Invariant Image Watermarking Using Accurate Zernike Moments

Ismail A. Ismail, Mohamed A. Shouman, Khalid M. Hosny and Hayam M. Abdel Salam
1Department of Computer Science, Faculty of Computers and Informatics, Misr International University, Cairo, Egypt
2Department of Decision Support, 3Department of Information Technology, Faculty of Computers and Informatics, Zagazig University, Zagazig, Egypt

Abstract: problem statement: Digital image watermarking is the most popular method for image authentication, copyright protection and content description. Zernike moments are the most widely used moments in image processing and pattern recognition. The magnitudes of Zernike moments are rotation invariant so they can be used just as a watermark signal or be further modified to carry embedded data. The computed Zernike moments in Cartesian coordinate are not accurate due to geometrical and numerical error. Approach: In this study, we employed a robust image-watermarking algorithm using accurate Zernike moments. These moments are computed in polar coordinate, where both approximation and geometric errors are removed. Accurate Zernike moments are used in image watermarking and proved to be robust against different kind of geometric attacks. The performance of the proposed algorithm is evaluated using standard images. Results: Experimental results show that, accurate Zernike moments achieve higher degree of robustness than those approximated ones against rotation, scaling, flipping, shearing and affine transformation. Conclusion: By computing accurate Zernike moments, the embedded bits watermark can be extracted at low error rate.

Key words: Zernike moments; polar coordinates; invariant watermarking; geometric attacks

INTRODUCTION

Digital image watermarking is a popular method for image authentication, copyright protection and content description (Hartung and Kutter, 1999). Digital image watermarking is an effective solution to the copyright infringement problem where the embedded watermark is used as a proof of ownership (Craver et al., 1998; Lin, 2001). Watermark is a signal embedded into the host image to be later detected or extracted. The watermarked image may be prone to various types of attacks. These attacks attempt to either destroy the embedded watermark or even completely remove it from the image. Therefore, robustness against different kinds of geometric attacks is an essential requirement of image watermarking techniques. Rotation, scaling, shearing, flipping and affine transformation are examples of these geometric attacks. Many watermarking algorithms are proposed to achieve robustness against different kinds of geometric attacks (Kim et al., 2003; Liu and Zhao, 2004; Li and Guo, 2008).

Invariant moments of images have been extensively used for invariant feature extraction. Hu (1962) derived seven moment invariants that are RST (Rotation-Scaling-Translation) invariant from regular moments. Alghoniemy and Tewfik (2000) used Hu's invariants as a watermark. Li et al. (2003) proposed a watermarking method in which the rotation angle and scaling factor are estimated after the watermarked image has been scaled or/and rotated by using geometric moments of original image. Alghoniemy and Tewfik (2004) embed the watermark by modifying the moment values of the image in a way such that a predefined function of the moment invariants lies within a predetermined value.

Orthogonal moments were first introduced by Teague (1980). Zernike moments are superior to the others in terms of their insensitivity to image noise, information content and ability to provide faithful image representation (Teh and Chin, 1988). Image Normalization can achieve scaling and translation invariance. Image normalization techniques have been used for invariant pattern recognition (Leu, 1989).

Corresponding Author: Hayam M. Abdel Salam, Department of Information Technology, Faculty of Computers and Informatics, Zagazig University, Zagazig, Egypt Tel: +2 055 2372400/+2 012 6961445 Fax: +2 055 2319920
Image is normalized by translating it to its centroid and scaling it to a standard size. Many image-watermarking techniques employed image normalization along with Zernike moments to achieve RST invariance. Kim and Lee (2003) proposed a watermarking method that applies Zernike moments as the invariant watermark by modifying the normalized Zernike moments vector of the image. Xin and Liao (2004) proposed a watermarking method that applies Zernike moments as the invariant watermark by modifying the normalized Zernike moments vector of the image. Xin and Liao (2004) proposed a watermarking algorithm that quantizes the magnitude of Zernike moments using dither modulation to embed an array of bits into the image. Most proposed watermarking methods that used Zernike moments adds watermark data to the cover image in the spatial domain after the reconstruction process.

In this study, we proposed a watermarking algorithm employing fast and accurate Zernike moments. Zernike moments are computed in polar coordinates by using a new fast, low-complexity and accurate method. Numerical experiments are performed to show the robustness against different kinds of geometric attacks. Results clearly show the efficiency of the proposed method.

Zernike moments: Zernike moments were introduced by Teague (1980). These moments are computed by mapping an image onto a set of complex Zernike polynomials. The two-dimensional Zernike moments $Z_{pq}$ of order $p$ and repetition $q$ are defined as:

$$Z_{pq} = \frac{p+1}{\pi} \int_0^{2\pi} \left[ \int_0^1 \psi_{pq}(r, \theta) f(r, \theta) r dr \right] d\theta$$  \hspace{1cm} (1)

where, $p = 0,1,2,\ldots,\infty$ and $q$ is a positive or negative integer determined according to the conditions $p-|q| = \text{even, } |q| \leq p$. The asterisk * refers to the complex conjugate and $\psi_{pq}(r, \theta)$ is the Zernike polynomial defined as:

$$\psi_{pq}(r, \theta) = R_{pq}(r) e^{-jq\theta}, \hspace{1cm} j = \sqrt{-1}$$  \hspace{1cm} (2)

where, $R_{pq}(r)$ is real-valued radial polynomial:

$$R_{pq} = \sum_{k=q}^{p} B_{pqk} r^k$$  \hspace{1cm} (3)

The coefficients $B_{pqk}$ are computed using the recurrence relations (Hosny, 2008).

Computation of Zernike moments requires a square-to-circle transformation. The square image plane is mapped over the unit circle where the center of the image is assumed to be the origin of the coordinates as (Chong et al., 2003). Therefore, computation of Zernike moments $Z_{pq}$ for a digital image of size $N \times N$ was done by replacing the integrals in Eq. 1 by summations as follows:

$$Z_{pq} = \frac{p+1}{\lambda_{(p,N)}} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} R_{pq}(t_i) e^{-jq\theta} f(i,j)$$  \hspace{1cm} (4)

where:

$$\lambda_{(p,N)} = \text{The total number of pixels that achieve the condition } \left| f(i,j) \right| \leq 1$$

Liao and Pawlak (1998) showed that, this approximation produced two types of errors; numerical error and geometrical error. The numerical error is caused by approximating the integrals in Eq. 1. These integrals are approximated through replacing them by summations. These summations are not fully accurate unless the numbers of the samples tend to infinity. The geometrical error is due to the different nature of Zernike polynomials and the input image. The numerical error is inversely proportional to the number of sampling points. On the other side, it is directly proportional to the order of moments. Therefore, numerical instabilities are affected when the moment order reaches a certain value.

MATERIALS AND METHODS

Accurate computation of Zernike moments in polar coordinate: Xin et al. (2007) proposed a novel method for computing Zernike moments in polar coordinates. Their method divided the circular unit disk into a set of non-overlapped circular sectors. Each of these sectors is represented by a point in its center and then; mapped the input image to be defined in a circular unit disk by using interpolation methods. This method is modified by Hosny et al. (2009). The computation steps of the modified method are:

- The unit disk of area $\pi$ is divided to $M$ non-overlapping circular rings. All circular rings are divided into circular sectors, such that all of these sectors must have the same area. The value of $M$ is dependent on the constraint $N/2 \leq M \leq N$ (Xin et al., 2007), where $N \times N$ is the size of the digital image.
- The radius of the $i$-th circular ring is $(i+1)/M$; where $i = 0,1,2,\ldots,M-1$ and $i = 0$ refers to the innermost circular ring.
- The area of the $i$-th circular ring is $A_i = \pi((2i+1)/M^2)$.
• Assume \( S \) is the number of circular sectors in the innermost circular ring, then, the total number of circular sectors is \( 2SM^2 \), where the area of each circular sector is \( \pi SM^2 \).

• The number of circular sectors in the \( i \)-th circular ring is \( \left( \frac{2i+1}{M} \right) \).

• Each circular sector is represented with only one point in its center. All sectors in the same circular ring have the same radial distance. The radial distance of the \( i \)-th circular ring is \( \left( \frac{2i+1}{M} \right) \).

• The upper and lower limits of the radial integral are:

\[
U_{i+1} = R_i + \Delta R_i / 2, \quad U_i = R_i - \Delta R_i / 2
\]

where, \( \Delta R_i = 1 / M \).

• The distribution of angles is dependent on the circular ring, where the value of increment is different for the different circular rings. The values of the angle \( \theta \) can be calculated using the following algorithm:

\[
\text{For } i = 0 \text{ to } M-1
\]

\[
K_i = \frac{2i+1}{M}
\]

\[
\text{For } j = 0 \text{ to } K_i - 1
\]

\[
\theta_{i,j} = (j + 0.5) \left( \frac{2\pi}{K_i} \right)
\]

endFor

endFor

• The upper and lower limits of the angle integral are:

\[
V_{i+1,j} = \theta_{i,j} + \Delta \theta_{i,j} / 2, \quad V_{i,j} = \theta_{i,j} - \Delta \theta_{i,j} / 2
\]

where, \( \Delta \theta_{i,j} = 2\pi / K_i \).

Equation 1 can be rewritten as:

\[
Z_{pq} = \frac{D + 1}{\pi} \sum_{i} \sum_{j} \hat{f}(r, \theta_{i,j})H_{pq}(r, \theta_{i,j})
\]

Where:

\[
H_{pq}(r, \theta_{i,j}) = I_{pq}(r_i)I_q(\theta_{i,j})
\]

\[
I_{pq}(r_i) = \int_{U_i}^{U_{i+1}} \frac{R_{pq}(r)}{U_i} \, rdr \quad I_q(\theta) = \int_{V_{i,j}}^{V_{i,j+1}} e^{-j\psi \theta} \, d\theta
\]

\[
\hat{f}(r, \theta_{i,j}) \quad \text{is the interpolated image (Xin et al., 2007).}
\]

Substituting Eq. 3 into 7 yields:

\[
I_{pq}(r_i) = \int_{U_i}^{U_{i+1}} \frac{R_{pq}(r)}{U_i} \, rdr = \int_{V_{i,j}}^{V_{i,j+1}} e^{-j\psi \theta} \, d\theta
\]

Applying the basic rules of definite integration, Eq. 8 could be written as follows:

\[
I_{pq}(r) = \sum_{k=1}^{M} B_{pq} \left( U_{i+1} - U_i \right)
\]

The angle based integral \( I_q(\theta_{i,j}) \) is rewritten as:

\[
I_q(\theta_{i,j}) = \begin{cases} 
\int_{0}^{\theta} \left( e^{-j\psi_{i,j} - e^{-j\psi_{i,j}}} \right), & q \neq 0 \\
V_{i,j+1} - V_{i,j}, & q = 0
\end{cases}
\]

Invariance property of Zernike moments: Rotational invariance of Zernike moments is very attractive property. Due to this property, Zernike moments are widely used in different image processing, pattern recognition and computer vision applications. If an image \( f(x, y) \) is rotated by angle \( \alpha \), \( Z_{pq} \) of the original image is related to and \( Z_{pq}^\alpha \) of the rotated image by:

\[
Z_{pq}^\alpha = Z_{pq} e^{-j\alpha}
\]

Then, the magnitudes of both sides lead to the rotation invariant property where \( |Z_{pq}^\alpha| = |Z_{pq}| \) (Hosny, 2008).

Image watermarking: In this study, we implement our modified method (Hosny et al., 2009) for accurate Zernike moments in polar coordinate instead of approximated Zernike moments. The ultimate goal is to embed real bits a watermark into the original image by quantizing the magnitudes of moments using dither modulation. At the decoder, the embedded watermark is extracted using the same quantizer. The goal is to generate a robust watermark that survives against geometric attacks like rotation, scaling, flipping, shearing and affine transformation. Implementing this algorithm prove that, the high accuracy of computed \( Z \) moments will save the Zernike moments save the embedded watermark even if the image subjected to geometrical attacks. Through the next subsections watermark embedding and extraction are discussed in details.

Watermark embedding: Three main steps are essential for embedding a sequence of bits into an image. These steps are moment selection, modification
of the selected moments and finally formation of the watermarked image.

**Selection of Zernike moments:** Selection process of Zernike moments is critical process, where the selected moments must be the most accurate moments to be suitable for data hiding. As discussed in (Xin et al., 2004), two major factors are considered in selection of moments for data hiding. Firstly, the moments with order higher than a certain value \( N_{\text{max}} \) cannot be computed accurately. Secondly, the moments with repetition \( q = 4i \) with integer \( i \) cannot be computed accurately. Therefore, these moments are not suitable for data hiding.

Assume the set \( S \) contains the rest of the moments that are eligible to be selected for carrying the watermark as \( S = \{ \forall (p,q), q \leq N_{\text{max}}, q \geq 0, q \neq 4i \} \). The vector of the pseudo-randomly selected moments is defined as \( \mathbf{A}(Z_{p,q}^{1}, ...., Z_{p,q}^{L}) \), where \( Z_{p,q} \) is an element in \( S \).

**Modification of Zernike moments:** The magnitudes of Zernike moments are modified to carry a generated randomly bit sequence, \( b = (b_{1}, ...., b_{L}) \), \( L < |S| \). Each element from \( b \) is embedding into each element of vector \( \mathbf{A} \) by using dither modulation. The modified vector of Zernike moments \( \tilde{\mathbf{A}} = (\tilde{Z}_{p,q}^{1}, ...., \tilde{Z}_{p,q}^{L}) \) where \( \tilde{Z}_{p,q}^{i} \) is the modified version of \( Z_{p,q}^{i} \) computed using the following formula:

\[
\tilde{Z}_{p,q}^{i} = \left[ \frac{\tilde{Z}_{p,q}^{i} - d(b_{i})}{\Delta} \right] \Delta + d(b_{i}), i = 1,2,......L
\]

where, \( \Delta \) is the step size of quantization, the dither vector \( (d_{0}(0), d_{0}(1), ...., d_{0}(0)) \) is generated randomly within the interval \([0,1]\), the Vector \( (d_{1}(1), d_{1}(1), ...., d_{1}(1)) \) is obtained form \( d(0) \) as follows:

\[
d(1) = \frac{\Delta}{2} + d(0)
\]

where, \( d(0) \in [0,1] \). The modified Zernike moments are computed using their modified magnitudes by:

\[
\tilde{Z}_{p,q}^{i} = \frac{\tilde{Z}_{p,q}^{i}}{Z_{p,q}^{i}}, i = 1, ...., L
\]

**Formation of the watermarked image:** The watermarked image is obtained by replacing the image part formed by the unchanged moments with the other part formed by the modified moments. The image part contributed by unchanged moments is:

\[
f_{\text{img}}(x, y) = f(x, y) - f_{s}(x, y)
\]

where, \( f_{s}(x, y) \) is the image part contributed by the selected moments before they were modified which can be computed by:

\[
f_{s}(x, y) = \sum_{i=1}^{L} Z_{p,q}^{i} V_{p,q}(x, y) + Z_{p,q} V_{p,q}(x, y)
\]

The modified image part contributed by the modified selected moments is obtained using:

\[
f_{s}(x, y) = \sum_{i=1}^{L} \tilde{Z}_{p,q}^{i} V_{p,q}(x, y) + \tilde{Z}_{p,q} V_{p,q}(x, y)
\]

The watermarked image \( \tilde{f}(x, y) \) is formed as:

\[
\tilde{f}(x, y) = f_{\text{img}}(x, y) + f_{s}(x, y)
\]

**Watermark extraction:** The process of watermark extraction takes the watermarked image as an input and outputs the embedded watermark bits. The watermarked image may be attacked by various kinds of attacks. Image normalization to standard size is an essential step before watermark extraction, where the goal is to estimate the extracted bits at low error rate.

In this study, the image is rescaled to a size 256×256 and then; selected Zernike moments of the test image are computed. The moment vector \( Z'(p,q) = (Z_{p,q}^{1}, ...., Z_{p,q}^{L}) \) is formed according to the previously discussed conditions. Using the same quantizer in (13) each moment magnitude \( |Z_{p,q}^{i}| \) are quantized with the two dithers \( d(0) \) and \( d(1) \) respectively:

\[
|A_{p,q}^{j}| = \left[ \frac{A_{p,q}^{j} - d_{j}(i)}{\Delta} \right] \Delta + d_{j}(i), j = 0,1
\]

The extracted bits \( b_{j} \) are estimated by comparing the distances between \( |Z_{p,q}^{i}| \) and its two quantized versions:

\[
b_{j} = \arg_{j=0,1} \min \left| |Z_{p,q}^{i}| - |Q_{j}| \right|^2
\]

The value of the estimated bit \( b_{j} \) is \( j \) that gives the minimum distance of its quantizer with \( |Z_{p,q}^{i}| \).
RESULTS AND DISCUSSION

Numerical experiments are conducted by using grayscale images of size 256×256 where various types of geometric attacks are examined. The watermarked image is transformed before the process of watermark extraction and Bit Error Rate (BER) is computed. A comparison of watermarking by using accurate Zernike moments and approximated Zernike moments is performed. The grayscale image of ‘House’ with size 256×256 is watermarked by a 128 bit sequence using accurate Zernike moments in the first experiment. Figure 1a shows the original image, Fig. 1b shows the watermarked image while Fig. 1c shows the absolute difference between them multiplied by 25 for better display. The difference in the Fig. 1c represents the spatial contribution of the embedded watermark.

Robustness to rotation: The watermarked image is rotated with angles form 0-45° with interval 2.5° and Δ = 2. BER is computed for the extracted bit sequence.

Two experiments are conducted, in the first one; a 160 bit long random sequence is used as the embedding information. In the second experiment, a 300 bit long random sequence is used. In the two cases, the watermarking algorithm is implemented by using both accurate and approximated Zernike moments.

Fig. 1: Example of watermarking embedding (a) the original image (b) the watermarked image (c) the absolute difference between a and b

Figure 2a show the watermarked image rotated by 15°, Fig. 2b shows the Bit Error Rate (BER) of the 160 bit embedded watermark extraction under rotation attack, while Fig. 2c shows the Bit Error Rate (BER) of the 300 bit watermark extraction under rotation attack. The results of the two experiments show that, accurate Zernike moments generates extremely low error rates than those generated by using approximated ones especially for rotations that exceed 5°.

Fig. 2: Robustness to rotation attack (a) watermarked image with 160 bits rotated by 15° (b) BER of rotation angles with 160 bits watermark (c) BER of rotation angles with 300 bits watermark
Robustness to flipping: The watermarked image is flipped horizontally and vertically. In Fig. 4a, the watermarked image is flipped horizontally and vertically in Fig. 4b. Table 1 shows the bit error rate for 128 bits sequence and Table 1 shows the bit error rate for 256 bits sequence.

Robustness to JPEG compression: JPEG compression is one of the most used operations for digital images. The watermark robustness is examined against lossy JPEG compression. The watermarked image is compressed with quality factors from 20-100 with interval of size 5. Figure 5a shows the watermarked image compressed with quality factor 20, Fig. 5b shows the bit error of the extracted 160 bits sequence while Fig. 5c show the bit error rate of the extracted 300 bits sequence.

Table 1: Bit Error Rate (BER) of flipping

<table>
<thead>
<tr>
<th></th>
<th>Vertical flipping</th>
<th>Horizontal flipping</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>BER (accurate ZM)</td>
<td>BER (approximated ZM)</td>
</tr>
<tr>
<td>128 bits</td>
<td>0.01560</td>
<td>0.1891</td>
</tr>
<tr>
<td>256 bits</td>
<td>0.01562</td>
<td>0.1266</td>
</tr>
</tbody>
</table>

Fig. 3: Robustness to scaling attack (a) BER of scaling factor with 128 bits watermark (b) BER of scaling factor with 256 bits watermark

Fig. 4: (a) the watermarked image flipped horizontally; (b) the watermarked image flipped vertically

Table 2: The bit error rates of the extracted bits after some affine transformation

<table>
<thead>
<tr>
<th>Geometric attack</th>
<th>BER (accurate ZM)</th>
<th>BER (approximated ZM)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>128 bits</td>
<td>256 bits</td>
</tr>
<tr>
<td>Scaling (0.6), rotation (10°)</td>
<td>0.1250</td>
<td>0.1289</td>
</tr>
<tr>
<td>Scaling (1.5), rotation (30°), horizontal flipping</td>
<td>0.0078</td>
<td>0.0430</td>
</tr>
<tr>
<td>Scaling (0.5), rotation (25°), compression (Q = 35)</td>
<td>0.2031</td>
<td>0.2148</td>
</tr>
<tr>
<td>Scaling (1.2), rotation (15°), flipping, compression (Q = 20)</td>
<td>0.1172</td>
<td>0.2031</td>
</tr>
</tbody>
</table>
Fig. 5: Robustness to JPEG compression (a) BER of compression quality factor with 160 bits watermark (b) BER of compression quality factor with 300 bits watermark

Affine transformation: The affine transformation of an image is performed by doing consecutive transformations to the image, in other words, the image is transformed by being multiplied by the transformation matrix. Experiments are conducted on the watermarked image by attacking it with some affine transformations as follows:

- The watermarked image is rotated by rotation degree 10° and then scaled by scaling factor 0.6
- The watermarked image is scaled by scaling factor 1.5, rotated by rotation degree 30° and then flipped horizontally
- The watermarked image is scaled by scaling factor 0.5, rotated by rotation degree 40° and then compressed by compression factor 30
- The watermarked image is scaled by scaling factor 1.2, rotated by rotation degree 20°, flipped vertically and then compressed by compression factor 20

Fig. 6: The watermarked image transformed by (a) rotation degree 10° and scaling factor 0.6; (b) scaling factor 1.5, rotation degree 30°, and flipped horizontally; (c) scaling factor 0.5, rotation degree 40°, and compression factor 30; (d) Scaling factor 1.2, rotation degree 40°, flipped vertically, and compression factor 20

Figure 6 shows the transformed watermarked image. Table 2 lists the bit error rate of the extracted bits from the transformed image for 128 and 256 bits sequence.

CONCLUSION

This study presents a new watermarking algorithm that embeds real bits into the original image. Fast, low-complexity accurate method is applied to compute Zernike moments in polar coordinate. Watermarked gray-scale images are subjected to various kinds of geometric attacks. The results of the conducted experiments clearly show that, employing accurate Zernike moments keep the embedded watermark almost intact when it is subjected to various types of attacks where the embedded watermark bits are extracted with lower bit error rates than the rates generated using approximated ones. According to its low-complexity requirements, the proposed algorithm is suitable for large images.

REFERENCES


