Efficient General Print-Scanning Resilient Data Hiding Based on Uniform Log-Polar Mapping

Xiangui Kang, *Member, IEEE*, Jiwu Huang, *Senior Member, IEEE*, and Wenjun Zeng, *Senior Member, IEEE*

***Abstract*—This paper proposes an efficient, blind, and robust data hiding scheme which is resilient to both geometric distortion and the general print-scan process, based on a near uniform log-polar mapping (ULPM). In contrast to performing inverse log-polar mapping (a mapping from the log-polar system to the Cartesian system) to the watermark signal or its index as done in the prior works, we apply ULPM to the frequency index (u, v) in the Cartesian system to obtain the discrete log-polar coordinate (l_1, l_2), then embed one watermark bit $w(l_1, l_2)$ in the corresponding discrete Fourier transform coefficient $c(u, v)$. This mapping of index from the Cartesian system to the log-polar system but embedding the corresponding watermark directly in the Cartesian domain not only completely removes the interpolation distortion and the interference distortion introduced to the watermark signal as observed in some prior works, but also largely expands the cardinality of watermark in the log-polar mapping domain. Both theoretical analysis and experimental results show that the proposed watermarking scheme achieves excellent robustness to geometric distortion, normal signal processing, and the general print-scan process. Compared to existing watermarking schemes, our algorithm offers significant improvement in terms of robustness against general print-scan, receiver operating characteristic (ROC) performance, and efficiency of blind resynchronization.**

***Index Terms*—Geometric distortion, print-scan, uniform log-polar mapping (ULPM), watermark.**

I. Introduction

DIGITAL watermarking technology is popularly used for proof of ownership, content authorization, owner identification, etc. [1]. The print-scan process is commonly used for image reproduction and distribution. Print-scan resilient data hiding provides a viable authentication method via the multibit watermark hidden in a picture in the document. Document authentication of passport, ID card, driving license, etc., is becoming more and more important today due to the security concerns. The general print-rescanned image is usually rotated, scaled, translated, and cropped (RSTC), and its pixel values largely changed [2], [3]. Though watermark robustness has been an active research issue in watermarking community, print-scan resilient data hiding has not been extensively studied. Some state-of-the-art multibit print-scan resilient data hiding schemes proposed to exploit the knowledge of the digital half-toning scheme employed by the LaserJet printer or boundary orientation of a print-scan image [4], [5]. But they did not achieve very good performance in resisting the general print-scan distortion combined with cropping. The image printer might be a LaserJet printer, Inkjet printer, thermal printer, or developing machine, etc. So it is also necessary to develop a device-independent watermarking scheme, which is robust to RSTC distortion and general print-scan simultaneously. Note that a data hiding scheme which is robust to general print-scan should be robust to RSTC distortion with blind resynchronization, but a data hiding scheme which is robust to RSTC distortion is not necessarily robust to general print-scan. Robustness against RSTC distortion with blind resynchronization is necessary for resisting general print-scan. Lin *et al.* [3] and Zheng *et al.* [6]–[8] provided a very good survey of RSTC resilient watermarking.

There are two different types of solutions to resisting geometric attacks: nonblind and blind methods [9]–[12]. The blind solution, which does not use the original image in watermark extraction, has wider application but is obviously more challenging. Although direct exhaustive search for the watermark may be used to combat geometric distortion, it is not an efficient and practical approach due to the high complexity in searching [13]. Three major approaches to the blind solution have been reported in the literature.

1) Invariant Watermark Embedding: The first approach hides a watermark signal in the geometric invariant domain of a host signal [3], [6], [14], [15]. It eliminates the need to identify geometric distortions and invert them, thus it has the potential to detect/extract a watermark from geometric distorted image in real time. Ruanaidh *et al.* [14] first proposed to embed a watermark into the transform invariants by applying the Fourier–Mellin transform [log-polar mapping (LPM) + discrete Fourier transform (DFT)] to the magnitude spectrum of the original image. Lin *et al.* [3] proposed to perform inverse log-polar mapping (ILPM) to the watermark signal, then embed the resulting watermark signal into a 1-D signal obtained by summing a function of the LPM Fourier magnitudes along the log-radius axis. This method eliminates the severe distortion introduced to the host image by performing LPM and ILPM as observed in [14], thus significantly enhancing the quality of stego image and achieving geometric distortion resilience. Zheng *et al.* [6] proposed to use ILPM to get the exact corresponding embedding positions in the Cartesian system and embed each watermark bit in the four neighboring points around the exact position. This method has the advantage of eliminating the interpolation distortion to the watermark, and when the number of watermark bits to be embedded is

Manuscript received March 15, 2009; accepted December 13, 2009. First published January 12, 2010; current version published February 12, 2010. This work was supported by NSFC (60633030), by NSF of Guangdong (9151027501000103), and by the 973 Program (2006CB303104). The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Min Wu.

X. Kang and J. Huang are with the School of Information Science and Technology, Sun Yat-Sen University, Guangzhou 510275, China (e-mail: isskxg@mail.sysu.edu.cn; isshjw@mail.sysu.edu.cn).

W. Zeng is with the Department of Computer Science, University of Missouri-Columbia, MO 65211 USA (e-mail: zengw@missouri.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2009.2039604

limited, potentially eliminating the interference distortion to the watermark by carefully choosing the embedding positions, thus enhances the watermark's robustness. These approaches [3], [6], [15] are based on performing ILPM on the watermark signal or its index in embedding; to be more specific, sample points of the watermark in the log-polar system are inversely log-polar mapped to sample points in the Cartesian system.

The above ILPM-based approaches, however, have the following four limitations. a) Introducing interpolation distortion. Since both of log-polar and Cartesian systems are discrete, one sample point of the watermark in the log-polar system is actually mapped to four discrete points in the Cartesian system (1-to-4 mapping) by bilinear interpolation or other interpolations. b) Introducing interference distortion. The resampled watermark is actually embedded in the DFT domain. But with the application of ILPM to the watermark, multiple sample points of the watermark (e.g., two bits "1", "-1") in the log-polar system may be mapped onto one DFT coefficient A [15], so the change of the value of the DFT coefficient A to embed the bit "1" is interfering with the change of the value of A to embed the bit "-1", thus causing potential watermark interference distortion. In other words, the change of the value of one DFT coefficient may cause changes of multiple points in the log-polar system. To avoid interference distortion, one DFT coefficient should be mapped onto by only one point in the log-polar system (i.e., one bit of the watermark). Some previous works, e.g., [6] and [15], achieve that by carefully choosing the limited embedding position, at the cost of reduced embedding space. c) Reducing the embedding space. The log-polar system is generally a nonuniform resampling system; the farther from the center of the DFT, the lower the sampling rate is, thus largely limiting the embedding space, i.e., limiting the cardinality of the watermark along the log-polar axis. The above-mentioned 1-to-4 mapping from the log polar system to the Cartesian system further reduces the embedding space by a factor of at least 4 (assuming no watermark interference) when compared to adopting a 1-to-1 mapping from the Cartesian system to the LPM system, as shown in Section III in our proposed uniform log-polar mapping (ULPM). In general, a larger watermark cardinality provides more flexibility and can be translated into more watermark energy as well. From another aspect, false positive rate decreases exponentially with the increase of the cardinality (length) of the watermark (see, e.g., (13) in Section V-C) if the detection statistic, i.e., the correlation coefficient between the extracted watermark and the original watermark is chosen to be larger than a constant threshold [3] or equivalently the bit error rate between them is chosen to be less than a constant threshold (see, e.g., (12) in Section V-C). The very limited cardinality of the watermark is believed to be one of the major limiting factors to the performance of the existing watermarking schemes [3], [6], [15]. Note that the limited cardinality of the watermark also encroaches on the space that can be used to embed a pilot signal for self-resynchronization. d) Depending on the original sampling rate. One sampling point of the watermark in the log-polar system is actually mapped to one lattice of the Cartesian system. Apparently, the lattice depends on the original sampling rate of the Cartesian system. After image scaling, the sampling rate of the Cartesian system is changed. It is necessary to recover the original sampling rate before watermark extraction, thus there is no self-resynchronization capability. That is probably why the exhaustive search-based resynchronization method or nonblind resynchronization method has been adopted in the watermark detection in [3], [6], and [15]. Overall, they cannot be used as an effective, general print-scan resilient data hiding (hiding a message of multibit) scheme.

Some other approaches based on moments normalization [17], Zernike moments [18], [19], and radon transform [20] have also been proposed. Their major limitation is the weak performance to resist geometric distortion combined with cropping because cropping results in the changes of moments. In addition, circular harmonic filtering-based watermarking scheme [21] is only rotation invariant, and the fidelity of the watermarked image of the bispectrum-based embedding approach is not satisfied [8], [22].

2) Template or Periodic Pattern Insertion: Different from the first blind approach, the second blind approach is to explicitly remove or invert the geometric distortion in order to resynchronize the geometrically distorted image before watermark extraction/detection [23]–[29]. One way to achieve this is to embed a template together with the embedded informative watermark (the message to be conveyed to the detector/receiver) [24], [25]. Another way is to let the watermark assume the roles of both a template and the copyright information bearer. Kutter [26] and Voloshynovskiy *et al.* [28], [29] exploit the self-reference principle based on an auto-correlation function or the Fourier magnitude spectrum of a periodical watermark. But the existence and the position of the template or periodic pattern in the frequency domain can be detected without a key, thus it is relatively easy to be removed by template removal attack [30], [32]. Recently, Dugelay *et al.* [16] proposed an optical-flow-based scheme to resist local geometric distortions such as the random bending introduced by Stirmark. But their method only works for small geometric distortions; it fails when the watermarked image undergoes large geometric distortion (such as rotation by 3°, large scaling, and large translation).

3) Feature Points-Based Embedding: The third blind approach is based on the image salient points, such as corners and edges, to construct a geometric distortion resilient watermarking scheme [30], [31]. The advantage of this method is that it can resist both global geometric distortion and local geometric distortion. The successful detection of the salient points against various image manipulations, including print-scan which corrupts an image severely, are crucial for this class of watermarking schemes.

Despite the above efforts, as pointed out in the state-of-the-art survey [7], [8],

> An ideal RST invariant image watermarking algorithm should be truly robust against RST transformations, be truly blind in detecting watermark, and guarantee correct and fast watermark detection with low error rate. In order to achieve this goal, more dedicated research is needed.

Furthermore, most of the above watermarking schemes are not specifically designed to be robust to print-scan. Robust to both general print-scan and geometric distortion is still a challenging issue. In this paper, we propose a multibit watermarking scheme, which is robust to both the general print-scan and geometric distortion, based on a novel near ULPM. The proposed scheme completely removes the limitations of the ILPM-based methods

mentioned above, significantly improves over prior solutions, and has self-resynchronization capability.

The rest of the paper is organized as follows. In Section II, we discuss the general print-scan distortion and review the log-polar system. In Section III, we propose ULPM and introduce the embedding process. Section IV presents the proposed watermark extraction scheme based on an efficient blind resynchronization. Experimental results are presented in Section V. Section VI draws the conclusion.

II. Print-Scan Distortion and Fourier Log-Polar System

In this section, we discuss the distortion of general print-scan and introduce the Fourier log-polar system.

A. Distortion of General Print-Scan

The distortions introduced by a print-scan process are very complex, and may depend on the particular printer and scanner. Lin *et al.* [2] first modeled the distortion after the print-scan process with an Inkjet printer as the geometric distortion augmented with the change of its pixel values due to the luminance and contrast adjustment and nonlinearity of the conventional printing and scanning system. The geometric distortion includes rotation, scaling, translation, and cropping. Solanki *et al.* [5] and He *et al.* [4] further analyzed the properties of the magnitudes of the DFT coefficients after print-scan with a LaserJet printer. After performing similar experiments on general print-scan with several different types of printers and scanners, we generalize the print-scan distortion as follows:

1) The distortion of image DFT coefficients includes both nonlinear distortion and additive random noise. Let y denote the magnitude of the DFT coefficients of a rescanned image and x the original coefficient magnitude, then $y = f(x) + n$, where n is additive random noise. $f()$ is of any form and is related to the particular printer and scanner, with a loose restriction to its average derivative: $E(f'(x)) > 0$. In other words, on average, large coefficients tend to be large after print-scan. This meets the requirement that the rescanned image should be perceptually similar to the original one. He *et al.* [4] also observed that most relationships between DFT coefficients are preserved though individual DFT magnitude may vary. Please refer to [5, p. 474] for some examples of the illustration on the nonlinear relationship between y and x with a LaserJet printer. Our experiments with an Inkjet printer and developing machine show similar results. This observation will be used to explain analytically why the proposed spread spectrum embedding is robust to general print-scan.
2) The geometric distortion generated by the print-scan process is the RSTC distortion. To combat the RSTC distortion, we adopt the Fourier log-polar method, but develop a more delicate treatment to improve embedding capacity and robustness.

B. Fourier Log-Polar System

Consider the Fourier transform $I_0(u, v)$ of an image and the Fourier transform $I_1(u, v)$ of a rotated , scaled, and translated version of this image, where u and v are the coordinates in the Cartesian Fourier coordinate system, and are also referred to as frequency index in this paper. Using the log-polar coordinates, we have

$$\begin{aligned} u &= a^{\rho}\cos\theta \\ v &= a^{\rho}\sin\theta \end{aligned} \tag{1}$$

where ρ and θ, respectively, are the log-radial (log-polar) and the angular coordinate in the log-polar coordinate system, and a is the base. The magnitude of the Fourier spectrum has the following property [3], [6], [14]:

$$|I_1(\rho,\theta)| = |\sigma|^{-2}\,|I_0(\rho - \log_a \sigma, \theta - \theta_0)| \tag{2}$$

where θ_0, σ are the rotation angle and scaling factor, respectively. Equation (2) implies that the image Fourier log-polar domain is very appropriate for watermark embedding because it simplifies the effects of RST transforms in the spatial system to shifts in the log-polar system.

III. Watermark Embedding Based on ULPM

In this section, we propose to perform the near ULPM to the frequency *index* in the Cartesian system to obtain a discrete log-polar point, the corresponding watermark bit of which is then embedded to the corresponding DFT coefficient in the Cartesian system.

A. Uniform Log-Polar Mapping

A watermark may be embedded in the frequency coefficients ranging from minimum frequency $r_{\min}$ to maximum frequency $r_{\max}$. We observe that in (1), the interval in the Cartesian system between two neighboring log-polar grid points (i.e., a^{i-1} and a^i) is $a^i - a^{i-1}$. The quotient of two neighboring intervals is $(a^{i+1} - a^i)/(a^i - a^i - 1) = a$. If the quotient a is closer to 1, there are more log-polar grid points between $r_{\min}$ and $r_{\max}$, and the intervals become more uniform. We thus choose the base a to be a value close to 1 but bigger than 1 to construct a near uniform mapping. We propose to choose $a = b^{1/M}$, where $b = r_{\max}/r_{\min} > 1$ and is chosen to be 2 in our work, M is the number of log-polar intervals between $r_{\min}$ and $r_{\max}$, and is related to the cardinality of the hidden data along the log-polar direction. Compared with adopting the base a being e or 2, the proposed ULPM significantly expands the number of intervals along the log-polar direction from 1 (since $a = b = r_{\max}/r_{\min} = 2$) to M. The LPM is applied on the frequency index to insure that one DFT coefficient is mapped onto by only one point in the log-polar system, obtaining a 1-to-1 (or many-to-1 if so chosen) mapping of sample index from the Cartesian system to the log-polar system. The actual watermark embedding is directly implemented in the DFT domain based on the discrete log-polar coordinate of the frequency index, without requiring watermark signal interpolation. This embedding method not only completely removes the interpolation and interference distortion introduced to the watermark, but also expands its cardinality and avoid relying on the original sampling rate, thus completely removes the limitations of the ILPM-based methods mentioned in Section I.

B. Data Embedding Based on ULPM

The hidden data, composed of a tracking sequence and an informative watermark, is arranged in the log-polar Fourier domain. The tracking sequence is used to resynchronize the

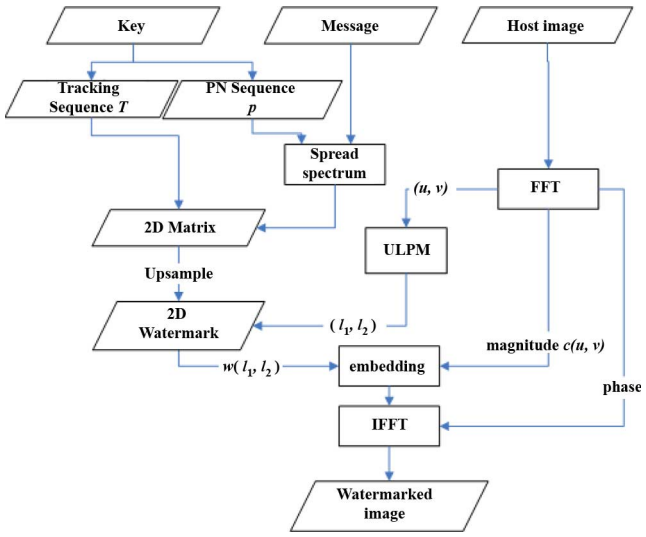


Fig. 1. Proposed embedding process based on ULPM.

multibit informative watermark. The proposed embedding process is shown in Fig. 1 and is described in detail in the following.

1) Watermark Formation: Using a key, we generate a tracking sequence $\boldsymbol{T}$ of length $N_T\{T_n; n = 0, \ldots, N_T - 1\}$, $T_n \in \{-1, 1\}$, and a N_p-bit bipolar PN-sequence $\boldsymbol{p} = \{p_j; j = 0, \ldots, N_p - 1\}$, respectively. $\boldsymbol{p}$ is a balanced sequence with half of the bits being "-1". An L-bit message $\boldsymbol{m}\{m(i), i = 0, \ldots, L - 1, m(i) \in \{0, 1\}\}$ is first encoded using an error correction code to obtain the message $\boldsymbol{m}_c\{m_{ci}; i = 0, \ldots, L_c - 1, m_{ci} \in \{0, 1\}\}$ of length L_c. Then each bit of $\boldsymbol{m}_c$, denoted as m_{ci}, is direct sequence spread spectrum (DSSS) encoded using $\boldsymbol{p}$, where a bit of "1" is encoded as a spread spectrum sequence $\boldsymbol{W}_i\{w_{ij}; w_{ij} \in \{-1, +1\}, 0 \le j < N_p\} = +1 \times \boldsymbol{p}$, and a bit of "0" as $\boldsymbol{W}_i = -1 \times \boldsymbol{p}$. Then we shape all tracking sequence bits and all DSSS encoded bits into a 1-D sequence. Note that images frequently have a large amount of energy along some directions, while having much less energy along the orthogonal direction. For example, images containing buildings and trees have significant vertical structure yielding more energy in the horizontal frequencies than in the vertical frequencies, while seascapes or sunsets are strongly oriented in the horizontal direction yielding higher vertical frequencies [3]. To take advantage of this property, we arange all bits from the obtained 1-D sequence column-wise to form an $M/2 \times N/2$ 2-D matrix. Then the obtained matrix is upsampled, along the row and column, respectively, by a factor of 2 (in practical implementation, each row is repeated once first to obtain another matrix, then each column of the obtained matrix is repeated once) to obtain an upsampled version, $M \times N$ 2-D matrix $\mathbf{W}\{w(m, n)\}(0 \le m < M, 0 \le n < N)$. $\mathbf{W}$ consists of the informative watermark (payload) portion $\mathbf{W}_1$ and the tracking pattern $\mathbf{W}_2$. Here $N_T = M/2 \times N/2 - L_c \times N_p$. The doubly upsampled pattern $\mathbf{W}_2$ is expected to have higher precision in tracking the location of $\mathbf{W}_1$ in the extraction process.

2) Applying ULPM to the Frequency Index: Apply 2-D DFT to a host image, shift the dc component to the center of the Fourier magnitude spectrum, and the center is used as the origin of the Cartesian plane. Choose the base a as

$$a = 2^{1/M}. \tag{3}$$

Apply the log-polar transform in (4) to the frequency index (u, v) (normalized frequencies) or polar coordinate (r, θ) to obtain the discrete log-polar coordinate (l_1, l_2)

$$\begin{aligned} l_1 &= \text{floor}\left(\log_a \frac{r}{R}\right) + \frac{M}{2} \\ l_2 &= \text{floor}\left(\frac{N \times \theta}{\pi}\right) \end{aligned} \tag{4}$$

where $r = \sqrt{u^2 + v^2}$, $\theta = \arctan(u/v)$, R is referred to as the base frequency in this paper, as $r = R$ results in a zero for $\log_a r/R$ may be chosen to be about $0.15 \sim 0.25$ because we embed watermark in low and middle frequencies to achieve a better compromise between robustness and invisibility. floor() represents the floor operation. For the chosen embedding magnitude coefficients, the polar r meets the condition

$$a^{-M/2} \times R \le r < a^{M/2} \times R. \tag{5}$$

It is easy to prove that $0 \le l_1 < M, 0 \le l_2 < N$. Equation (5) shows that the watermark embedding area in the DFT domain is a circular area (see Fig. 2), almost centered at the base frequency R. If $R = 0.2$, r is between $r_{\min} = R \times 2^{-0.5} = 0.14$ and $r_{\max} = R \times 2^{0.5} = 0.28$.

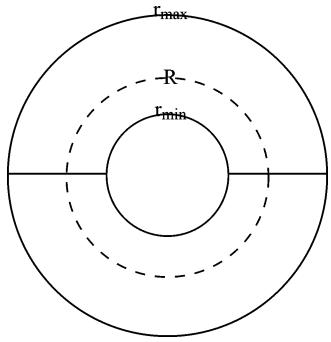


Fig. 2. Embedding frequency ranges from $r_{\min}$ to $r_{\max}$. The dashed line corresponds to the base frequency R.

3) Data Embedding: The watermark is actually embedded into DFT coefficients according to its discrete log-polar coordinate (l_1, l_2) which is obtained with (4). Note that one bit is embedded into all the DFT coefficients with the same log-polar coordinate (l_1, l_2) using a multiplication embedding method as illustrated in (6)

$$c'(u, v) = c(u, v) \times (1 + \alpha \times w(l_1, l_2)) \tag{6}$$

where $c(u, v)$, $c'(u, v)$ are the Fourier magnitude coefficients before and after embedding. α is the embedding strength. For example, α may be chosen to be $0.20 \sim 0.25$ in our work to achieve a good trade-off between robustness and invisibility of watermark. There is no interference distortion or interpolation distortion. Note that one advantage of implementing watermark embedding in the Fourier magnitude domain is the ease in controlling the watermark energy associated with each Fourier coefficient which facilitates perceptual quality control. For a

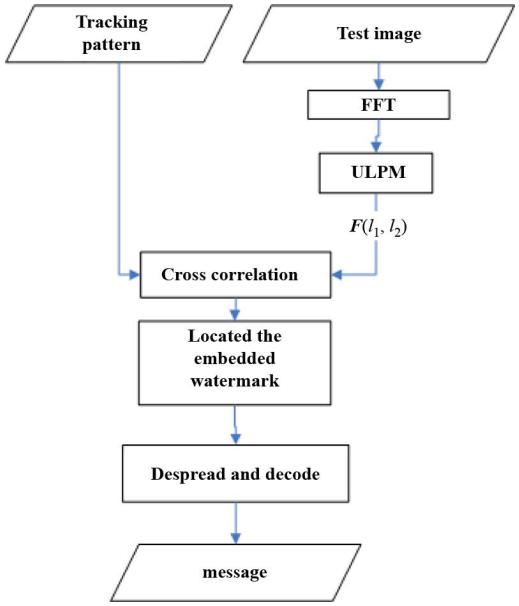


Fig. 3. Proposed watermark extraction process.

512×512 cover image, if we choose $M = 64$, the actual cardinality of the hidden data is $M/2 = 32$, the minimum resampling interval (in the Cartesian system) of the LPM system shown in (4) with base ($a = 2^{1/32} = 1.0219$) is $0.14 \times 512 \times (a^1 - a^0) = 1.6$, which is larger than the sampling interval $\sqrt{2}$ of the Cartesian system, so it is a one-to-one mapping or many-to-one mapping from the Cartesian system to the log-polar system. The cardinality of the hidden data along the log-radius axis can be larger than 32. The proposed watermark embedding in the Fourier magnitude domain is conceptually equivalent to embedding in the log-polar Fourier domain.

Finally, the inverse DFT is applied to the modified Fourier coefficients to obtain the watermarked image.

IV. Watermark Extraction

The watermark detector/extractor is assumed to have no prior knowledge of the original image. The tracking pattern and the original PN-sequence $\boldsymbol{p}$ may be generated by a key, which is known to the detector. The watermark extraction process as illustrated in Fig. 3 is divided into three steps.

1) Performing ULPM: We apply the log-polar transformation in (4) to the frequency index, as applied in embedding, to obtain the log-polar coordinate (l_1, l_2). Let r denote the polar of the coefficients within the tracking area, then

$$a^{-\lambda M} \times R \leq r < a^{\lambda M} \times R \tag{7}$$

where λ is a parameter which only controls the size of the tracking area. A larger λ results in a larger tracking area, but a higher false tracking rate. To take into account the scaling impact (scaling in the image spatial domain results in a reciprocal scaling in the frequency domain), λ should be chosen to be larger than 1/2 to lead to a larger tracking area in the extraction than that in the embedding. We choose $\lambda = 1$ in our work. Because it is a many-to-one LPM, we compute the mean of all magnitude coefficients with the same coordinate (l_1, l_2) to obtain an LPM matrix . $F(l_1, l_2)(0 \leq l_1 < 2\lambda M, 0 \leq l_2 < N)$.

2) Watermark Resynchronization: One way to track the embedded watermark's location is to slide tracking pattern $\mathbf{W}_2$ over $F(l_1, l_2)$ along the l_1 axis and l_2 axis and measure the cross correlation between $\mathbf{W}_2$ and $F(l_1, l_2)$ at discrete shift positions $\{(k_1, k_2),\ 0 \leq k_1 < 2\lambda M, 0 \leq k_2 < N\}$. Search for the maximum correlation to locate the best matching position. This exhaustive search method takes too much time. A faster way is to use the correlation theorem [33]. To achieve that, $\mathbf{W}_2$ is first padded with 0s to obtain a new matrix $g(l_1, l_2)$ of the same size. The cross correlation is shown in equation (8) at the bottom of the page. According to the correlation theorem [33]

$$\begin{aligned} r'(k_1, k_2) &= F(l_1, l_2) \otimes g(l_1, l_2) \\ &= \mathrm{IDFT}(\bar{F}(u, v) G^*(u, v)) \end{aligned} \tag{9}$$

where "$\otimes$" represents the cross correlation operation which is shown in (8), $\bar{F}(u, v) = \mathrm{DFT}(F(l_1, l_2))$, $G(u, v) = \mathrm{DFT}(g(l_1, l_2))$. That is, $\bar{F}(u, v)$, $G(u, v)$ are the DFT coefficients of $F(l_1, l_2)$, $g(l_1, l_2)$, respectively. $G^*(u, v)$ represents the complex conjugate of $G(u, v)$.

Both of the above methods might cause a false alarm because the dynamic range of $F(l_1, l_2)$ is large for low frequency magnitude coefficients. Zheng *et al.* [6] proposed to use phase-only cross correlation between the Fourier LPM of the original image and the Fourier LPM of the watermarked image to resynchronize the watermark in the LPM domain, and demonstrated that it is efficient and effective for nonblind resynchronization. We extend their work and the previous works [34]–[36] to the blind synchronization problem we have here, and propose the following customized phase correlation method to find the matching location as follows:

$$\begin{aligned} r(k_1, k_2) &= \mathrm{IDFT}[\bar{F}_\phi(u, v) G^*(u, v)] \\ \bar{F}_\phi(u, v) &= e^{j\phi_{\bar{F}}(u, v)} \end{aligned} \tag{10}$$

where $\phi_{\bar{F}}(u, v)$ is the phase of $\bar{F}(u, v)$. It is noted that the customized phase correlation method in (10) is different from the phase-only cross correlation used in [6]. Here we use $G(u, v)$ instead of phase $G_\phi(u, v) = e^{j\phi_G(u, v)}$ since the elements of the weak signal $g(l_1, l_2)$ assume a value between -1, 0, and 1, so its dynamic range is limited, and the bipolar values (-1 and 1) help to suppress the matching noise (i.e., contributed by the strong cover image). This advantage of suppressing the matching noise disappears if only phase of the weak signal is used. Our proposed phase correlation method also has some computational advantages.

Then we find the maximum phase correlation of $r(k_1, k_2)$ (see, e.g., Fig. 4) to locate the matching position. We performed a lot of hidden data recovery experiments to compare the cross correlation operation with three methods: 1) the cross

$$r'(k_1, k_2) = \sum_{l_1=0}^{2\lambda M-1} \sum_{l_2=0}^{N-1} F(l_1, l_2) g((l_1 + k_1) \bmod 2\lambda M, (l_2 + k_2) \bmod N) \tag{8}$$

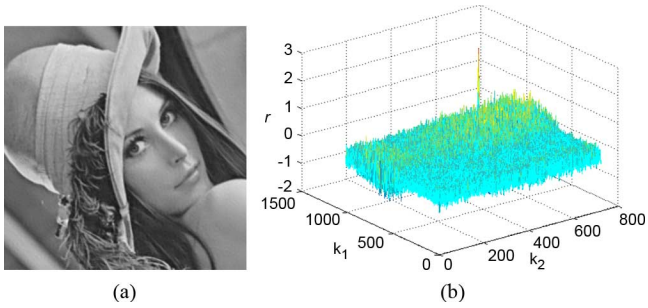


Fig. 4. (a) Watermarked image rotated by 45°, cropped for reframing, then scaled back to 512 × 512. The 60-bit message can be recovered without error. (b) The corresponding peak of the phase correlation.

correlation $r'(k_1,k_2)$; 2) the customized phase cross correlation $r(k_1,k_2)$; 3) the phase-only cross correlation, which is used in [6], i.e., $r''(k_1,k_2) = \mathrm{IDFT}[\bar{F}_\phi(u,v)G^*_\phi(u,v)]$. The customized phase cross correlation $r(k_1,k_2)$ gives the best hidden data extraction results among the above three methods. For example, when the watermarked Lena image is subjected to a combination attack of JPEG compressed with quality factor 50% and print-scan, the success ratio of recovering a hidden 60-bit message with the three methods are 65%, 75%, 53%, respectively. We then obtain the resynchronized magnitude coefficients matrix $\hat{F}_u(l_1,l_2)(0 \le l_1 < M, 0 \le l_2 < N)$ which has been embedded with the watermark $\mathbf{W}$. The $\hat{F}_u(l_1,l_2)$ is then downsampled to obtain a magnitude coefficients matrix $\hat{F}(l_1,l_2)(0 \le l_1 < M/2, 0 \le l_2 < N/2)$. In the implementation, for each element of $\hat{F}(l_1,l_2)$, we compute the average of its value at 4 repeating positions in matrix $\hat{F}(l_1,l_2)$ corresponding to upsampling.

3) Despread and Decode: We then extract N_p magnitude coefficients from matrix $\hat{F}(l_1,l_2)$ to form a sequence $\boldsymbol{W}^*_i$, which corresponds to the embedded spread spectrum sequence $\boldsymbol{W}_i$, and correlate it with the original PN sequence $\boldsymbol{p}$ (generated by a key shared by the detector). If the correlation is larger than 0, the extracted bit m^*_{ci} is determined to be "1"; otherwise, m^*_{ci} is determined to be "0". This process is referred to as the despread spectrum process. Then the obtained sequence $\boldsymbol{m}^*_c$ is error correction decoded to recover the L-bit message $\boldsymbol{m}^*$.

Now we examine the despread process in detail. Suppose the magnitude coefficients before and after attack (such as print-scan) are c'_j, w^*_j . The restriction to function $w^*_j = f(c'_j)$ is its average derivative $E(f'(c'j)) > 0, 0 \le j < N_p$. When the magnitude coefficients are embedded with $+\boldsymbol{p}\{p_j\}$, if $p_j = +1$, $c'_{j+} = c_j + \alpha c_j$; if $p_j = -1$, $c'_{j-} = c_j - \alpha c$. The correlation value

$$\begin{aligned} W^*_i \times \boldsymbol{p} &= \sum_{w^* \in w^*_+} w^*_j - \sum_{w^* \in w^*_-} w^*_j \\ &= \frac{N_p}{2}[E(f(c'_{j+})) - E(f(c'_{j-}))] \\ &\approx \frac{N_p}{2}[E(f(c_j) + \alpha c_j f'(c_j)) - E(f(c_j) - \alpha c_j f'(c_j))] \\ &= N_p \alpha E(c_j)[E(f'(c_j))] > 0 \end{aligned} \tag{11}$$

where $w^*_+ = \{w^*(j)|p_j = 1\}$, $w^*_- = \{w^*(j)|p_j = -1\}$, $E()$ denotes the average operation, and the additive noise is omitted. When the magnitude coefficients are embedded with $-\boldsymbol{p}$, the correlation value is less than zero. So theoretically, the spread spectrum embedding can be robust to nonlinear distortion of the magnitude coefficients introduced in print-scan.

In summary, the watermark extraction process as illustrated in Fig. 3 is divided into three steps:

1) Perform ULPM. Perform ULPM to the test image to obtain an LPM matrix $F(l_1,l_2)$.
2) Watermark auto-synchronization. Perform an efficient cross correlation between the tracking pattern and $F(l_1,l_2)$ to locate the embedded watermark.
3) Despread and decode. Despread with the original PN sequence, decode with error correction code to recover the message.

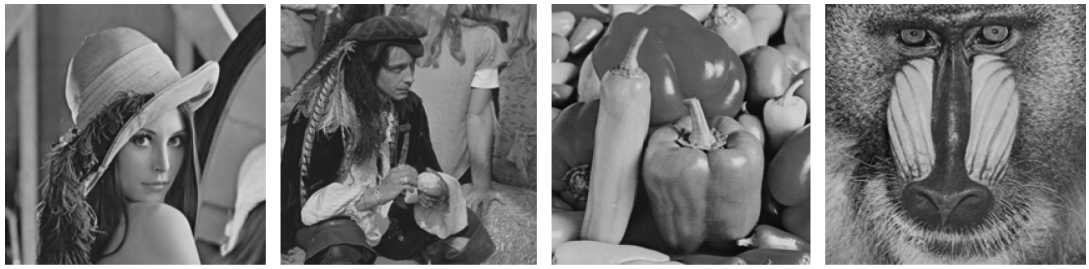
V. Experimental Results

The proposed watermarking scheme is applied on a variety of images. In our experiments, we choose $M = 64$, $N = 360$, $R = 0.2$, $N_p = 64$. BCH (72, 60) code [25] is adopted, which can correct up to 5 bits of error. We also observe that having tracking sequence bits being about 20% (1152 bits in this case) is a good choice to achieve a compromise between tracking the resynchronization location and decoding message $\boldsymbol{m}$ correctly. The embedded message is 60 bits; after BCH and spread spectrum coding, it is $72 \times 64 = 4608$ bits. In Section V-A, we will show the robustness test results for four selected sample images which have varying texture contents. In Section V-B, we perform the psycho-visual quality assessment with a set of 45 images and compare the proposed scheme with the state-of-the-art print-scan resilient work proposed in [5]. In Section V-C, the proposed scheme is compared with some other geometric distortion resilient watermarking schemes.

A. Test Results on Robustness

We test the watermark robustness to a number of distortions/attacks, including JPEG compression, Gaussian filtering, median filtering, sharpening, cropping, scaling, translations, the combination of rotation, scaling, and cropping (RSC), print-scan, developing-scan, etc. The results on the $512 \times 512 \times 8$ images "Lena," "Man," "Peppers," and "Baboon" are reported here. The peak-signal-to-noise ratios (PSNRs) of the watermarked "Lena," "Man," "Peppers," and "Baboon" images are 43.7, 41.6, 43.1, and 38.0 dB (note that "Baboon" is a complex image which can accommodate more watermark energy), respectively. The watermark is invisible as shown in Fig. 5. The robustness test results shown in Tables I–VI and Items 1–8 below are the test results with Stirmark 4.0 Benchmark. "Erroneous bits" refers to the number of erroneous bits in a total of 72-extracted watermark bits in $\boldsymbol{m}^*_c$ before BCH decoding; "y" indicates that the 60-bit message "SunYatSenU" can be recovered without error after BCH decoding; otherwise we use "n" to indicate that there is at least one bit error after BCH decoding.

1) Robustness to Normal Signal Processing: The 60-bit message can be recovered without error from JPEG compression (Table I) with a quality factor as low as 20% (i.e., JPEG_20) for "Lena," 15% for "Man," 20% for "Peppers," and 10% for "Baboon," respectively. The watermark is also robust to 3 × 3 Gaussian filtering, 3 × 3 sharpening, and 3 × 3 median filtering as shown in Table I.



(a) (b) (c) (d)

Fig. 5. Watermarked images. (a) Lena; (b) Man; (c) Peppers; (d) Baboon.

TABLE I
ROBUSTNESS TO NORMAL SIGNAL PROCESSING

signal processing	Lena		Man		Peppers		Baboon	
	Erroneous bits	message recovered?	Erroneous bits	message Recovered?	Erroneous bits	Message Recovered?	Erroneous bits	Message Recovered?
JPEG_20	3	y	1	y	2	y	0	y
JPEG_ 25~100	0	y	0	y	0	y	0	y
Gaussian filtering	0	y	0	y	1	y	1	y
sharpening	0	y	0	y	0	y	0	y
median filtering	0	y	0	y	0	y	0	y

"Erroneous bits" refers to the number of erroneous bits in a total of 72 extracted watermark bits before BCH decoding. "y" indicates that the 60-bit message can be recovered without error after BCH decoding

TABLE II
ROBUSTNESS TO CROPPING

	Lena		Man		Peppers		Baboon	
	Erroneous bits	Message Recovered?	Erroneous bits	Message Recovered?	Erroneous bits	Message Recovered?	Erroneous bits	Message Recovered?
Cropping_1~30%	0	y	0	y	0	y	0	y
Cropping_35%	0	y	0	y	2	y	1	y
Cropping_40%	2	y	3	y	1	y	2	y
Cropping_45%	1	y	1	y	1	y	1	y
Cropping_50%	2	y	1	y	2	y	3	y

TABLE III
ROBUSTNESS TO RESCALING

	Lena		Man		Peppers		Baboon	
Scale factor	Erroneous bits	Message recovered?	Erroneous bits	Message recovered?	Erroneous bits	Message recovered?	Erroneous bits	Message recovered?
0.6	0	y	1	y	1	y	1	y
0.7~1.6	0	y	0	y	0	y	0	y
1.7	0	y	0	y	0	y	0	y
1.8	1	y	0	y	0	y	0	y
1.9	1	y	0	y	0	y	0	y
2.0	3	y	0	y	2	y	4	y

2) Robustness to Cropping and Translation: In Table II, "cropping_$x\%$" means that the watermarked images are cropped by $x\%$ along both the width axis and the height axis, e.g., for $x = 50, 75\%$ of the image pixels are cropped. Table II shows that the 60-bit message can be recovered without error even after cropping_50%. The watermark is also robust to translation.

3) Robustness to Rescaling: It is also robust to image size scaling with the rescaling factor σ (for each dimension) between $0.60 \sim 2.0$ (Table III). That is, the variation range of σ (the largest σ over the smallest σ) can be more than 3, and the variation range of the scaled image size can be about 11. This is very useful in resisting print-scan distortion because the size of the rescanned image usually differs largely from the original size of its digital version.

4) Robustness to Rotation Without Cropping: We perform the rotation without cropping by angles between $0^\circ \sim 360^\circ$ with step $= 0.1^\circ$. The 60-bit message survives all of the rotation angles for all the images tested.

5) Robustness to Rotation With Auto-Cropping and Scaling (RSC): The watermarked image is rotated by an angle, then auto-cropped by reframing, then rescaled back to the original size. Fig. 4(a) shows an example of the attacked image of RSC $- 45^\circ$. The watermarked image is rotated by 45°, cropped

TABLE IV
ROBUSTNESS TO ROTATION, CROPPING, AND SCALING

	Lena		Man		Peppers		Baboon	
rotation angle(°)	Erroneous bits	message recovered ?	Erroneous bits	message recovered ?	Erroneous bits	message recovere d?	Erroneous bits	message recovered ?
0.3	1	y	0	y	0	y	0	y
0.5	1	y	0	y	0	y	0	y
1	0	y	0	y	0	y	0	y
1.5	0	y	0	y	0	y	1	y
2	0	y	0	y	0	y	2	y
5	0	y	0	y	1	y	2	y
5.5	0	y	0	y	1	y	2	y
10	1	y	1	y	0	y	1	y
10.5	1	y	2	y	1	y	0	y
20	0	y	1	y	0	y	2	y
30	0	y	0	y	0	y	2	y
40	1	y	1	y	2	y	0	y
44.5	2	y	1	y	2	y	2	y
44.7	0	y	1	y	4	y	1	y
45	1	y	1	y	2	y	2	y

TABLE V
ROBUSTNESS TO SHEARING, ROW AND COLUMN REMOVAL

	Lena		Man		Peppers		Baboon	
Scale factor	Erroneous bits	message recovered?	Erroneous bits	message recovered?	Erroneous bits	message recovered?	Erroneous bits	message recovered?
shearing_x_0.00_y_1.00	1	y	0	y	1	y	2	y
shearing_x_1.00_y_0.00	2	y	0	y	0	y	1	y
1_row_1_col_removed	1	y	0	y	0	y	1	y
5_row_1_col_removed	0	y	5	y	0	y	0	y
1_row_5_col_removed	0	y	0	y	0	y	0	y

TABLE VI
ROBUSTNESS TO SMALL RANDOM DISTORTION

strength of random distortion	Lena		Man		Peppers		Baboon	
	Erroneous bits	message recovered ?	Erroneous bits	message recovered ?	Erroneous bits	message recovere d?	Erroneous bits	message recovered ?
0.1	1	y	0	y	1	y	0	y
0.2	1	y	0	y	1	y	0	y
0.3	1	y	2	y	1	y	0	y
0.4	1	y	3	y	7	n	3	y
0.5	2	y	15	n	9	n	9	n
0.6	10	n	21	n	12	n	11	n
0.7	12	n	19	n	15	n	22	n
0.8	18	n	27	n	29	n	27	n
0.9	24	n	27	n	18	n	27	n
1.0	26	n	29	n	34	n	33	n

to 363×363 due to reframing in order to remove the padded area during rotation, then scaled back to 512×512. RSC $- 45°$ has the most severe distortion among all the rotation angles because it undergoes the most severe cropping (due to reframing) and the most severe scaling (scaling back to 512×512) among all RSC StirMark functions. We perform RSC with rotation angles between $0° \sim 360°$ with step $= 0.1°$. The 60-bit message survives all of the rotation angles for all the images tested. Some of the results are shown in Table IV (because of the symmetry of DFT and that RSC $-$ $45°$ has the most severe distortion, we only list angles between $0° \sim 45°$).

6) Robustness to the Combination Attack of RSC and JPEG Compression: Our scheme is also robust to the combination attack of RSC and JPEG compression. The watermarked image is attacked by RSC $-$ $45°$, then is JPEG_50 compressed. The message can be recovered without error for all tested images.

7) Robustness to Shearing, and Row and Column Removal: The watermark is also robust to mild shearing, and row and column removal as shown in Table V. For example, the message can be recovered from Shearing_x_0.00_y_1.00 (shearing 1% along the y-axis) and 1_row_5_col_removed (randomly remove one row and five columns).

8) Robustness to Stirmark Small Random Distortion Attack: The results with varying strength are shown in Table VI. It shows that the watermark is robust to small random distortion attack with strength less than or equal to 0.3.

9) Robustness to Aspect Ratio Change: For the aspect ratio change, the 512×512 watermarked image is resized with bilinear interpolation to size between 512×504 and 512×530, the watermark is shown to be also robust to the mild aspect ratio change ($\pm 8/512 = \pm 0.0125$). This is important for the robustness against print-scan because there exists mild aspect

TABLE VII
SUCCESS RATIOS SURVIVING PS (COLOR LASERJET PRINTER) WITH DIFFERENT JPEG QF

JPEG QF	Lena	Man	Baboon	Peppers
100	100%	100%	100%	100%
80	100%	100%	100%	100%
50	97%	100%	100%	100%

TABLE VIII
SUCCESS RATIOS SURVIVING PS (B/W LASERJET PRINTER) WITH DIFFERENT JPEG QF

JPEG QF	Lena	Man	Baboon	Peppers
100	100%	100%	100%	100%
80	100%	100%	100%	100%
50	75%	100%	100%	86%

(a) (b)

Fig. 6. Print-scanning images. (a) 690×770 (HP LaserJet 2600n); (b) 680×763 (HP LaserJet 2015n).

(a) (b)

Fig. 7. Cropping and print-scanning images. (a) Cropping_50% +PS; (b) cropping_40% +PS. The 60-bit message can be recovered without error.

ratio change ranging from $-0.01 \sim +0.01$ in the rescanned image.

10) Robustness to Print-Scan With Laserjet Printer: Particularly, the proposed watermarking scheme is robust to the combination attack of JPEG compression and print-scan (PS). For every test image reported here ("Lena," "Man," "Baboon," or "Peppers"), we choose ten random key k_w to generate ten watermarked images. Each watermarked image was JPEG compressed with a quality factor (QF) of 100%, 80%, and 50%, respectively. The watermarked and JPEG compressed images are printed by HP Color LaserJet 2600n with a resolution of 300 dpi (dots per inch) first, then scanned with the resolution of 100ppi (pixels per inch) with random placement of the print on the flatbed of the HP ScanJet 8300 scanner. The scanner automatically adjusts the brightness, contrast, gamma correction, and all other settings. After scanning, we obtain the scanned images [Fig. 6(a)], which have good perceptual quality and are perceptually similar to the original, from the scanner automatically which are saved in a .Tiff format file. Each watermarked and JPEG compressed image is printed then scanned 10 times. Thus, for every test image and one JPEG QF, we obtained 100 samples. Table VII shows the success ratios of extracting 60-bit message without error from 100 samples. It is observed that with both of JPEG_100 and JPEG_80, the success ratio is 100%. With JPEG_50, the success ration is larger than 97% for "Lena," and is 100% for "Man," "Baboon," and "Peppers." If we replace the above color printer with a black-white (B/W) printer HP LaserJet 2015n [Fig. 6(b)], the results are shown in Table VIII. It shows that the proposed scheme with B/W printer HP LaserJet 2015n has similar robustness. In Table VIII, with JPEG_50, the success ratio is 75% for "Lena;" failure ratio is 25% which includes 21% decoding failure and 4% synchronization failure.

11) Surviving Combination Attack of Cropping and Print-Scan: The test image is cropped using Stirmark test function "cropping_x%" and is printed with HP LaserJet 2015n printer, then scanned with HP ScanJet 8300 scanner. The watermark is robust to the combination attack of cropping and print-scan. For example, it is robust to the combination attack of "cropping_50% +print-scan" and "cropping_40% +print-scan" for "Lena" and "Peppers," respectively (Fig. 7).

12) Robustness to Print-Scan With Inkjet Printer: Our scheme is theoretically device-independent; we will further use a few experiment results to support it. We substitute the laser printer with an Epson STYLUS R230 Inkjet printer. The other setting is similar to Item 9). For each of the "Lena," "Man," "Baboon," or "Peppers" image, we get 20 print-and-scan samples with two keys k_w and ten scanning for each key. The success ratio of message recover is 100% for all images.

13) Surviving Print-Scan With Developing Machine: We call this kind of print-scan developing-scanning. The developed prints from the developing machine have better image quality compared with the prints from the printer. But they have no halftoning characters which may be used to estimate and reverse rotation distortion [5]. The setting of the scanner is similar to the above. For each image, we get six print-and-scan samples with two watermark keys and three scanning for each key. The message can all be recovered.

14) Print-Scan Robustness Is Independent of the Scanner: In Items 10–12, the Gamma value for Gamma compensation with the scanner is chosen to be the default value 2.2. Now for the "Lena" image and HP Color LaserJet 2600n printer, we change

TABLE IX
COMPARISON WITH THE SCHEME IN [25]

	The proposed scheme	The scheme in [25]
the success rate of PS with JPEG QF 100	100%	0%
cropping_x%	x≥50	x≤25
time taken by watermark extraction	1s	29s

the Gamma value with the HP ScanJet 8300 scanner to be between 1.0 and 4.0 with step 0.2. The message can be recovered in all of these cases. We also substitute HP ScanJet 8300 scanner with HP ScanJet 4570c, HP ScanJet 3055. In all cases, we can correctly recover the message.

B. Psycho-Visual Quality Assessment and Comparison With the Recent Print-Scan Resilient Work

To better assess the perceptual quality of the watermarked images, we conducted the psycho-visual quality assessment test. The proposed scheme is used to embed a watermark into a set of 45 images. We can recover the hidden message without error from all of the watermarked images after printing and scanning. Thirty-two people were presented a slide show of the set of 45 original images. Then each person was given a different set of 45 images, about half of which contain hidden data and the others are original, and was asked to decide which is original and which is not. The false miss rate (the stego image is falsely judged as the original image) is 73.2%; the false alarm rate (the original image is falsely judged as a stego image) is 17.3%. The standard deviations for both false rates are 0.19 and 0.16, respectively. The total false rate is 90.5%. Both of the false miss rate and total false rate are higher than that of the print-and-scan resilient data hiding scheme in [5], which are 62.1% and 89.8%, respectively. This shows the excellent perceptual transparency.

The authors in [5] did an excellent work in addressing watermarking resisting scan-print though their algorithm has some limitations. It is assumed in [5] that the original image size is known in the detection and only mild cropping exists in the print-scan process, so the geometric distortion can be eliminated (except the mild cropped portion) when rotation is reversed and the image is rescaled to the original size. There are no such assumptions in our proposed scheme, so some geometric distortions such as mild aspect ratio change and cropping that occur in a practical print-scan process may not be eliminated. Even with this practical limitation, the proposed scheme achieves good performance in resisting the general print-scan, as elaborated below. 1) Our proposed data hiding scheme can be applied to different printers (including the developing machine), different scanners, and different Gamma compensations in the print-scan, thus significantly facilitating the print-scan watermark detection. The work in [5], as the authors noted, is only effective with a LaserJet printer. 2) Our scheme is robust to the general geometric distortion (e.g., if the image is geometric distorted digitally) and the combination attack with more severe cropping and print-scan. 3) To recover the hidden data, the scanner resolution can be chosen to be as low as 100 ppi in our scheme, while much higher resolution, say, 600 ppi should be chosen in [5] in order to correct the rotation distortion.

C. Comparison With Other Blind Geometric Distortion Resilient Schemes

We compared the proposed scheme with the discrete wavelet transform (DWT)-DFT composite watermarking scheme [25], [37] on the "Lena" image. For a fair comparison, the PSNR of the watermarked "Lena" is set to about 43.7 dB in both schemes. Both schemes have similar excellent robustness to JPEG compression and RST geometric distortion as mentioned above. But the proposed scheme achieves much better performance in terms of robustness against cropping and print-scan compared with the scheme in [25], and is much faster in watermark extraction. The comparison of the test results are shown in Table IX. The 60-bit message in [25] was not recovered from StirMark test function cropping_$x\%$ with $x > 25$, while the 60-bit message with the proposed scheme can be recovered from cropping_$x\%$ with $x \geq 50$. For print-scan using HP LaserJet 2600n Printer with JPEG quality factor 100, the success ratio of the proposed scheme is 100%, while the scheme in [25] always fails to recover the 60-bit message. The watermark extraction of the proposed scheme takes about 1 s on a computer with a 2.8-GHz Intel Pentium CPU using C language, while the scheme in [25] takes about 29 s.

We further compare the proposed scheme with the pioneering LPM-based watermarking scheme in [3]. The later embeds a watermark which is a vector of length 74. Based on ULPM, our scheme embeds a random sequence watermark message $\boldsymbol{m}_c$ of L_c-bit ($L_c = 72$), every watermark bit m_{ci} is further spread spectrum encoded with a N_p-bit ($N_p = 64$ here) bipolar PN-sequence $\boldsymbol{p}$. For a fair comparison, no error correction code is employed in our scheme in this experiment. We consider that watermark $\boldsymbol{m}_c$ exits if the bit-error rate between $\boldsymbol{m}_c$ and the extracted watermark is less than a constant threshold (t_0)

$$P_e = \frac{1}{L_c}\sum_{i=1}^{L_c}(m_{ci} \oplus m_{ci}^*) \leq t_0. \tag{12}$$

Under hypothesis H_0 in which watermark $\boldsymbol{m}_c$ is not embedded, it is reasonable to assume that it is a random sequence because $\boldsymbol{p}$ is a balanced sequence. Thus, we can calculate the corresponding probability of false positive rate as

$$f_p = \frac{1}{2^{L_c}}\sum_{k=L_c-e}^{L_c}\binom{L_c}{k} \tag{13}$$

where $e = \mathrm{round}(L_c \times t_0)$ denotes the number of error bits, $\mathrm{round}()$ means taking the nearest integer. The experimental results of true positive rate are collected on 5000 watermarked images from the same (Corel) image database as in [3], and the average signal-to-noise ratio of the watermarked image is set to the same 40 dB as in [3]. The receiver operating characteristic (ROC) curves prior to JPEG compression and after JPEG_70 compression are shown in Fig. 8. It can be seen that the proposed scheme achieve much better ROC performance in both the case of prior to and after the attack of JPEG_70. This significant improvement is attributed mainly to the proposed ULPM method.

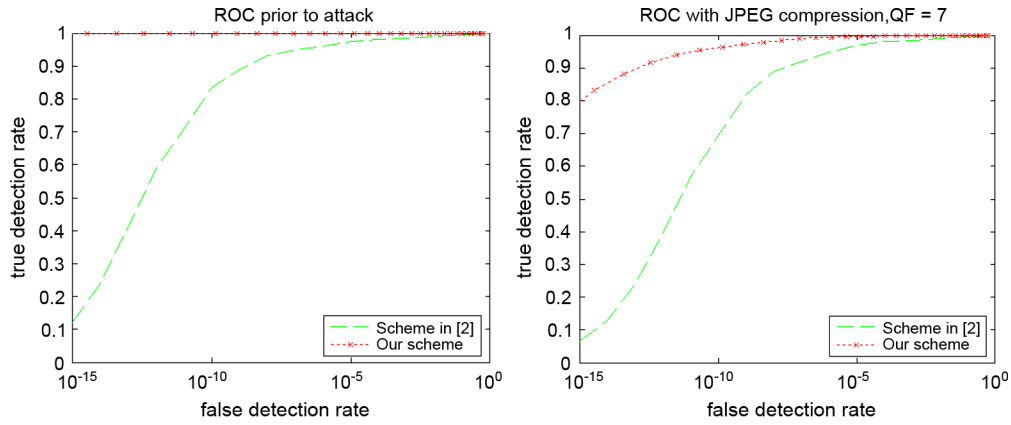


Fig. 8. ROC curve prior to attack and after JPEG_70. (a) ROC curve prior to attack; (b) ROC curve after JPEG_70. Results for Lin [3] are directly quoted from [3].

VI. Conclusions

A fast and robust watermarking scheme based on a ULPM was proposed in this paper. The contributions of this paper are summarized as follows.

1) We perform a near ULPM to the frequency index, as opposed to performing ILPM to the watermark signal or its index as done in previous works, in order to achieve the effect of embedding watermark in the Fourier LPM domain, but perform actual watermark embedding in the Cartesian Fourier domain. This approach not only completely eliminates the interpolation distortion and interference distortion introduced in embedding as observed in some previous works but also expands the embedding space significantly.
2) The proposed multibit watermarking scheme has excellent robustness. It is robust against RSTC distortion, general print-scan, and JPEG compression with low quality factor simultaneously. It is robust to scaling with the scaling factor being $0.6 \sim 2.0$, rotation by any degree, and the RSC combination attack.
3) Compared with other related watermarking schemes, our scheme provides significant improvement in terms of robustness against general print-scan, ROC performance, and efficiency of blind multibit watermark synchronization. The tracking pattern detection is key-dependent, so it is not detectable by a malicious party and cannot be easily removed by template removing attacks [32] because the energy of the tracking pattern is not distributed only on a small number of points.

The proposed ULPM can be exploited in pattern recognition, etc., to extract the geometric invariant feature, etc. These are part of future works

Acknowledgment

The authors would like to thank the anonymous reviewers and Associate Editor Dr. M. Wu for their very valuable comments and suggestions.

References

[1] 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.

[2] C. Y. Lin and S. F. Chang, "Distortion modeling and invariant extraction for digital image print-and-scan process," in *Proc. Int. Symp. Multimedia Information Processing*, Taipei, Taiwan, Dec. 1999.

[3] C. Y. Lin, M. Wu, J. Bloom, I. Cox, M. Miller, and Y. Lui, "Rotation, scale, and translation resilient watermarking for images," *IEEE Trans. Image Process.*, vol. 10, no. 5, pp. 767–782, May 2001.

[4] D. He and Q. Sun, "A practical print-scan resilient watermarking scheme," in *IEEE Int. Conf. Image Processing*, 2005, vol. 1, pp. 257–260.

[5] K. Solanki, U. Madhow, B. S. Manjunth, S. Chandrasekaran, and I. El-Khalil, "Print-scan' resilient data hiding in images," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 4, pp. 464–478, Dec. 2006.

[6] D. Zheng, J. Zhao, and A. E. Saddik, "RST-invariant digital image watermarking based on log-polar mapping and phase correlation," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 753–765, Aug. 2003.

[7] D. Zheng, Y. Liu, J. Zhao, and A. E. Saddik, "A survey of RST invariant image watermarking algorithms," *ACM Computing Surveys*, vol. 39, no. 2, Jun. 2007, Article 5.

[8] D. Zheng, Y. Liu, and J. Zhao, "A survey of RST invariant image watermarking algorithms," in *Proc. IEEE Canadian Conf. Electrical and Computer Engineering*, Ottawa, ON, Canada, May 7–10, 2006, pp. 2051–2054.

[9] J.-L. Dugelay and F. A. P. Petitcolas, "Possible counter-attackers against random geometric distortions," in *Proc. SPIE: Security and Watermarking of Multimedia Contents II*, CA, Jan. 2000, vol. 3971.

[10] G. W. Braudaway and F. Minter, "Automatic recovery of invisible image watermarks from geometrically distorted images," in *Proc. SPIE: Security and Watermarking of Multimedia Contents I*, CA, Jan. 2000, vol. 3971.

[11] X. Kang, J. Huang, and Y. Q. Shi, "An image watermarking algorithm robust to geometric distortion," in *Lecture Notes in Computer Science: Proc. Int. Workshop on Digital Watermarking*, Seoul, Korea, 2002, vol. 2613, pp. 212–223.

[12] Y. Liu, D. Zheng, and J. Zhao, "A rectification scheme for RST invariant image watermarking," *Special Section on Cryptography and Information Security, IEICE Trans. Fundamentals*, vol. E88-A, no. 1, pp. 314–318, 2005.

[13] V. Solachidis and I. Pitas, "Circularly symmetric watermark embedding in 2-D DFT domain," *IEEE Trans. Image Process.*, vol. 10, no. 11, pp. 1741–1753, Nov. 2001.

[14] J. O'Ruanaidh and T. Pun, "Rotation, scale, and translation invariant digital image watermarking," *Signal Process.*, vol. 66, no. 3, pp. 303–317, 1998.

[15] D. He and Q. Sun, "A RST resilient object-based video watermarking scheme," in *Proc. IEEE Int. Conf. Image Processing*, 2004, pp. 737–740.

[16] J.-L. Dugelay, S. Roche, C. Rey, and D. Doerr, "Still-image watermarking robust to local geometric distortions," *IEEE Trans. Image Process.*, vol. 15, no. 9, pp. 2831–2842, Sep. 2006.

[17] M. Alghoniemy and A. H. Tewfik, "Geometric invariance in image watermarking," *IEEE Trans. Image Process.*, vol. 13, no. 2, pp. 145–153, Feb. 2004.

[18] H. S. Kim and H.-K. Lee, "Invariant image watermark using Zernike moments," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 766–775, Aug. 2003.
[19] X. Kang, C. Liu, W. Zeng, and J. Huang, "Fast and automatic watermark resynchronization based on Zernike moments," in *Proc. SPIE, IS&T/SPIE 19th Ann. Symp.—Security, Steganography, and Watermarking of Multimedia Contents*, San Jose, CA, 2007, vol. 6505, pp. E1–E12.
[20] D. Simitopoulos, D. E. Koutsonanos, and M. G. Strintzis, "Image watermarking resistant to geometric attacks using generalized Radon transformations," in *Proc. Digital Signal Processing*, 2002, vol. 1, pp. 85–88.
[21] H. Kim and B. V. K. Vijaya Kumar, "Rotation tolerant watermark detection using circular harmonic function correlation filter," in *Lecture Notes in Computer Science: Proc. Int. Workshop on Digital Watermarking*, 2004, vol. 2939, pp. 263–276.
[22] H. Kim, Y. Baek, and H. K. Lee, "Rotation, scale and translation invariant image watermark using higher order spectra," *Opt. Eng.*, vol. 42, no. 2, pp. 340–349, 2003.
[23] A. Herrigel, J. J. K. O'Ruanaindh, H. Petersen, S. Pereira, and T. Pun, "Secure copyright protection techniques for digital images," in *Proc. Int. Workshop on Information Hiding*, 1998, vol. 1525, pp. 169–190, Lecture Notes in Computer Science.
[24] S. Pereia and T. Pun, "Robust template matching for affine resistant image watermarks," *IEEE Trans. Image Process.*, vol. 9, no. 6, pp. 1123–1129, Jun. 2000.
[25] X. Kang, J. Huang, Y. Q. Shi, and Y. Lin, "A DWT-DFT composite watermarking scheme robust to affine transform and JPEG compression," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 776–786, Aug. 2003.
[26] M. Kutter, "Watermarking resistant to translation, rotation and scaling," in *Proc. SPIE, Int. Symp. Multimedia Systems and Applications*, 1998, vol. 3528, pp. 423–431.
[27] S. Voloshynovskiy, F. Deguillaume, and T. Pun, "Multibit digital watermarking robust against local nonlinear geometrical distortions," in *Proc. IEEE Int. Conf. Image Processing*, Thessaloniki, Greece, 2001, vol. 3, pp. 999–1002.
[28] S. Voloshynovskiy, F. Deguillaume, and T. Pun, "Content adaptive watermarking based on a stochastic multiresolution image modeling," in *Proc. 10th Eur. Signal Processing Conf.*, Tampere, Finland, Sep. 2000.
[29] S. Voloshynovskiy, F. Deguillaume, and T. Pun, "Multibit digital watermarking robust against local nonlinear geometrical distortions," in *Proc. IEEE Int. Conf. Image Processing*, Thessaloniki, Greece, 2001, vol. 3, pp. 999–1002.
[30] C.-S. Lu, S.-W. Sun, C.-Y. Hsu, and P.-C. Chang, "Media hash-dependent image watermarking resilient against both geometric attacks and estimation attacks based on false positive-oriented detection," *IEEE Trans. Multimedia*, vol. 8, no. 4, pp. 668–685, Aug. 2004.
[31] P. Bas, J. M. Chassery, and B. Macq, "Geometrically invariant watermarking using feature points," *IEEE Trans. Image Process.*, vol. 11, no. 9, pp. 1014–1028, Sep. 2002.
[32] A. Herrigel, S. Voloshynovskiy, and Y. Rytsa, "The watermark template attack," in *Proc. SPIE, Security, Steganography, and Watermarking of Multimedia Contents*, San Jose, CA, 2001.
[33] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, 2nd ed. Englewood Cliffs, NJ: Prentice-Hall, 2002, pp. 200–210.
[34] L. G. Brown, "A survey of image registration technique," *ACM Computing Surveys*, vol. 24, no. 4, pp. 325–376, 1992.
[35] B. S. Reddy and B. N. Chatterji, "A FFT-based technique for translation, rotation, and scale-invariant image registration," *IEEE Trans. Image Process.*, vol. 5, no. 8, pp. 1266–1271, Aug. 1996.
[36] Y. Liu and J. Zhao, "A new filtering method for RST invariant image watermarking," in *Proc. IEEE Int. Workshop on Haptic. Audio and Visual Environments and their Applications*, Sep. 2003, pp. 101–106.
[37] X. Kang, J. Huang, and W. Zeng, "Improving robustness of quantization-based image watermarking via adaptive receiver," *IEEE Trans. Multimedia*, vol. 10, no. 6, pp. 953–959, Oct. 2008.

Xiangui Kang (M'00) received the B.S., M.S., and Ph.D. degrees from Peking University, in 1990, Nanjing University in 1993, and Sun Yat-Sen University, China, in 2004, respectively.

He is currently an associate professor with the School of Information Science and Technology, Sun Yat-Sen University, Guangzhou, China. His research interests include watermarking, multimedia communications, and security.

Dr. Kang is a member of the IEEE ComSoc's Multimedia Communications Technical Committee.

Jiwu Huang (M'97–SM'00) received the B.S. degree from Xidian University, China, in 1982, the M.S. degree from Tsinghua University, China, in 1987, and the Ph.D. degree from Institute of Automation, Chinese Academy of Science, in 1998.

He is currently a Professor with the School of Information Science and Technology, Sun Yat-Sen University, Guangzhou, China. His current research interests include multimedia forensics and security.

Dr. Huang has served as a Technical Program Committee member for many international conferences. He serves as a member of IEEE CAS Society Technical Committee of Multimedia Systems and Applications and the chair of IEEE CAS Society Guangzhou chapter. He is an associate editor of the *EURASIP Journal of Information Security*.

Wenjun Zeng (S'94–M'97–SM'03) received the B.E., M.S., and Ph.D. degrees from Tsinghua University, China, in 1990, the University of Notre Dame in 1993, and Princeton University in 1997, respectively, all in electrical engineering.

He is an Associate Professor with the Computer Science Department, University of Missouri, Columbia, MO. Prior to joining Univ. of Missouri in 2003, he had worked for PacketVideo Corp., Sharp Labs of America, Bell Labs, and Matsushita Info. Tech. Lab of Panasonic Tech. He has also consulted with Microsoft Research, Huawei Technologies, and a couple of start-up companies. From 1998 to 2002, he was an active contributor to the MPEG4 Intellectual Property Management and Protection standard and the JPEG 2000 image coding standard, where four of his proposals were adopted. His current research interests include multimedia communications and networking, distributed source and video coding, and content and network security.

Dr. Zeng is an Associate Editor of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, and of *IEEE Multimedia Magazine*, and is on the Steering Committee of IEEE TRANSACTIONS ON MULTIMEDIA, of which he also served as an Associate Editor from 2005 to 2008. He is serving as the Steering Committee Chair of the IEEE International Conference Multimedia and Expo (ICME), and has served as the TPC Vice Chair of ICME 2009, the TPC Chair of the 2007 IEEE Consumer Communications and Networking Conference, the TPC Co-Chair of the Multimedia Communication and Home Networking Symposium of the 2005 IEEE International Conference Communications. He was a Guest Editor of the SPECIAL ISSUE ON RECENT ADVANCES IN DISTRIBUTED MULTIMEDIA COMMUNICATIONS, PROCEEDINGS OF THE IEEE published in January 2008 and the Lead Guest Editor of SPECIAL ISSUE ON STREAMING MEDIA, IEEE TRANSACTIONS ON MULTIMEDIA published in April 2004