ROTATION AND CROPPING RESILIENT DATA HIDING WITH ZERNIKE MOMENTS

Palak Amin, K. P. Subbalakshmi *

Department of Electrical and Computer Engineering
Stevens Institute of Technology
Hoboken, New Jersey 07030
Email: {pamin,ksubbala}@stevens.edu

ABSTRACT

Most digital data hiding schemes are sensitive to simple geometric attacks namely rotation, cropping, and scaling. Of these, rotational attacks possess the capability to not only change each pixel value but also dislocate the image pixels in a circular fashion, thus creating a synchronization issue for any linear data hiding algorithm. So far, Fourier Mellin transform (FMT) based algorithms have been considered a standard for rotation invariant data hiding. This method causes some difficulties in implementation due to unstable log-polar mapping, iterative inversion of the interpolation and aliasing effects on the FMT magnitude and phase spectra. In this paper, we propose a data hiding algorithm that is based on the Zernike moment transform (ZMT), accompanied with an odd-even quantizer based embedding scheme to defeat the effects of rotation and cropping attacks. We note that this algorithm is robust to a combination of rotation and other popular attacks. The proposed algorithm has good embedding capacity and very low induced distortion. Experimental results over a range of rotational attacks (from 0^o to 360^o) show a recovery rate (of the embedded bits) of 97% or greater.

1. INTRODUCTION

With the growth of new digital media applications, security issues such as copyright protection, copy control and illegal distribution have assumed importance. Data hiding schemes have been proposed in recent years as a viable method to address some of these security concerns. Some examples of attacks on these schemes include re-quantization, dithering, rotation, scaling, cropping etc [2]. Among these, geometric attacks can be considered the strongest. Several algorithms have been published that address the severity of geometric attacks [3,4,5,6,7]. Examples of work on geometric attack resilience can be found in [8,9,10,11,12,13,14,15]. Pereira et al. [8] and Csurka et al. [9] have proposed to embed a template based watermark in their algorithm. Upon extraction, comparison of the extracted template with the original, gives information on the type and amount of geometric distortion that the embedded media was subjected to. This addition to the watermark can result in lower payload of the embedded data. Kutter et al. [10] have proposed to use the watermark itself as the template. In this case the choice of watermark media is limited to the template. O'Ruanaidh et al. [11] and Lin et al. [12] have proposed a version each of FMT based watermarks. These algorithms demonstrate some implementation issues due to unstable log-polar mapping. Furthermore, these are watermark detecting algorithms as compared to our proposed retrieving algorithm. Kutter et al. [13] and Guoxiang et al. [14], have described a second generation watermarking algorithm that is collectively based on FMT and image feature vectors. They conclude that their algorithms are unable to achieve rotation invariance for all angles of rotation. This is mainly due to the effects of aliasing on FMT magnitude spectrum. Kim et al. [15] propose an enhanced version of the second generation watermarking system that is based on FMT phase spectrum and higher order spectra of the radon transform. The authors report that their algorithm works only for very small angles of rotation due the complexity of interpolating values in the FMT phase spectrum.

In this paper, we propose an algorithm based on the Zernike Moment Transform (ZMT) and an odd-even quantizer (OEQ) that demonstrates excellent robustness against rotation and cropping attacks. To test this algorithm the stego-images were rotated by several angles in the range of 0^o to 360^o and it was found that the recovery rate was always greater than 97%. For simplicity we use 64x64 pixel binary images in our experiments; although our algorithm is equally applicable to grayscale images.

2. THE ZERNIKE MOMENT TRANSFORM

Hu [16] introduced the concept of moment invariants and the use of moments in digital imaging and the use of Zernike moments in digital imaging was pioneered by Teague [17].

*This work was funded partly by the National Science Foundation and the Air Force Research Laboratory, Rome, NY.

Zernike moments consist of a set of complex polynomials that form a complete orthogonal set over the interior of the unit circle, $x^2 + y^2 = 1$. If the set of these polynomials is denoted by $V_{nm}(x, y)$, then the form of this polynomials is as follows

$$V_{nm}(x, y) = V_{nm}(\rho, \theta) = R_{nm}(\rho)\mathrm{e}^{(\mathrm{j}m\theta)}$$

where $n \in \mathcal{N}$(the set of all positive integers including zero) is the order of the ZMT, $m \in \mathcal{Z}$(the set of all integers) is the rotation degree; as long as $n - |m|$ is even and $|m| \leq n$, ρ is the length of the vector from the origin to a the pixel (x, y), θ is the angle between the X-axis and the vector ρ in the counterclockwise direction, and $R_{nm}(\rho)$ is a radial polynomial defined as follows

$$R_{nm}(\rho) = \sum_{s=0}^{n-|m|/2} (-1)^s \left(\frac{(n-s)!}{s!(\frac{n+|m|}{2} - s)!(\frac{n-|m|}{2} - s)!}\right)\rho^{n-2s}$$

These polynomials are orthogonal and hence satisfy

$$\int\int_{(x^2+y^2)\leq 1} [V_{nm(x,y)}]^* \, V_{pq}(x, y) \, dx \, dy = \frac{\Pi}{n+1}\delta_{np} \, \delta_{mq} \quad (1)$$

with $\delta_{ab} = 1$ if $a = b$ and 0 otherwise. Zernike moments are projections of the image function onto these orthogonal basis functions. Hence, the Zernike moment of order n, with repetition m for a continuous image function $f(x, y)$ is given by

$$A_{nm} = \frac{n+1}{\Pi} \int\int_{(x^2+y^2)\leq 1} f(x, y) \, V^*_{nm}(\rho) \, \theta \, dx \, dy \quad (2)$$

where $n \in \mathcal{N}$ and $m \in \mathcal{Z}$. Equivalently, for a digital image,

$$A_{nm} = \frac{n+1}{\Pi} \sum_x \sum_y f(x, y) \, V^*_{nm} \, (\rho) \, \theta \, \forall \, (x^2 + y^2) \leq 1$$

To compute the Zernike moments of an image, the center of the image is taken as the origin and the pixel coordinates are mapped to the range of a unit circle following a square to circular transform [21].

3. ROTATION INVARIANCE

Teague [17] discussed the derivation of Zernike moments from the geometric moments of an image based upon the rotational properties of geometric moments. Let f^α denote the image f that has been rotated by α degrees, then the relationship between the original and the rotated versions of the image in the same polar coordinates is

$$f^\alpha(\rho, \theta) = f(\rho, \theta - \alpha)$$

The Zernike moments of the image can be expressed in polar co-ordinates by replacing x and y with $\rho\cos\theta$ and $\rho\sin\theta$ respectively in Eqn 2. Using Eqns 1 and 2 the Zernike moments, A_{nm} of the image and those of its rotated version, A^α_{nm} can be written as

$$\begin{aligned}
A_{nm} &= \frac{n+1}{\Pi}\int_0^{2\Pi}\int_0^1 f(\rho,\theta)\, R_{nm}(\rho)\, \mathrm{e}^{(-\mathrm{j}m\theta)}\, \rho\, \mathrm{d}\rho\, \mathrm{d}\theta \\
A^\alpha_{nm} &= \frac{n+1}{\Pi}\int_0^{2\Pi}\int_0^1 f(\rho,\theta-\alpha)\, R_{nm}(\rho)\, \mathrm{e}^{(-\mathrm{j}m\theta)}\, \rho\, \mathrm{d}\rho\, \mathrm{d}\theta \\
&= \frac{n+1}{\Pi}\int_0^{2\Pi}\int_0^1 f(\rho,\theta_1)\, R_{nm}(\rho)\, \mathrm{e}^{(-\mathrm{j}m(\theta_1+\alpha))}\, \rho\, \mathrm{d}\rho\, \mathrm{d}\theta_1 \\
A^\alpha_{nm} &= A_{nm}\, \mathrm{e}^{(-\mathrm{j}m\alpha)}
\end{aligned}$$

So, we see that rotation of an image in spatial domain merely causes its Zernike moments to acquire a phase shift and hence the magnitudes of the Zernike moments i.e. $|A_{nm}|$ are identical for several rotations of the same image. Experimentally, this property of Zernike moments is demonstrated below. In Fig 1, we see the original image along with several rotations of itself; while, Table 1 shows some of the Zernike moment values for these rotations of the test image along with the mean (μ) and the standard deviation (σ) of these moments. We use this rotation invariance property in our proposed algorithm, by embedding the data in the magnitude of the Zernike moments of the image.

Figure 1: Image of the numeral 5 with rotated versions of itself.

Table 1: Magnitude of the Zernike Moments for the Examples Shown in Fig 1

	A_{20}	A_{22}	A_{31}	A_{33}
0^o	439.61	41.72	57.92	172.58
30^o	436.73	40.28	63.84	171.95
60^o	440.60	40.01	66.29	169.43
150^o	438.53	41.54	65.48	170.87
180^o	439.07	46.85	62.33	168.44
300^o	438.44	39.11	65.75	170.87
μ	438.80	41.63	63.68	170.69
σ	1.31	2.75	3.11	1.58
$\sigma/\mu\%$	0.32	6.53	4.91	0.95

4. PROPOSED EMBEDDING SCHEME

In this section we propose to use a quantizer based embedding scheme in the Zernike moment domain. We use the odd-even quantizer [23,24,25] concept in the embedding process. For any digital image, the Zernike moment values for any order and rotation can assume a real value i.e. $A_{nm} \in \mathcal{R}$. The set of these moment values over a finite real range are divided into S quantization intervals each of length Δ such that, $(\max_{n,m}(A_{nm}) - \min_{n,m}(A_{nm})) = S\Delta$. Let each of these quantization intervals be denoted by Q_t where $t \in \{0, \cdots, S\}$, and their corresponding representation value (in the source coding sense [26]) be denoted by r_t. For data hiding purposes, these intervals are also associated with a bit '0' or a bit '1' as per the following relationship.

$$Q_t \leftarrow \begin{cases} 1, & t\Delta \leq A_{nm} < (t+1)\,\Delta \quad \forall\,(t \bmod 2) = 1 \\ 0, & \text{otherwise} \end{cases}$$

Now, given the hidden message W, there are two possibilities,

1. The i^{th} bit of the hidden message, W_i is a '0' and the i^{th} moment value, A_i, from the Zernike moment vector, $\vec{A} = A_i \; i \in \{1, \cdots, nm\}$, is mapped to a '0'. In this case, we change A_i to the representation value of that bin denoted by r_t.

2. Otherwise we change A_i to the representation value of the closest quantization interval (either on its left or right) which corresponds to a binary '1'. That is,

$$A_i = \begin{cases} r_{t-1}, & (|A_i - r_{t-1}|) \leq (|A_i - r_{t+1}|) \\ r_{t+1}, & (|A_i - r_{t-1}|) > (|A_i - r_{t+1}|) \end{cases}$$

Hence, all the bits of the hidden message are inserted by quantizing each value of A_{nm}. Upon, inverse transforming this modified moment array to reconstruct the original image, the visual degradation is not perceivable by the human visual system (HVS), due to rather small modifications to the moments of the host image. This fact is substantiated by the images in Fig 2 below, which shows the original image (64x64 pixels), the hidden message (23x20 pixels) and the resulting image after embedding (64x64 pixels).

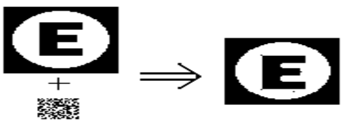

Figure 2: The original image and the hidden message on the left and the stego-image on the right

5. EXPERIMENTAL RESULTS

In our experiments, we compute the Zernike moments of order $n = 36$ and $m = 0 \; to \; 30$, since $n = 36$ has been shown to be optimal for reconstruction in image processing applications [21]. Note that the number of Zernike moments calculated does not depend on the complexity of the image. Thus a forward ZMT for the test images resulted in a (462x1) invertible ZMT matrix. Since it is possible to embed one bit per moment, it is possible to embed 462 bits in this set-up. So our hidden signals were randomly generated images of size (23x20) i.e. 460 bits. The retrieval rates were calculated by dividing the number of correctly recovered bits by the length of the embedded signal (460 bits). Fig-3 below shows the retrieval rates for an image that was rotated in increments of 30^o clockwise in the range of 0^o to 360^o. As seen in Fig-3 above, in all cases of rotation attacks our retrieval rate is at least 97%. Also we note that we have a mirror effect about the vertical axis at the 180^0 point. Table-2 compares our algorithm's retrieval rates with that of several popular rotation invariant algorithms. The results indicate that, the proposed algorithm outperforms the other algorithms and while most of the other algorithms provide acceptable results for only small angles of rotation ($0^o \, to \, 45^o$), the proposed algorithm provides higher retrieval rates for any angle of rotation. The comparison algorithms do not provide any results of extraction for rotation angles beyond 45^o. The algorithm was also tested for a combination of rotation, cropping and other popular attacks such as, JPEG compression, sharpening, despeckling, blurring, median filtering, and random noise addition. Table-3 below reports the extraction results for the attacks listed above followed by 90^o rotation. As seen, except in cases of noise addition, the algorithm works exceptionally well for combination attacks. In all other cases of combination attacks, the retrieval rate is greater than 90% and even in case of noise addition

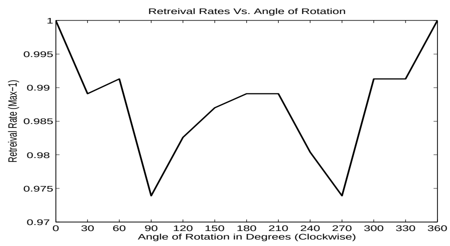

Figure 3: Retrieval rates of the hidden message from rotated versions of the image. Note that the changes in retrieval rates are less than 3%.

Table 2: Performance Comparison with Several Published Algorithms

Rot. Angle	Prop. Algo.	Lin et al.[12]	Kim et al.[15]	Digi-marc[27]	Sure-sign[28]
4^o	100%	97.2%	95%	94%	50%
12^o	99%	94.9%	95%	94%	50%
45^o	99.2%	93.6%	95%	94%	50%

Table 3: Extraction Results After Combination Of Attacks Prior To 90^o Rotation

Test	Retrieval Rate
JPEG (Q 90-20)	96.4% - 94.1%
Sharpening	91%
Despeckle	93.2%
Smart Blur (Rad. 5)	91.4%
Median Filtering	95%
Uniform Noise (10%-15%)	85.6%-82%
Gaussian Noise (10%-15%)	83.3%-76.1%

prior to rotation, at least 75% of the embedded signal is decoded correctly.

6. CONCLUSION

We proposed an algorithm that is resilient to rotation and cropping attacks with retrieval rates exceeding 97% for all angles of rotation. When the rotation angle is between 0^o and 45^o, the proposed algorithm retrieves 99% of the embedded bits correctly. Experiments show that the proposed algorithm is robust not only to rotation and cropping attacks, but also works well in the presence of a combination of rotation, cropping and several other popular attacks. In all cases of combination attacks except for noise addition, at least 90% of the embedded signal is correctly retrieved. For the case of additive random noise attack followed by rotation attack, at least 75% of the embedded signal is decoded correctly.

7. ACKNOWLEDGMENTS AND DISCLAIMER

This work was jointly funded by National Science Foundation (NSF) award number NSF-DAS 0242417 and Air Force Research Laboratory (AFRL). This material is based on research sponsored by Air Force Research Laboratory (AFRL) under agreement number F30602-03-2-0044. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of Air Force Research Laboratory or the U.S. Government.

8. REFERENCES

[1] F. Hartung and M. Kutter, "Multimedia watermarking techniques," in Proc. IEEE, 87(7) 1079-1107 (1999).

[2] F.A.P. Petitcolas, R.J. Anderson and M.G. Kuhn, "Attacks on Copyright Marking Systems," in Workshop on Info. Hiding, Portland, OR, 15-17 April, 1998.

[3] M. Mansour and A. Tewfik, "Techniques for Data Embedding in Images Using Wavelet Extrema", Proc. SPIE on Sec. and Watermarking of Mult. Cont., San Jose, January 2001.

[4] I. Cox, J Kilian, T Leighton and T Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", in IEEE Trans. On Image Proc., Vol 6, Number 12 1997.

[5] D. Zheng, J. Zhao, and A Saddik, "RST Invariant Watermarking Based on Log-Polar Mapping and Phase Corr.", in IEEE Trans. On Circ. and sys. for video Tech., Sept 2003.

[6] S.A.M.Gilani and A.N.Skodras, "DLT-Based Digital Image Watermarking", First IEEE Balkan Conf. on Sig. Proc., Comm., Circ. and Sys., Istanbul, Turkey, June 2-3, 2000.

[7] M. Alghoneiemy and A.H. Tewfik, "Progressive Quantized Projection Watermarking Scheme", Proc. ACM Multimedia 99, Orlando FL, Nov 2-5 1999, pp 295-298.

[8] S. Pereira and T. Pun, "Robust template matching for affine resistant watermarks," IEEE Trans. Image Proc, 9(6) 2000.

[9] G. Csurka, F. Deguillaume, J. J. K. O'Ruanaidh, and T. Pun, "A Bayesian approach to affine transformation resistant image and video watermarking," in Proc. 3 rd Int. Workshop on Information Hiding, 315-330 (1999)

[10] M. Kutter, "Watermarking resisting to translation, rotation, and scale", Proc. SPIE Mult. Sys. Appl., 3528 423-431 (1998)

[11] J. J. K. O'Ruanaidh and T. Pun, "Rotation, scale, and translation invariant spread spectrum digital image watermarking," Signal Processing, 66 303-317 (1998)

[12] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, and Y. M. Lui, "Rotation, scale, and translation resilient watermarking for images," IEEE Trans. Image Proc., 10(5) 767-782 (2001)

[13] M. Kutter, S. K. Bhattacharjee, and T. Ebrahimi, "Towards second generation watermarking schemes," in Proc. IEEE Int. Conf. Image Processing, 320-323 (1999)

[14] S. Guoxiang and W. Weiwei, "Image-feature based second generation watermarking in wavelet domain," in Lecture Notes in Computer Science, 2251 16-21 (2001)

[15] H. S. Kim, Y. Baek and H. K. Lee, "Rotation, scale and translation invariant watermark usinghigher order spectra," Optical Engineering , Vol.42, No.2, pp.340-349., February 2003.

[16] M.K. Hu, "Visual problem recognition by moment invarian", IRE Trans. Inform. Theory, vol. IT-8, pp. 179-187, Feb. 1962.

[17] M.R. Teague, "Image analysis via the general theory of moments", J. Optical Soc. Am., vol. 70, pp. 920-930, 1980.

[18] A. Khotanzad and Y.H. Hong, "Invariant image recognition by Zernike moments", IEEE Trans. Pattern Anal. Mach. Intelligence PAMI-12, 1990, pp. 489-498.

[19] S. X. Liao, Image Analysis by Moments, Ph. D. dissertation, The University of Manitoba, 1993.

[20] C.H. Teh and R.T. Chin, "On image analysis by the methods of moments", IEEE Trans. Pattern Anal. Machine Intell., vol. PAMI-10, pp. 496-512, July 1988.

[21] R. Mukundan and K. R. Ramakrishnan, "Moment Functions in Image Analysis" World Scientific Publishing, 1988.

[22] K. Y. Chang, The LANS Patrec Toolbox homepage "http://www.lans.ece.utexas.edu/ lans" 2003.

[23] A. B. Warson, G. Y. Yang, and J. Villasenor, "Visibility of wavelet quantization," IEEE Trans. Image Proc. 6(8), 1997.

[24] D. Kundur and D. Hatzinakos, "Digital watermarking for telltale tamper proofing and auth," Proc. IEEE 87, 1999.

[25] G. J. Yu, C. S. Lu and H. Y. M. Liao, "Mean-quantization-based fragile watermarking for image authentication," Optical Engineering, Vol. 40, No. 7, pp. 1396-1408, 2001.

[26] R. Veldhuis and M. Breeuwer, "An Introduction to Source Coding", Prentice Hall, New York, 1993

[27] Digimarc Inc. "http://www.digimarc.com"

[28] Suresign, Signum Tech. "http://www.signumtech.com"