Rotation, Scale, and Translation Resilient Digital Watermark Based on Complex Exponential Function

Siriporn Pholsomboon and Sartid Vongpradhip, Non-members

ABSTRACT

In this paper, a novel digital image watermarking scheme has been proposed based on spread spectrum technique. By exploiting complex exponential function to generate a multiple-rings shaped pattern, the watermark is invariant to rotation and translation, and resilient to scaling without truly inverse transformation needed. The proposed scheme is performed in regular frequency domain without additional log-polar mapping required which can reduce computational complexity of such transformation. Furthermore, the original image is not needed for detection in this scheme. Experimental results against translation, rotation, scaling, JPEG compression, brightness adjustment, image filtering, noise adding, printing-and-scanning, watermark counterfeiting, and collision attacking demonstrate performance of the proposed scheme that the watermark is correctly detected although the image was undergone by various geometric and non-geometric transformations.

Keywords: Digital Image Watermarking, Copyright Protection, Rotation, Scale, and Translation (RST) Resilient, Complex Exponential Function

1. INTRODUCTION

The rapid growth of information technology makes accessing information much easier than before and causes many multimedia data needed to be protected from piracy at the same time. Researches on copyright protections have greatly been spent in these several years. This leads to an application of digital watermarking that embeds small information about copyright or ownership without introducing of visible change on digital media [1-2]. A robust digital watermark must be recognizable although the embedded media have been severely degraded by most transformations [3-4].

Many robust digital watermarking schemes for images have been proposed, mainly based on spread spectrum principle [5]. The original proposed scheme requires inverse operation in detection if a test image has been geometrically transformed. For instance, if the image is rotated by any angle, the image is needed to be rotated back to its original orientation. Such operation requires huge calculation and this becomes more complex when more transformations have been applied.

Although there are some spread-spectrum-watermarking schemes invariant to RST (Rotate, Scale, and Translation) transformations in which no additional inverse operation is needed in detection [6-10]. The schemes are performed in log-polar coordinate of Fourier domain called Fourier-Mellin. The concept is perfect in theory but very difficult in practice. Those schemes require additional Log-Polar mapping (LPM) and inverse Log-Polar mapping (ILPM) beyond fundamental frequency transformation in both processes of embedding and detection. As described in the literatures, there are many difficulties and problems in practical implementation. Furthermore, to obtain an adequately fine quality of embedded image, the resolution of the LPM and ILPM at least $256 \times 256$ must be used [6]. As a result, sophisticated algorithm must be investigated in order to avoid unacceptable computational imprecision of such samplings. This is clearly additional complexity other than essential watermarking process.

In this paper, we propose a novel watermarking scheme for digital image that is invariant to rotation and translation, and resilient to scaling. The watermarking pattern of this scheme 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). The watermark has a multiple-rings shape, which is not exactly circularly symmetric. This is contrasted to the circularly symmetric watermark scheme as proposed in [11] that their watermarking pattern is constructed from a binary sequence (-1, 1). To allow for arbitrary rotating angle, the watermark pattern along each ring of their scheme needs to be kept constant. This greatly limits the ‘spreading’ capability of the watermark pattern. As a result, larger watermarking pattern is needed to achieve reliable detection [12].

The scheme proposed here can reduce complexity in not only the inverse transformation needed, but also additional calculation for conversions between regular frequency domain and log-polar domain re-
required in those LPM-based schemes. Furthermore, the scheme does not even require an original image in detection process. This can reduce unnecessary computation time of searching for the original image as well as ignore space needed for keeping. However, the scheme can also be applied in spatial domain as described in [12-13].

2. PROPOSED SCHEME

The proposed watermarking pattern is constructed in circular shape, based on spread spectrum technique. The watermark is separated into rings in which each one represents each spreading code of the watermark. Fig.1 shows an example of the pattern. Let \((r, \theta)\) be a position in polar coordinate with a corresponding \((x, y)\) in Cartesian coordinate. By exploiting complex exponential function, the watermarking pattern is represented by

\[
W(r, \theta) = e^{j(\omega \theta + \phi_r)}
\]  

(1)

where \(\omega\) and \(\phi_r\) are arbitrary angular frequency and random phase, respectively. Let \(R\) be radius of the outermost ring, \(1 \leq r \leq R\) and \(0 \leq \theta < 2\pi\).

Let \(f(x, y)\) be an image of size \(M \times N\), the DFT and the inverse discrete Fourier transform (IDFT) of \(f(x, y)\) are defined as follows [14]:

\[
F(u, v) = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y)e^{-j2\pi(\frac{ux}{M} + \frac{vy}{N})} \tag{2}
\]

\[
f(x, y) = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u, v)e^{j2\pi(\frac{ux}{M} + \frac{vy}{N})} \tag{3}
\]

The watermarked image \(F'(u, v)\) in frequency domain is obtained by

\[
F'(u, v) = (|F(u, v)|(1 + \alpha W(x, y)))e^{j\Phi(u, v)} \tag{4}
\]

where \(|F(u, v)|\) and \(\Phi(u, v)\) are Fourier spectrum and phase angle of \(F(u, v)\), respectively. An \(\alpha\) is a watermarking strength factor which can be viewed as a relative measure of how much the image should be modified to alter the perceptual quality. Choice of \(\alpha\) may vary based on some general assumption as suggested in [5]. Note that \(W(x, y)\) may have the same size as that of \(f(x, y)\) or smaller. In case that the watermark is smaller than the image, zeros must be padded to the outside of the watermark as wrapping around. If the size of the watermark is too small, then only the high frequency components in the magnitude spectrum of image will be embedded. This is contrary to [8] and [11] which suggested that watermark should be spread between the most and the least significant frequency components in order to keep robustness against lossy compression or filtering processes and fidelity of the image at the same time. For our proposed watermark, the larger the pattern, the wider the range of magnitude spectrum of image is embedded. Fig. 2 shows an example of watermarked image compared with its original one using watermarking strength factor \(\alpha = 0.2\). To yield the watermarked image \(f'(x, y)\), simply apply IDFT to \(F'(u, v)\)

\[
f'(x, y) = IDFT(F'(u, v)) \tag{5}
\]

Fig. 3 compares frameworks of embedding process between LPM-based scheme (from [6]) and the proposed scheme which clearly manifests that the proposed scheme requires less computation since it does not need LPM and ILPM conversions.

Detection process for the presence of the watermark can be done without needing of original image which avoids unnecessary computation for the searching. Let \(g(x, y)\) be a possibly watermarked image, we have

\[
D(u, v) = \log(1 + |G(u, v)|) \tag{6}
\]

as an intensity displaying function for Fourier spectra of \(g(x, y)\) [14]. The watermark is detected by computing the correlation between \(D(u, v)\) and the original
watermark $W(x, y)$ by using similarity function [5], [15]

$$\text{sim}(D, W) = \frac{\sum_{u=0}^{M-1} \sum_{v=0}^{N-1} D(u, v) W^*(x, y)}{\sqrt{\sum_{u=0}^{M-1} \sum_{v=0}^{N-1} D(u, v) D^*(x, y)}}$$

where $W^*(x, y)$ and $D^*(u, v)$ are the complex conjugates.

Assuming that $D(u, v)$ and $W(x, y)$ are independently distributed according to $N(0, 1)$ (where $N(\mu, \sigma^2)$ denotes a normal distribution with mean $\mu$ and variance $\sigma^2$), then sim $(D, W)$ will be distributed according to $N(0, 1)$. This watermark detection function follows that of [5]. The watermark is successfully detected if sim $(D, W)$ is greater than predefined threshold $\delta$ (for example, $\delta = 6$ as suggested in [5]).

Fig. 4 compares frameworks of detection process between LPM-based scheme (from [6]) and the proposed scheme. Again, it is clearly that the proposed
scheme requires less complexity since it does not need LPM conversion nor the original image that ignores unnecessary computation time of searching and space needed for keeping the image.

3. ROBUSTNESS TO GEOMETRICAL TRANSFORMATIONS

To show how the described watermark is invariant to translation and rotation, and resilient to scaling, consider the properties of the Fourier representations below.

3.1 Translation Invariant

Shifts in spatial domain do not effect the magnitude of its Fourier transform [14]

\[
f(x - x_0, y - y_0) \Leftrightarrow F(u, v)e^{-j2\pi(\frac{ux_0 + vy_0}{N})}
\]

\[
|F(u, v)e^{-j2\pi(\frac{ux_0 + vy_0}{N})}| = |F(u, v)|
\]

It is clear that spatial shifts affect only the phase components of an image, which is known as circular translation invariant [6].

3.2 Rotation Invariant

Rotation in the spatial domain causes the Fourier components to be rotated through the same angle in frequency domain [14]

\[
f(r, \theta + \theta_0) \Leftrightarrow F(\Omega, \Phi + \theta_0)
\]

where \((\Omega, \Phi)\) is a corresponding polar-coordinate point of \((u, v)\) in frequency domain.

For any rotated angle \(\epsilon\), \(W'(r, \theta)\)can be rewritten as

\[
W'(r, \theta) = e^{j(\omega r + \epsilon) + \phi_r}
\]

Correlation between the original watermark \(W(r, \theta)\) and the rotated one \(W'(r, \theta)\) is defined by

\[
W(r, \theta) \circ W'(r, \theta) = \int_{\theta=0}^{2\pi} e^{-j(\omega r + \phi_r)} e^{j(\omega r + \epsilon + \phi_r)} d\theta
\]

\[
= |\int_{\theta=0}^{2\pi} e^{j(-\omega \epsilon - \phi_r + \omega \epsilon + \phi_r)} d\theta|
\]

\[
= |\int_{\theta=-\pi}^{\pi} e^{j\omega \epsilon} d\theta|
\]

\[
= |e^{j\omega \epsilon (2\pi - 0)}|
\]

\[
= 2\pi
\]

By using standard trigonometry and the well-known Euler’s formula, it can be shown that \(W(r, \theta) \circ W'(r, \theta) = 2\pi\) irrespectively of the rotated angle \(\epsilon\). This is proven that the proposed watermark gives a constant result of correlation without additional inverse rotation required.

3.3 Scale Resilient

Scaling the image in the spatial domain causes an inverse scaling in the frequency domain [14]

\[
f(ax, by) \Leftrightarrow \frac{1}{|ab|}F\left(\frac{u}{a}, \frac{v}{b}\right)
\]

As the pattern of the proposed watermark has a multiple-rings shape in which each ring is constructed by same property, i.e. same angular frequency, but different random phases, this implies that inner and outer rings are scaled versions of each other. Consider the correlation between two different rings below

\[
W(r_1, \theta) \circ W'(r_2, \theta) = \int_{\theta=0}^{2\pi} e^{-j(\omega \theta + \phi_r)} e^{j(\omega \theta + \phi_r)} d\theta
\]

\[
= |\int_{\theta=0}^{2\pi} e^{j(-\omega \phi_r - \omega \phi_r)} d\theta|
\]

\[
= |\int_{\theta=0}^{2\pi} e^{j(-\phi_r + \phi_r)(2\pi - 0)} d\theta|
\]

\[
= 2\pi
\]

By using the same derivation as that of (12-16), the result of \(W(r_1, \theta) \circ W'(r_2, \theta) = 2\pi\) regardless of random phase \(\phi_r\). This is shown that scaling the size of the pattern does not effect the value of correlation when consider to a particular pair of rings. Thus, if the watermarked image is scaled, the original watermark does not need to be resized correspondingly to the new size of scaled image in detection. However, in practice, the new size of scaled image will differ from the original size of watermark. Therefore, if the watermarked image is enlarged, zeros must be padded to the outside of the watermark to avoid wrap-around error. In case that the image is reduced, then only center of the watermark of the corresponding size should be cropped and remained. No further sophisticated calculation is required before the similarity function. The property of such multiple-rings shape is not exactly ‘invariant’ to scale, but rather ‘resilient’.

4. EXPERIMENTAL RESULTS

In this section, we illustrate performance of the proposed scheme against translation, rotation, scaling, JPEG compression, brightness adjustment, filtering, noise adding, printing-and-scanning, watermark counterfeiting, and collision attacking. Experimental results on dominant horizontal and vertical structured images are also provided as well as the performance comparison against the original LPM-based scheme. The original image Lena of size 512×512 was tested using watermarking strength factor \(\alpha = 0.2\). The watermarked image was imperceptible without comparing to the original one (as shown in Fig. 2).
The PSNR (Peak Signal-to-Noise Ratio) of the watermarked image was 44.92 dB.

4.1 Translation

We first performed experiment with translation. The outside of the original image was padded with 100 zeros each that made the image became size $712 \times 712$. Fig. 5 (a) shows the result. The proposed watermark was constructed using (1) with size $R = 356$ and angular frequency $\omega = 32$. The padded image was watermarked and then replaced with zeros again to the padded area in order to see the result of translation-invariant property. Translation experiment was performed by shifting only the image part by 100 pixels up, down, left, and right. Fig. 5 (b) shows an example of the shifted image. Table 1 shows the similarity values obtained from each translation using (7). From the result, it is clear that translation does not effect the correlation result since the magnitude part of image is not changed.

<table>
<thead>
<tr>
<th>Translation</th>
<th>Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 pixels left &amp; up</td>
<td>52.0730</td>
</tr>
<tr>
<td>100 pixels up</td>
<td>52.0730</td>
</tr>
<tr>
<td>100 pixels right &amp; up</td>
<td>52.0730</td>
</tr>
<tr>
<td>100 pixels left</td>
<td>52.0730</td>
</tr>
<tr>
<td>No translation</td>
<td>52.0730</td>
</tr>
<tr>
<td>100 pixels right</td>
<td>52.0730</td>
</tr>
<tr>
<td>100 pixels left &amp; down</td>
<td>52.0730</td>
</tr>
<tr>
<td>100 pixels down</td>
<td>52.0730</td>
</tr>
<tr>
<td>100 pixels right &amp; down</td>
<td>52.0730</td>
</tr>
</tbody>
</table>

4.2 Rotation

Next, we performed experiment with rotation. The outside of the original image was padded with zeros to the possibly maximum size when it is rotated. In this case, the image was padded to $725 \times 725$. A second watermark was constructed with size $R = 362$ and $\omega = 32$. The watermark was then embedded into the padded original image. Rotation was applied to the image at various degrees with step size of 5 degrees from 0 to 355. At each step of rotation, the image was cropped to the original padded size. This obviously removed some watermark components off. Fig. 6 shows an example of the experiment. Fig. 7 shows the similarity values obtained from each rotation angle. As the result, the watermark was correctly detected at all degrees of rotation, using detection threshold $\delta = 6$. Note that the correlation results decrease as the watermarked part was cropped larger.

4.3 Scaling

We next performed experiment with scaling. Third watermark was constructed with size $R = 256$ and $\omega = 32$ (This watermark is used in the all following experiments.) The watermark was embedded into the original image without padding. The watermarked image was then resized by different factors with step of 2.5% from 50% to 200%. The result presented in Fig. 8 shows that the watermark was successfully detected at all experimented scaling sizes. Note that the value changes up and down alternatively due to
incompletely matching between rings of the original watermark and the scaled image.

4.4 JPEG Compression

We next experimented on JPEG compression. The watermarked image was compressed by quality factors at 75%, 50%, 25%, 10%, and 5%. Fig. 9 shows the result of similarity values. The watermark was still detectable although the image was severely compressed.

4.5 Brightness Adjustment

We next experimented on brightness adjustment. The watermarked image was adjusted the brightness by factors from -100% to 100% with step of 10%. Fig. 10 shows the result of similarity values.

4.6 Filtering

We next experimented on image filtering. The watermarked image was blurred and sharpened using different sizes of masking: $3 \times 3$, $5 \times 5$, and $7 \times 7$. Fig. 11 shows the result of similarity values.

4.7 Noise Adding

We next experimented on noise adding. The watermarked image was added Salt & Pepper noise at different intensities from 10% to 100% with step of 10%. Fig. 12 shows the result of similarity values.

4.8 Printing and Scanning

We next experimented on printing and scanning. The watermarked image was laser printed at 1200 × 1200 dpi and then scanned back at 1200 × 1200 dpi. Fig. 13 shows result of the image. The watermark was still detected and the similarity value was 32.9223.
4.9 Watermark Counterfeiting

We next experimented on watermark counterfeiting. The watermarked image was tested for the presence of 99 uncorrelated watermarks. Fig. 14 shows the result of similarity values obtained from each watermark. Only one (true) watermark matched gives high correlation value, while the other 99 uncorrelated watermarks have the similarity values distributed between 0 and 3 according to [5].

4.10 Collision Attacking

We next experimented on collision attacking. The watermarked image was re-watermarked again with another 4 different random watermarks. Detection process was then performed. All 5 watermarks were successfully detected on the final watermarked image. Table 2 shows the similarity values obtained from each watermark. Although all 4 versions of fake watermarks are successfully detected on the final multi-watermarked image, but in fact there is only one version of watermarked image that contains only the first (true) watermark. In this case, therefore, the genuine owner can prove his true ownership by showing the first watermarked image version that contains no other watermarks.

4.11 Perceptibility Measuring

We also performed measurement on perceptibility against specific structures of image. Images with a particular structure usually have a large amount of energy in one group of directions while having much lower energy in an orthogonal way [7]. In this experiment, a dominant horizontal structured image Beach of size 512 × 512 (Fig. 15) and a dominant vertical structured image Timberland of size 512 × 512 (Fig. 16) were tested using watermarking strength factor \( \alpha = 0.2 \). Both watermarked images were a little noticeable. The PSNR of Fig. 15 was 33.93 and was 31.80 in Fig. 16. Correlation values at no transformation taken were 34.81 and 37.27, respectively. However, to compensate the quality of the watermarked image, the watermarking strength factor can be slightly decreased in order to improve the value of PSNR. From the result, it is proven that the proposed scheme requires much less computation than the original LPM-based scheme. This advantage conquers limitation in practical implementation of those LPM-based schemes.

5. CONCLUSION

In this paper, we proposed a novel digital watermarking scheme that is invariant to rotation and
translation, and also resilient to scaling. The described scheme has circular shape with multiple rings constructed by exploiting complex exponential formula. Experimental results shown in Section 4 demonstrate performance of the watermark that is robust to translation, rotation, and reasonable range of scaling. The watermark was correctly detected without inverse transformation or original image required. The watermark is also robust to JPEG compression as well as other non-geometric transformations including subterfuge attack and watermark counterfeiting. Similar results were found on other standard tested images (e.g. Cameraman, Baboon, Peppers, for example) but are not reported here. Performance comparison against the original LPM-based scheme shows that the proposed scheme consumes much less computational complexity. The proposed scheme also profits more advantage that it does not require the original image in detection process, which can reduce unnecessary computation time of searching and space needed for keeping the image.

Table 3: Number of FLOPs of Embedding Process.

<table>
<thead>
<tr>
<th>Step</th>
<th>The original LPM-based scheme</th>
<th>The proposed scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>DFT</td>
<td>20089856</td>
<td>20089856</td>
</tr>
<tr>
<td>IDFT(1)</td>
<td>21662722</td>
<td>-</td>
</tr>
<tr>
<td>ILPM</td>
<td>58760305</td>
<td>-</td>
</tr>
<tr>
<td>IDFT(2)</td>
<td>21662722</td>
<td>21662722</td>
</tr>
<tr>
<td>Add watermark</td>
<td>786432</td>
<td>5767176</td>
</tr>
<tr>
<td>Total</td>
<td>122963037</td>
<td>47519754</td>
</tr>
</tbody>
</table>

Table 4: Number of FLOPs of Detection Process.

<table>
<thead>
<tr>
<th>Step</th>
<th>The original LPM-based scheme</th>
<th>The proposed scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>DFT(1)</td>
<td>20089856</td>
<td>20089856</td>
</tr>
<tr>
<td>Intensity Display</td>
<td>-</td>
<td>1572868</td>
</tr>
<tr>
<td>ILPM</td>
<td>58760305</td>
<td>-</td>
</tr>
<tr>
<td>DFT(2)</td>
<td>20089856</td>
<td>-</td>
</tr>
<tr>
<td>Correlation</td>
<td>4194320</td>
<td>2622987</td>
</tr>
<tr>
<td>Total</td>
<td>103134337</td>
<td>24285711</td>
</tr>
</tbody>
</table>

References

Siriporn Pholsomboon was born in Bangkok, Thailand, in 1977. She received the B.S. degree in computer science from Ramkhamhaeng University in 1995. She was with Research Center for Communications and Information Technology (ReCCIT) and received the M.S. degree in information technology from King Mongkut’s Institute of Technology Ladkrabang (KMITL) in 2000. She is currently pursuing the Ph.D. degree in Computer Engineering at Chulalongkorn University where she has joined Digital System Engineering Laboratory (DSEL) since 2002. Her research interests include digital image processing, data hiding, digital watermarking, and information security.

Sartid Vongpradhip was born in Bangkok, Thailand, in 1954. He received his Bachelor degree (honors) in Electrical and Electronic Engineering from Newcastle Upon Tyne Polytechnic in 1979 and Master degree in Electronics Engineering from King’s College University of London in 1981. He became a lecturer at the Department of Computer Engineering, Chulalongkorn University in 1983. He received a scholarship from Chulalongkorn University, in 1990, to continue his study in Digital System Engineering at The University of Technology Sydney, Australia, and received his Ph.D. in 1994. Now he is an Associate Professor at the Department of Computer Engineering, Chulalongkorn University. His research interests include fault tolerant computing, hardware testing, information security and hiding, and digital watermarking.