

Fig. 1 Attack Image

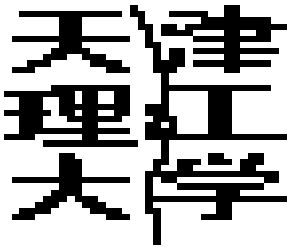

Fig. 2 Original Image

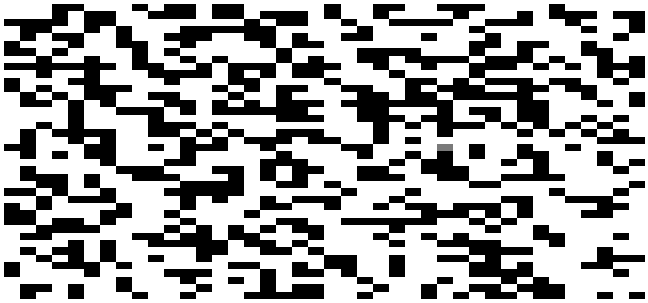

Fig. 3 Recover Image

Fig. 4 Attach Image

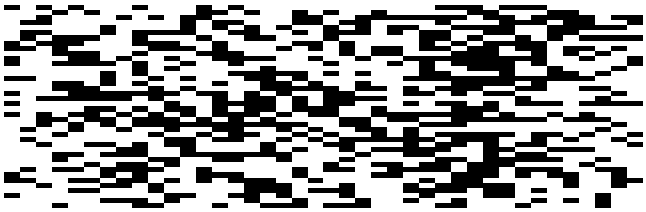

Fig. 5 Recover Image

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. 5 shows the tessellation, probe triangle and the watermark recovered from the attacked image at an *NC* of 0.74.

Table I: Result

Different Attacks	Lena Result			
	PSI (%)	PSW (%)	PSNR (dB)	NC
Translational Attack(10)	63.97	71.62	45.91	0.83
Rotation Attack(10^0)	63.97	55.06	45.91	0.67
Scaling(1.1)	63.97	70.3	45.91	0.79
Rotation Attack(90^0)	63.97	45.18	45.91	0.47
Scaling(2)	63.97	79.31	45.91	0.85

where,

PSI=Pixel similarity between original image and recovered image.

PSW=Pixel similarity between original watermark and extracted watermark.

Translation attacks for various *TF* were also simulated and The watermark was recovered satisfactorily. Computer simulation experiments were also conducted with other common test images such as Barbara, Peppers, Lena and Baboon among others. These experiments tested the robustness of the watermark to signal processing attacks such as JPEG compression and histogram equalization.

Fig6.We has Implemented Our Algorithm Using Above Images.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

V. CONCLUSION

Several types of watermarking algorithms have been developed so far each of which has its own advantage and limitations. No method can provide fully perfect solution. Each type of solution has robustness to some type of attacks but is less resilient to some other types of attacks. Main focus of the current research in this field is to make the watermarking algorithms resilient to geometric transformations. In case of practical application, choice of solution type actually depends on the nature of application and requirements Instead of creating a truly RST invariant signal, we create a signal that changes in a trivial manner when undergo RST attack. The calculation of this projection is performed by taking the Fourier transform of the image, performing a log-polar resampling, and then integrating along the radial dimension. We note that an alternative implementation can be performed using the Radon transform. We have investigated this implementation but do not report it here. Future work will focus on more effective embedding and RST resilient watermarking designed to survive cropping and compression.

VI. 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] Felix O. Owalla, Student Member," A Robust Image Watermarking Scheme Invariant to Rotation,Scaling and Translation Attacks" IEEE and Elijah Mwangi, Member, IEEE,2012
[2] IEEE Trans." Image Process". :Vol. 20, No. 12, pp.3524-3533, 2011.
[3] Ó Ruanaidh et al., "Rotation, Scale and Translation Invariant Digital Image Watermarking," Proc. IEEE Int. Conf. on Image Processing, Oct. 1997, pp. 536-539.*
[4] R. Gonzalez, R.E. Woods, S.LProcessing, 3rd Edition, New Delhi, InLearning Pvt. Ltd, 2008.
[5] H.C. Huang, S.C. Chu "VQ-Based Watermarking Techniques", Journal of Comput., Vol.17, No.2,pp.37-50, July 2006.
[6] 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.
[7] I. Cox, M. Miller, and J. Bloom, Digital Watermarking. New York:Morgan Kaufmann, 2002.
[8] I. J. Cox, M. L. Miller, and J. A. Bloom," Digital Watermarking", SanFrancisco, CA: Morgan, Kaufman, 2001.

Mr Bhalchandra D Dhokale, is PG Engineering. Student in Electronic & Telecommunication. Publish three papers in International and Nation journals and also doing research on Image processing. Particularly robust watermarking for geometric attack in Dhole Patil College of Engineering, wagholi, Pune.

Ramesh Y. Mali, is Assistant Professor in Electronics & Telecommunication Department of Maharashtra Institute of Technology College of Engineering. Kothrud, Pune. He is pursuing Ph.D from University of Pune. He received the M.E. (Electronics) in 2006 from Bharati Vidyapeet, Pune University of Pune, He received the B.E. (Electronics)in 2001 from PVPIT, Sangli, under Shivaji University, Satara, Publish several papers in International and Nation journals and also doing research in image and signal processing, particularly in robust reversible watermarking.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.