A Robust Image Watermark Algorithm for AD/DA Conversion

DongHwan Shin[1], KyungJun Park, TaeYoon Lee, ChangWon Kim and JongUk Choi
Content Solution Business Division
MarkAny Inc.
Seoul, Korea
e-mail:{dhshin[1], kjpark, tylee, permedia, juchoi}@markany.com

Abstract— **This paper is proposing a new watermarking approach which is robust to the AD / DA (from Analog to Digital, or from Digital to Analog) conversion attack, and especially strong against print-scan attack. The new algorithm is designed to be robust for the RST (Rotation, Scaling and Translation) attack and AD/DA attack in order to be used in print-scan applications. The proposed algorithm makes the 12 circular digital signal templates in the frequency domain and shifts them circularly according to the watermark information to be embedded. In order to extract watermark, we use a method to calculate the correlation between the extracted patterns and reference patterns. As a result, our new watermark approach was robust against color print & scan attack on a paper, with 600 dpi color printer, with watermark detection rate of 83.5% in a normal condition room, and 81% in a normal outdoor condition while detection rate was 45% on a monitor display & scan attack case. The difference of detection rates was not large between indoor and outdoor environments.**

Keywords- Image; Watermark; RST; AD/DA; Circular shift.

I. INTRODUCTION

Image watermark algorithm has been used to protect copyrights of digital image content. This digital content can be distributed with embedding watermarks in it and the watermark information can be extracted on the receiver side to recognize the first downloader information or to know the copyright information of the digital image content [1][2][3][7][9]. In addition to this, two informative use cases, the watermark algorithm is recently used to inform subsidiary information of digital image contents.

Image watermark techniques are classified as spatial domain based methods and frequency domain based methods, according to the region of watermark embedding. In the spatial domain based method, the image watermark is embedded by using pixel information of the digital image. The advantage of this method is speed of embedding. It can be relatively fast because a watermark signal is embedded in a spatial domain directly. Because watermark extraction can happen from spatial domain directly, the extracting speed is also fast. Because of those advantages, many of image watermark techniques are using the spatial domain based method. However, this method is known for its weakness in attack cases, such as compression (encoding) attacks. In addition, this technique has a characteristic that it should know where the watermark information starts in a digital image to extract the watermark information. For example, there is a spread spectrum method, which is one of the famous methods in the spatial domain based approach, and one of its disadvantages is that sync signal should be used to know the exact starting point of the embedded watermark [4]. M. Kutter tried to solve this problem with a new method which adds an additional watermark pattern, beside a message watermark, to detect this sync signal against RST attack [5][6]. The disadvantage of this method was that the performance of recover logic against RST attack affects a lot the overall performance of the image watermark algorithm.

The other image watermark technique is when the image watermark is embedded in the frequency domain. There have been several different frequency transformation ways for this approach, such as DFT (Discrete Fourier Transform), DCT (Discrete Cosine Transform), and DWT (Discrete Wavelet Transform). In the frequency domain based method, before embedding the watermark, the pixel information of the image goes through the frequency domain transformation stages. After that, the watermark information is embedded on the image by using the frequency coefficient information which is the output of the transformation. The advantage of this method is that specific properties of various frequency transformation methods can be used. Furthermore, in lossy compression, such as JPEG or MPEG, various kinds of frequency transformation methods are basically used already to remove information redundancy for improving the efficiency of the compression. Because of this, the watermark embedding method in frequency domain has characteristics that make the robust watermarking approach a relatively easily technique against compression attacks.

In this paper, the proposed watermark method embeds the watermark signal on the frequency domain. DFT is used for the frequency transformation method. This method has a feature which stores the watermark information distributed over several pixels in the spatial domain, without making a huge distortion in specific pixels even if the watermark is embedded strongly in the frequency domain. In addition, by designing the watermark embedding pattern to be in regardless of the starting point of digital image, this approach could prove to be strong against cropping attacks. In this paper, the robustness of this method is proved by extracting the image watermark through taking pictures with digital cameras of mobile smartphones.

The rest of the paper is structured as follows. In Section 2, the circular shift watermark algorithm is explained. We

 ISBN: 978-1-61208-452-7

give details on both the watermark embedding method and also the watermark extraction method. In Section 3, several tests are conducted in order to verify the effectiveness of the proposed algorithm. We conclude the paper in Section 4.

II. CIRCULAR SHIFT WATERMARK

In this paper, to embed the watermark, the method sets the standard pattern in frequency domain plane by using template and shifts circularly the pattern according to watermark information.

Figure 1 shows the example of circular shift with angle (θ) of a specific pattern. The moving phase with angle (θ) for minimum basic unit, 1, is different according to the watermark payload amount for one specific pattern. Equation (1) shows the level value to embed x bits of information in the pattern. When the watermark information is increased by 1, the phase angle moves by Δ_θ, as shown in equation (2).

$$level = 2^x \quad (1)$$

$$\Delta_\theta = \pi / level \quad (2)$$

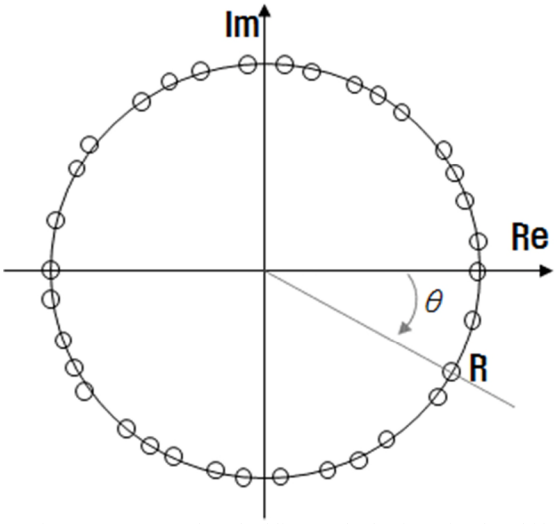


Figure 1. Watermark embedding method using Circular Shift

Figure 2 shows an example of embedded watermarks by producing multiple reference patterns.

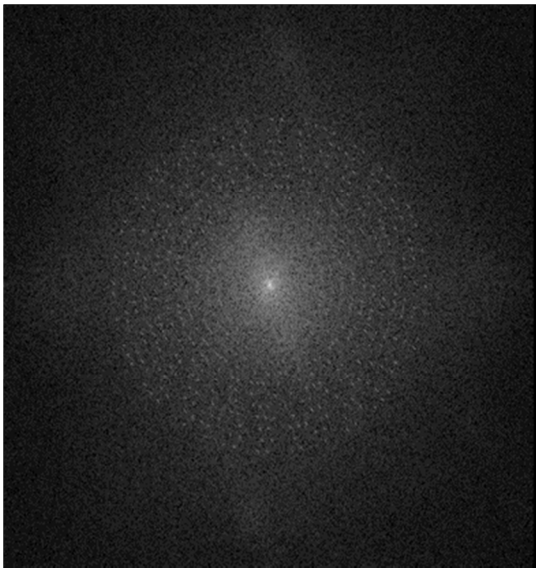


Figure 2. Example of embedding watermark in frequency plane

A. Embedding Watermark

Figure 3 shows the order of embedding the watermark.

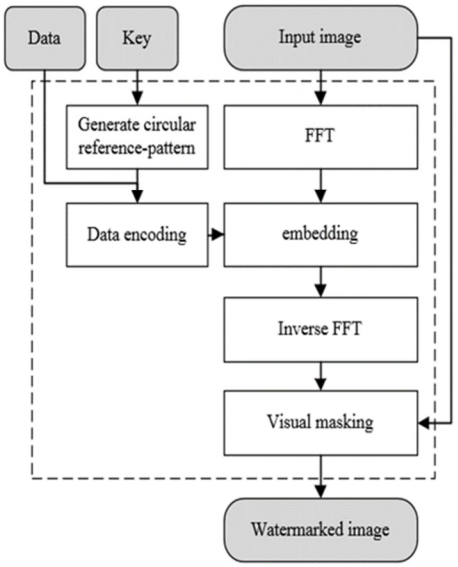


Figure 3. Order of watermark embedding

1) First, when the watermark embedding algorithm is started, a watermark message data and secret key are received as inputs, and a watermark embedding pattern data is generated based on the inputs.

2) In 1), based on the produced pattern, the watermark pattern is produced in order to be embedded in the original digital images with watermark embedding data.

3) The input digital image is transformed to frequency domain data by FFT (Fast Fourier Transform).

4) On the frequency domain of 3), the watermark pattern from 2) is embedded.

 ISBN: 978-1-61208-452-7

5) By using Inverse FFT, the image in the frequency domain is transformed into the image in the spatial domain.

6) To ensure the invisibility of embedded watermark, the strength of watermark is adjusted by using the visual masking method.

Equation (3) shows the visual masking method.

$$I' = WI \cdot maskoffset + (1 - maskoffset) \cdot I \quad (3)$$

Here,

WI : the watermark embedded digital image

maskoffset : [0.0 – 1.0], if the value is closer to 0, the image is closer to the original one.

I: Original image

I' : The final image after watermark embedding

B. Extracting Watermark

Figure 4 shows the order of extracting the watermark.

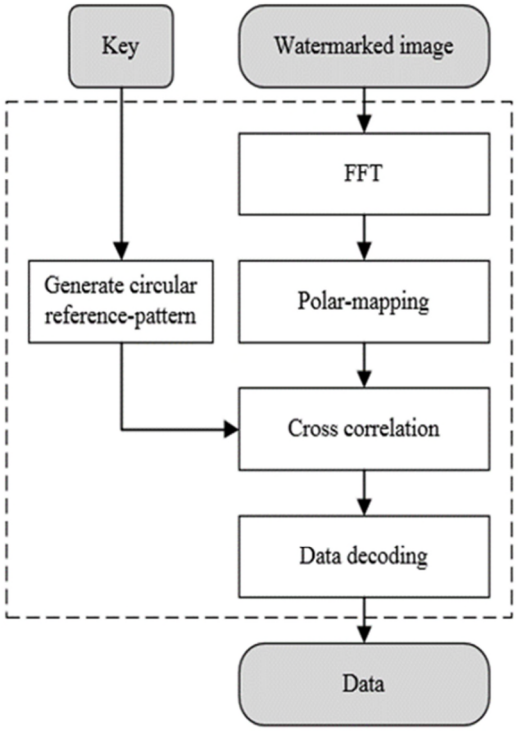


Figure 4. Order of extracting watermark

1) The watermark embedded image is transformed to frequency domain by FFT.

2) By using polar mapping, the angle component of the image is translated to horizontal axis value and the radius component of the image is transformed to vertical axis value.

3) The reference pattern is generated with the key which is used for watermark embedding.

4) The cross-correlation value is calculated between the reference pattern in 3) and the value in 2)

5) The embedded data are decoded by using the local maximum value of cross-correlation.

To extract the watermark, the correlation value between the reference pattern of each frequency and the extracted signal from each frequency band is calculated. The maximum value is selected and the phase value on the point is measured, then the watermark is extracted using the measured value. To calculate the correlation value between signals of circular form in frequency domain, a polar transformation is used to change them to a 1 dimension array of the same size.

The basic geometry of polar mapping is shown in Figure 5. Equally spaced concentric circles are drawn centered at the image center, and a number of equally spaced sectors are drawn. Pixels at the points of intersection of these circles and radial lines are plotted on a rectangular grid, and the resulting image is a polar view. In a log polar mapping, the radii of the concentric circles vary on a logarithmic scale [10][11].

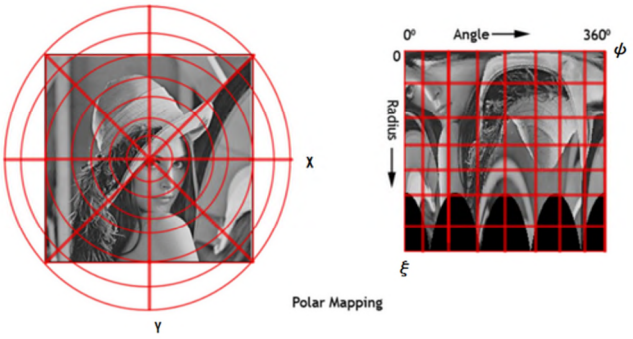


Figure 5. Comparison between rectangular coordinate system and polar coordinate system

Descartes coordinate plane:

$$z = x + yi \quad (4)$$

Polar coordinate plane:

$$\xi = \mathrm{r}, \qquad \psi = \theta$$

$$, \text{where } r^2 = x^2 + y^2, \ \theta = \arctan(\frac{y}{x}) \quad (5)$$

III. EXPERIMENT RESULTS

Watermarks could hardly be extracted when a previous watermark algorithms, which is based on spread spectrum in spatial domain, was used for a robustness test against DA/AD conversion attack of Print-Scan method [5][12].

 ISBN: 978-1-61208-452-7

TABLE 1. TEST ENVIRONMENTS

Test components	Settings
Resolution	1024x1024
Printer	HP Color LaserJet4650
Camera	Samsung galaxy S4
Message bit size	66bit
PSNR	36.21dB
SSIM	0.95162

For a performance test of our algorithm, we proceeded by taking photographs in several different environments. Table 1 shows the basic test environment. The resolution of original digital image is 1024 X 1024. The printer is HP Color LaserJet 4650 for image printing. The camera is Samsung Galaxy S4 to take pictures. 66 bits of watermark payload are embedded and extracted from the taken pictures. The watermark payload does not include any error correction or error detection code.

To evaluate the visual quality of the watermark embedded image, PSNR (Peak Signal to Noise Ratio) and SSIM (Structured Similarity Index Measure) are calculated.

o PSNR – Peak Signal-to-Noise Ratio :

$$PSNR = 10 \cdot log_{10}\left(\frac{255^2}{MSE}\right) \quad (6)$$

$$,where \quad MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[x(i,j) - y(i,j)]^2$$

o SSIM – Structured Similarity Index Measure

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (7)$$

$$,where$$
$$c_1 = (k_1 L)^2, c_2 = (k_2 L)^2$$
$$L = the\ dynamic\ range\ of\ the\ pixel\ values$$
$$k_1 = 0.01,\ \ k_2 = 0.03\ by\ default$$

For taking pictures, Samsung Galaxy S4 is used. Table 2 shows the test conditions of: picture resolution, picture object, and picture place. Two image resolutions of 1280x720 and 1920x1080 are used. The output resolution for rendering in monitor is 1920x1080. In the case of printing papers, a color printer with 600 dpi is used. In capturing from a monitor, only indoor light condition is target for test. However, in capturing from the printed papers, both indoor light and outdoor light are used for the test.

TABLE 2. CAPTURE ENVIRONMENTS

Resolution	Object	Place (experiment environment)
1280x720	Monitor (resolution: 1920x1080)	Indoor
2M pixels (1920 x1080 included)	Prints(color/resolution : 600 dpi)	Indoor/outdoor

Figure 6 shows the digital images which are used for tests. The test digital images are globe image, landscape, and video color bar image.

Figure 6. Digital images used for tests

Figure 7 shows the example of extracting the watermark process: (a) is the result of 2 dimension FFT of the input digital image. To embed 66 bits, a total of 12 circular patterns are used with 11 patterns for message and 1 pattern for reference (b) shows 3 dimensional picture which renders the result of the cross correlation between the reference pattern and entire image values. It shows that the locations of maximum peak for phase are different according to the watermark information (c) shows the changes of maximum correlation values according to radius changes (d) shows the correlation value with the reference pattern.

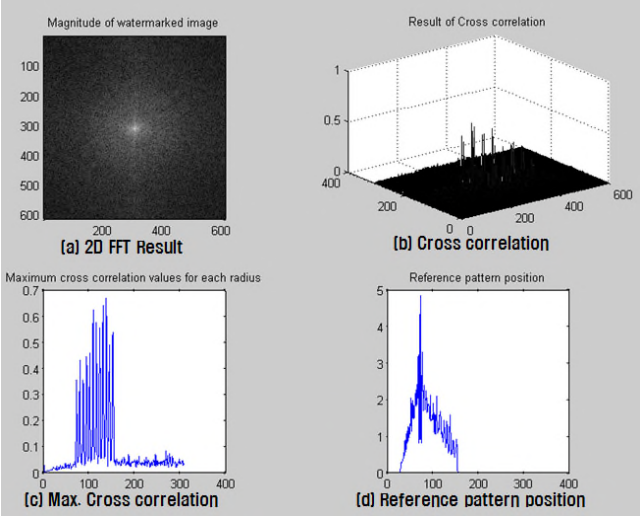
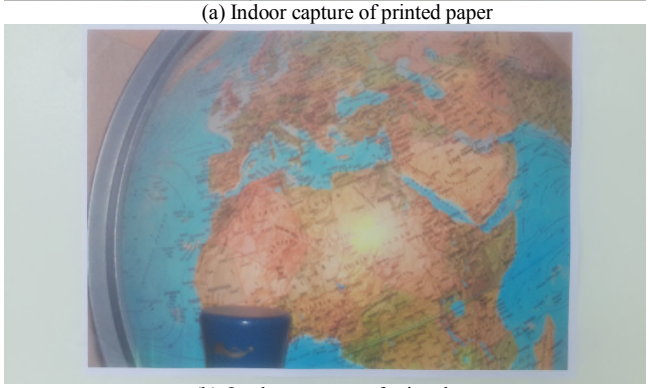


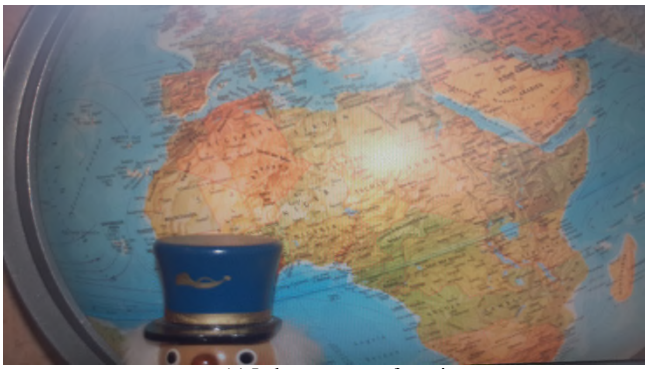
Figure 7. Example of extracting watermark

Figure 8 shows the captured image for watermark detection tests (a) is the camera captured image of the printed paper with watermark embedded in indoor environment (b) is the camera captured image of the printed paper with watermark embedded in outdoor environment (c) is the camera captured image of monitor screen with watermark embedded in indoor environment.

(a) Indoor capture of printed paper



(b) Outdoor capture of printed paper



(c) Indoor capture of monitor

Figure 8. Example of the captured images in test

Table 3 shows the test results to compare the performance of the proposed and spread spectrum method. The spread spectrum method was implemented by Kutter's method [5][6]. Success cases indicate no-error extraction cases with 66 bit data size.

The performance of the algorithm is tested with the captured images of monitor and captured images of the printed images.

When the watermarked digital image is displayed through indoor monitor, the results of extraction rate of same resolution capture is 32% and with 720p resolution is 58%.

In the case of 600 dpi color printed on paper, extraction rate of 1920x1080 resolution is 83% and with 720p is 84% in indoor cases. In the outdoor case, those were 81% and 79% for 1080p and 720p cases respectively.

TABLE 3. EXPERIMENTAL RESULTS

Test	Environment	Proposed Result(Success cases/entire tries, extract rate)	Spread spectrum Method
Indoor print	Color printed in 600 dpi, Captured resolution : 1920x1080	83/100 (83%)	0/100 (0%)
Indoor print	Color printed in 600 dpi, Captured resolution : 1280x720	84/100 (84%)	0/100 (0%)
Outdoor print	Color printed in 600 dpi, Captured resolution : 1920x1080	83/100 (83%)	0/100 (0%)
Outdoor print	Color printed in 600 dpi, Captured resolution : 1280x720	79/100 (79%)	0/100 (0%)
Indoor monitor	Monitor resolution : 1920x1080, Captured resolution : 1920x1080	16/50 (32%)	3/100 (3%)
Indoor	Monitor resolution:	29/50	2/100

monitor	1920x1080, Captured resolution : 1280x720	(58%)	(2%)

IV. CONCLUSION

In this paper, a strong watermark method against AD/DA transformation is proposed. In previous watermark algorithm approach in spatial domain, there is a disadvantage that the algorithm is weak at prints-scan attacks, which is one very strong AD/DA attack. Our algorithm is proposed to overcome this disadvantage and can be extracted regardless of RST attack. This is implemented through a method that generates a reference template watermark pattern in the frequency domain, and extracts watermark using maximum peak location by calculating the correlation between reference pattern and the extracted pattern from the watermarked image.

For evaluating the performance of the algorithm, tests were performed by capturing monitor output and printed images and extracting of watermarks. In the case of monitor output, our algorithm achieved 45% extraction rate on average. In the case of 600dpi color printer, the extraction rate is 83.5% in indoor case, and 81% in outdoor case. Because those results are without error correction mechanisms, we can expect higher extraction rates if we apply it in the future. The performance of proposed algorithm is affected by the capture angle. Further research is required in this area.

ACKNOWLEDGMENT

This research project was supported by Government Fund from Korea Copyright Commission in 2015. (Development of high performative watermarking embedding and detecting system for copyright protection of UHD real-time broadcasting content.).

REFERENCES

[1] J. Nah, J. Kim, and J. Kim, "Video Forensic Marking Algorithm Using Peak Position Modulation," Journal of Applied Mathematics & Information Sciences (AMIS), Vol. 6, No. 3S, pp.2391-2396, 2013.

[2] D. Li, and J. Kim, "Secure Image Forensic Marking Algorithm using 2D Barcode and Off-axis Hologram in DWT-DFRNT Domain," Applied Mathematics and Information Sciences, Vol. 6, 2S, pp. 513-520, 2012.

[3] J. Nah, J. Kim, and J. Kim, "Image Watermarking for Identification Forgery Prevention," Journal of the Korea Contents Association, Vol. 11, No. 12, pp.552-559, 2011.

[4] S. P. Maity, P. K. Nandi, and T. S. Das, "Robustness improvement in spread spectrum watermarking using M-ary modulation," Proc. 11th NationalConferenceonCommunication, NCC2005, pp.569-573, 2005.

[5] M. Kutter, "Performance improvement of spread spectrum based image watermarking schemes through M-ary modulation", Lecture Notes in Computer Science, 1728, pp.238~250, 2000.

[6] M. Kutter, "Watermarking resistant to translation, rotation and scaling," in Proc. SPIE, Int. Symp. Multimedia Systems and Applications, vol. 3528, pp. 423–431, 1998.

[7] C. Lin, C Chang, and Y. Chen, "A Novel SVD-based Watermarking Scheme for Protecting Rightful Ownership of Digital Images," Journal of Information Hiding and Multimedia Signal Processing, Vol.5, No.2, pp.124-143, April 2014

[8] Makhloghi, M., Tab. F. A., and Danyali, H. "A new robust blind DWT-SVD based digital image watermarking", ICEE 2011, Vol.1, pp.1-5, 2011.

[9] M. Wu, and B. Liu, "Data hiding in image and video: Part I—Fundamental issues and solutions," IEEE Trans. Image Process., vol. 12, no. 6, pp. 685−695, Jun. 2003.

[10] P. Pu, X. Guo, and L. Lei., "Application of Image Interpolation in Log-Polar Transformation. Computer Engineering," 34, 5 (2008), pp.198-199.

[11] B. Yu, L. Guo, and T. Zhao, "Gray projection image stabilizing algorithm based on log-polar image transform. Computer Applications," 28, 12 (2008), pp.3126-3128.

[12] Y. Xin, and M. Pawlak, "M-ary Phase Modulation for Digital Watermarking" Int. J. Math. Comput. Sci. 2008, Vol. 18, No. 1, pp.93-104.

 ISBN: 978-1-61208-452-7