

Contourlet-Based Image Watermarking Using Optimum Detector in a Noisy Environment

Mohammad Ali Akhaee, *Member, IEEE*, S. Mohammad Ebrahim Sahraeian, *Student Member, IEEE*, and Farokh Marvasti, *Senior Member, IEEE*

Abstract—In this paper, an improved multiplicative image watermarking system is presented. Since human visual system is less sensitive to the image edges, watermarking is applied in the contourlet domain, which represents image edges sparsely. In the presented scheme, watermark data is embedded in directional subband with the highest energy. By modeling the contourlet coefficients with General Gaussian Distribution (GGD), the distribution of watermarked noisy coefficients is analytically calculated. The tradeoff between the transparency and robustness of the watermark data is solved in a novel fashion. At the receiver, based on the Maximum Likelihood (ML) decision rule, an optimal detector by the aid of channel side information is proposed. In the next step, a blind extension of the suggested algorithm is presented using the patchwork idea. Experimental results confirm the superiority of the proposed method against common attacks, such as Additive White Gaussian Noise (AWGN), JPEG compression, and rotation attacks, in comparison with the recently proposed techniques.

Index Terms—Contourlet transform, maximum likelihood detector, multiplicative image watermarking.

I. INTRODUCTION

DIGITAL watermarking is progressively applied for several purposes such as broadcast monitoring, data authentication, data indexing, and secret communication systems [1]–[3]. A digital watermark must have special features to guarantee desired functionalities. Perceptual transparency, data rate, and robustness against attacks are three major requirements of any watermarking system. There is a trade-off among these requirements which has been investigated in [4] and [5] from an information-theoretic perspective. However, depending on the application, the importance of these features varies. For example, for secret communication systems, the robustness against noise and data rate is the most important feature, while

for data authentication, imperceptibility and robustness against different processing attacks are the most significant ones.

The increase of the power of watermark causes more resistance against attacks. This point leads designers to choose the energy of the watermark to be dependent on the still image powers. In the attempt to match the characteristics of the watermark to those of the image features, larger image information contents bear greater watermark. In other words, the power of the watermark is proportional to the corresponding image feature samples. The simplest way to implement this principle is by means of multiplicative watermarking. In order to employ the Human Visual System (HVS) properties, multiplicative watermarking is often used in the transform domain. The transforms usually selected for digital watermarking are Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT) [6]–[9], which concentrate the energy of the host signal in a fewer components. It has been proven that the kernel of DWT is well suited for representing one-dimensional discontinuities. However, when the dimension increases, wavelets fails to represent singularities.

The limited capability of wavelet transform in capturing directional information in two dimensions, resulted in introducing many directional image representations in recent years which can capture the intrinsic geometrical structures in natural images such as smooth curves and contours. Some examples include the steerable pyramid [10], brushlets [11], complex wavelets [12], dual tree complex wavelets [13], directional wavelet frames [14], wave atoms [15], bandlets [16], ridgelets [17], curvelets [18], and contourlets [19], [20].

Curvelet transform is defined to represent two dimensional discontinuities more efficiently, with less error in a fixed term approximation [18]. However, since curvelet transform has been introduced in continuous domain, it does not have acceptable performance in critical discrete applications. As an improvement on the curvelet transform, Contourlet Transform (CT) is proposed by Do *et al.* [19] using Pyramidal Directional Filter Bank (PDFB). The main advantage of contourlet transform over other directional representations is that it allows different number of directions at each scale while achieving nearly critical sampling [19]. Besides, it employs iterated filter banks, which makes it computationally efficient. By utilizing the performance of the contourlet transform in capturing directional information of image edges, some watermarking algorithms have been proposed so far [21]–[25]. In [21]–[23], the additive watermarking methods are proposed, while references [24] and [25] investigate the multiplicative watermarking approaches.

Manuscript received December 14, 2008; revised November 02, 2009. First published December 18, 2009; current version published March 17, 2010. A preliminary version of this work was presented in part at the IEEE International Conference on Image Processing 2008. This work is supported by the National Research Institute for Science Policy. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. James E. Fowler.

M. A. Akhaee and F. Marvasti are with the Advanced Communication Research Institute (ACRI), Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran, 14588-89694 (e-mail: akhaee@ee.sharif.edu; marvasti@sharif.edu).

S. M. E. Sahraeian was with the Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran, 14588-89694. He is now with the Genomic Signal Processing (GSP) Lab, Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843 USA (e-mail: msahraeian@tamu.edu).

Digital Object Identifier 10.1109/TIP.2009.2038774

Different approaches have been used for implementing multiplicative watermarking schemes. In [3] and [26], a correlation detector has been used for this purpose. However, since correlation detection is suboptimal for multiplicative watermarking in a transform domain, several alternative optimum and sub-optimum decoders have been proposed [27]–[31]. In [27], a robust optimum detector for the multiplicative rule $y_i = x_i(1 + \alpha_i w_i)$ in the DCT, DWT and DFT domains is proposed. The distribution of high frequency coefficients of DCT and DWT are assumed to be Generalized Gaussian (GG) while the magnitude of DFT coefficients are modeled by Weibull distribution. Solachidis *et al.* [32] has calculated the distribution of DFT coefficients analytically and has shown that it is not exactly Weibull. They have designed an optimum detector for multiplicative watermarks in the DFT domain of nonwhite signals. In [31], the locally optimum detector for Barni's [28], [29] multiplicative watermarking scheme using HVS in the wavelet transform domain has been proposed. Li *et al.* have proposed an ML detector for multiplicative watermarking in the contourlet transform domain [24]. They have assumed that the distribution of the received coefficients is GG, and hence their receiver is sub-optimum for noise free environments.

In this paper, in order to achieve higher robustness against AWGN and JPEG compression attacks, the multiplicative watermarking approach in the contourlet transform domain is used. We introduce a new multiplicative watermarking scheme to match the watermark message to the contourlet coefficients in an optimum way. The contourlet coefficients are multiplied by two special functions depending on the value of the watermark bits. These functions are optimized for the highest robustness against AWGN and JPEG attack. For data extraction, similar to [8], [33], the ML detector has been used utilizing GGD property of the contourlet coefficients. To this aim, the density function of the noisy contourlet coefficients is analytically computed. In order to decrease the complexity of the receiver, the distribution of these coefficients is approximated with a suitable function. Under this estimation, the optimum threshold of the proposed multiplicative watermarking method is evaluated. We also extend the proposed method to a blind technique which does not need side information.

The rest of the paper is organized as follows. In Section II, a brief introduction of contourlet transform is given. The statistical modeling of the proposed watermarking scheme is presented in Section III. In Section IV, the proposed multiplicative watermarking method based on the contourlet transform is introduced. In the same section, the optimum threshold in the ML detector is analytically investigated. The multi-objective optimization approach to find the best value for the strength factor is elaborated in Section V. Section VI contains simulation results about the robustness of the proposed approach against common attacks and the comparison of its performance over other watermarking techniques. Finally, Section VII concludes the paper.

II. CONTOURLETS

For piecewise continuous 1-D signals, wavelets have been established as a right tool in generating efficient representation. However, natural images are not simply stacks of 1-D piecewise smooth scan-lines, but they have many discontinuity points

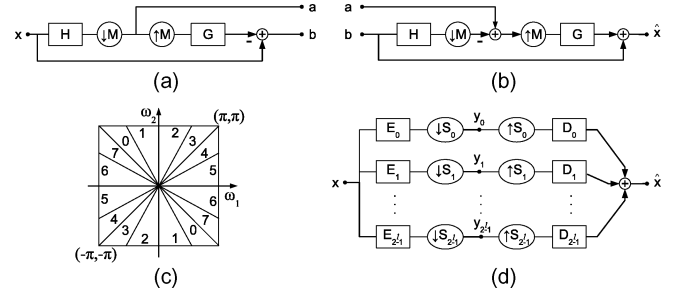


Fig. 1. (a), (b) Laplacian pyramid one level of decomposition and reconstruction; (c), (d) directional filter bank frequency partitioning and the multichannel view of tree-structured directional filter bank.

along smooth curves and contours. Thus, separable wavelets cannot capture directional information in two dimensions. To overcome this shortcoming, many directional image representations have been proposed in recent years [10]–[20].

Implementing the idea of combining subband decomposition with a directional transform, Do and Vetterli [19] introduced a multidirectional and multiscale transform known as the contourlet transform, which consists of two major stages: the subband decomposition and the directional transform. Laplacian Pyramid (LP) [34] filters are used as the first stage and Directional Filter Banks (DFB) [35] as the second stage.

First, for the multiscale decomposition it uses Laplacian Pyramid (LP) filters. The LP decomposition at each level generates a downsampled lowpass version of the original and the difference between the original and the prediction, resulting in a bandpass image. Fig. 1(a) and (b) depicts the decomposition and reconstruction processes as suggested in [36], where H and G are orthogonal analysis (lowpass) and synthesis filters, respectively, and M is the sampling matrix. The process can be iterated on the coarse (downsampled lowpass) signal.

The directional decomposition stage is also constructed based on the idea of using an appropriate combination of shearing operators together with two-direction partition of quincunx filter banks at each node in a binary tree-structured filter bank, to obtain the desired 2-D spectrum division as shown in Fig. 1(c). As discussed in [19], it is instructive to view an l level tree-structured DFB equivalently as a 2^l parallel channel filter bank with equivalent filters and overall sampling matrices as shown in Fig. 1(d), where the equivalent (directional) synthesis filters are represented by $D_k^{(l)}$, $0 \leq k < 2^l$. The corresponding overall sampling matrices were shown in [19] to have the following diagonal forms:

$$S_k^{(l)} = \begin{cases} \text{diag}(2^{l-1}, 2), & \text{for } 0 \leq k < 2^{l-1} \\ \text{diag}(2, 2^{l-1}), & \text{for } 2^{l-1} \leq k < 2^l. \end{cases} \quad (1)$$

This basis exhibits both directional and localization properties.

Combining the Laplacian pyramid and the directional filter bank into a double filter bank structure the contourlet transform is developed. Fig. 2(a) shows the decomposition used in the contourlet filter bank. Bandpass images from the LP are fed into a DFB to capture the directional information. By iterating this scheme on the coarse image, the image decomposes into directional subbands at multiple scales. This cascade structure helps the user to decompose different scales into different directions. An example of frequency partition of the contourlet transform

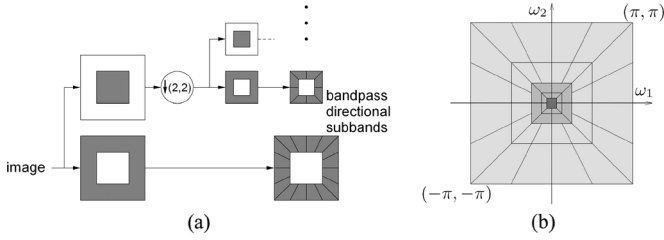


Fig. 2. (a) Contourlet filter bank: Laplacian pyramid as the first stage and directional filter bank as the second stage. (b) Example of frequency partition by the contourlet transform [19].

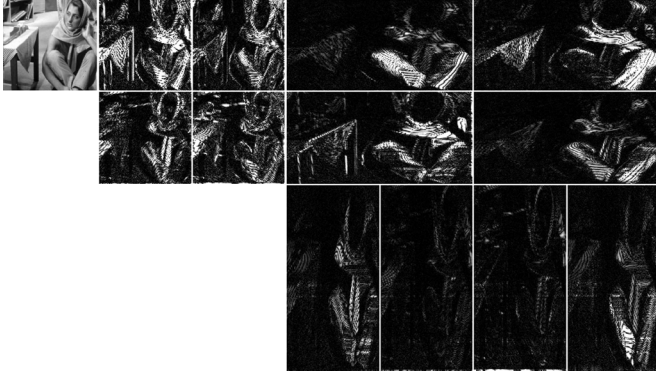


Fig. 3. Contourlet transform of the *Barbara* image. The image is decomposed into two pyramidal levels, which are then decomposed into four and eight directional subbands. Small coefficients are shown by black while large coefficients are shown by white [19].

is shown in Fig. 2(b). This type of frequency partitioning leads to the sparsity of the contourlet coefficients, i.e., only the coefficients with both direction and location on the original image edges has significant values. This can be clearly seen in Fig. 3, where the contourlet transform sub-bands of the *Barbara* image is shown.

III. STATISTICAL MODELING

As discussed in [20], the contourlet coefficients are highly non-Gaussian. As an example, the histograms of two finest contourlet subbands of the image *Barbara* are shown in Fig. 4. The peaks near the mean decline rapidly unlike the Gaussian distribution. As a criterion, consider the kurtosis which is defined as

$$k_x = \frac{1}{(\sigma_x^4)} \frac{1}{N} \sum_{i=1}^N x_i^4 \quad (2)$$

where x is a zero-mean random variable with the standard deviation of σ_x . For the Gaussian distribution, the kurtosis is 3. As shown in Fig. 4, the kurtosis of the two finest contourlet subbands of *Barbara* image are 26.95 and 19.58, respectively, which are much higher than 3.

However, as studied in [37], the contourlet coefficients are well modeled by i.i.d. random variables with Generalized Gaussian Distribution (GGD)

$$GG_{\sigma_x, \beta}(x) = C(\sigma_x, \beta) e^{-[\alpha(\sigma_x, \beta)|x|]^\beta} \quad -\infty < x < \infty, \sigma_x > 0, \beta > 0 \quad (3)$$

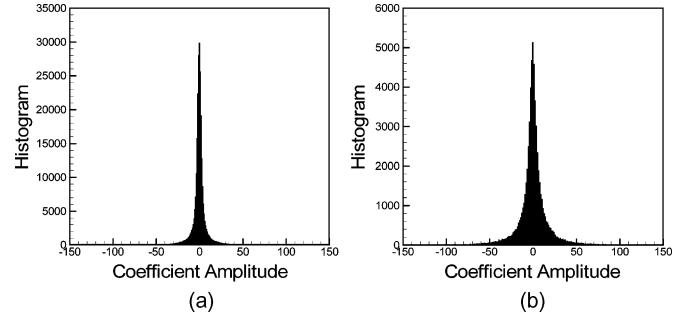


Fig. 4. Histogram of two finest contourlet subbands of the image *Barbara*. The kurtosis of the two distributions are measured at (a) 26.95 and (b) 19.58, showing that the coefficients are highly non-Gaussian.

where $\alpha(\sigma_x, \beta) = \sigma_x^{-1} [\Gamma(3/\beta)/\Gamma(1/\beta)]^{1/2}$, $C(\sigma_x, \beta) = \beta \alpha(\sigma_x, \beta) / 2\Gamma(1/\beta)$, σ_x is the standard deviation of x , β is the shape parameter, and $\Gamma(t) = \int_0^\infty e^{-u} u^{t-1} du$ is the Gamma function. Special cases of the GGD density function include the Gaussian distribution with ($\beta = 2$), and the Laplacian with ($\beta = 1$).

In our watermarking approach, as will be used in the next section, the contourlet coefficient x is multiplied by an even monotonic (for $x > 0$) strength function $f(x)$. Thus, if we show the watermarked coefficients by w , we have $w(x) = xf(x)$. $f(x)$ is selected such that $w(x)$ is still monotonic for all x . According to [38], for a monotonic function $y = g(x)$ we have

$$P_y(y) = \frac{P_x(g^{-1}(y))}{|g'(g^{-1}(y))|} \quad (4)$$

where P_y and P_x are the density functions of the random variables y and x , respectively. Therefore, the distribution of $w(x)$ can be defined as

$$P(w) = \frac{P(x)}{xf'(x) + f(x)}. \quad (5)$$

At the receiver, we receive the coefficients contaminated by noise or other kinds of attacks. We assume that the attack noise is zero mean AWGN with the distribution of $\mathcal{N}(0, \sigma_n^2)$. Therefore, the received coefficients are $y = w + n$. Since the contourlet coefficients are considered to be independent of the noise term, we have $P(y) = P(w) * P(n)$, where $*$ is the convolution operator. Then, considering the contourlet coefficients to be GGD, we have

$$P(y) = \int_{-\infty}^{\infty} \frac{C e^{-[\alpha|g(z)|]^\beta}}{g(z)f'(g(z)) + f(g(z))} \cdot \frac{1}{\sqrt{2\pi\sigma_n^2}} e^{-\frac{(y-z)^2}{2\sigma_n^2}} dz \quad (6)$$

where $g(x)$ is the inverse function of the $w = xf(x)$; that is, $g(w) = x$.

To find a closed form answer for $P(y)$, we estimate the Gaussian function, i.e.,

$$\Lambda_G(x) = \begin{cases} \frac{-x+3\sigma_n}{9\sigma_n^2}, & 0 < x \leq 3\sigma_n \\ \frac{x+3\sigma_n}{9\sigma_n^2}, & -3\sigma_n \leq x < 0 \\ 0, & |x| > 3\sigma_n. \end{cases} \quad (7)$$

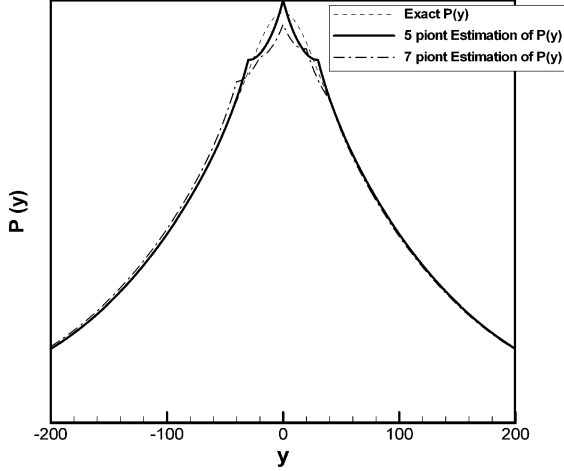


Fig. 5. Distribution function of the noisy watermarked contourlet signal, $P(y)$ (6), compared with the five point (8) and seven point estimations (11).

Then, substituting this function in (6), and using the trapezoidal rule, we can compute the integral as

$$P(y) \simeq \frac{3\sigma_n}{2} \left[\frac{K(y + \frac{3\sigma_n}{2})\Lambda_G(-\frac{3\sigma_n}{2}) + K(y + 3\sigma_n)\Lambda_G(-3\sigma_n)}{2} + \frac{K(y)\Lambda_G(0) + K(y + \frac{3\sigma_n}{2})\Lambda_G(-\frac{3\sigma_n}{2})}{2} + \frac{K(y)\Lambda_G(0) + K(y - \frac{3\sigma_n}{2})\Lambda_G(\frac{3\sigma_n}{2})}{2} + \frac{K(y - \frac{3\sigma_n}{2})\Lambda_G(\frac{3\sigma_n}{2}) + K(y - 3\sigma_n)\Lambda_G(3\sigma_n)}{2} \right] \quad (8)$$

where

$$K(y) = \frac{C e^{-[\alpha|g(y)]^\beta}}{g(y)f'(g(y)) + f(g(y))}. \quad (9)$$

Then, after some manipulations, (8) is converted to

$$P(y) \simeq \frac{1}{2} \left[\frac{K(y - \frac{3\sigma_n}{2})}{2} + K(y) + \frac{K(y + \frac{3\sigma_n}{2})}{2} \right]. \quad (10)$$

If we use the trapezoidal rule with seven points, instead of five points as used in (8), in the calculation of (6), $P(y)$ can be estimated as

$$P(y) \simeq \frac{1}{9} [K(y - 2\sigma_n) + 2K(y - \sigma_n) + 3K(y) + 2K(y + \sigma_n) + K(y + 2\sigma_n)]. \quad (11)$$

To verify the accuracy of the estimation used in calculation of $P(y)$ in (10) and (11), we have simulated these two estimations along with (6) in Fig. 5 for an example case of $\beta = 1.2$, $\sigma_x = 50$, and $\sigma_n = 20$. As we can see, the estimations are both well matched with the exact density function. However, as (10) provides less computational complexity, we use this estimation for further calculations.

IV. PROPOSED METHOD

A. Watermark Embedding

Imperceptibility of the watermarking algorithm is commonly achieved by exploiting the weaknesses of the HVS. As demonstrated in HVS, the human eye is less sensitive to high entropy blocks instead of smooth ones as there are usually stronger edges in the high entropy blocks. For this purpose, we select N blocks with the highest entropy in the whole image for the watermarking purpose. We then apply the contourlet transform to each selected block. Calculating the energy of the coefficients in each directional subband of the finest scale, we choose the directional subband with the highest energy for embedding purpose. This way, we hide the code in the most significant direction of each block.

We embed data in these coefficients using a multiplicative based approach. In the multiplicative watermarking, we look for samples with large values. Thus, we should apply transforms that concentrate the energy of the image in a few coefficients. As discussed in Section II, wavelet transform fails in representing 2-D discontinuities occur in image edges. As a result, using the multiresolution nonseparable filter bank structures such as contourlets yields sparser coefficients, i.e., it represents the edges in a few samples. Therefore, in the proposed method, we insert the watermark in the edges of the most energetic contourlet subband of high entropy blocks which are the right places to be visually acceptable to HVS.

We embed a single bit of “0” or “1” in each block by manipulating the coefficients x_i in the most energetic directional subband based on the following strategy [39]:

$$w_i = \begin{cases} x_i \cdot f_1(x_i), & \text{for embedding 1} \\ x_i \cdot f_0(x_i), & \text{for embedding 0} \end{cases} \quad (12)$$

where $f_1(x)$ and $f_0(x)$ are strength functions.

With the same inference that the most energetic directional subband relates to the dominant direction of the block, we can say that the large coefficients in that subband are relates to the strong edges in the block and we can embed more data in these coefficients. This verifies that the strength function $f_1(x)$ must be an increasing function for $x > 0$. Although a linear function may be a straightforward choice in this case, we found that the rate of increasing should not be linear because we have much higher capacity in larger coefficients and with linear function we either may miss this capacity or may cause visible distortions in the image because of high changes in small coefficients. Thus, we need a nonlinear increasing function. Exponential function is a good choice which gives us a large change in larger coefficients and small changes in smaller coefficients.

Considering these facts, we suggest the strength functions to be even and monotonically exponential functions, i.e.,

$$f_1(x) = a_1 e^{a_2|x|} + a_3 \quad (13)$$

$$f_0(x) = b_1 e^{b_2|x|} + b_3. \quad (14)$$

To define the parameters used in these functions we use the following reasoning.

- a_2 : This parameter has an important role in the rising rate of strength function. In our experiments, we found that

considering the amplitude of contourlet coefficients, $a_2 = -0.05$ gives us a suitable rate for the exponential function because we now that the exponential function vanishes to 95% after three time constants, which is at $x = 3/0.05 = 60$ in our case. Thus, the strength function reaches its final value after $x = 60$, which is a good point for us as for many directional subbands the maximum amplitude of coefficients occurs near this value.

- a_1 : For small coefficients we have $f_1(x) \simeq a_1 + a_3$. This is the minimum strength we use for embedding. We fixed this value to 1.3. As we see in our experiments that this minimum strength is enduring in most of the energetic subbands and preserves the transparency.
- b_1, b_2, b_3 : Our reasoning to define the parameter in $f_0(x)$ is to make this function to show the behaviour of $1/f_1(x)$ for large x values. This way, we increase the host coefficients for “1” embedding and decrease them for “0” embedding. Thus, considering the fact that for large x values, the exponential term is small in compare with a_3 , we can approximate this function as

$$\frac{1}{f_1(x)} = \frac{1}{a_1 e^{a_2|x|} + a_3} \simeq \frac{1}{a_3} - \frac{a_1}{a_3^2} e^{a_2|x|}.$$

Thus, we have, $b_1 = -(a_1/a_3^2)$, $b_2 = a_2$, $b_3 = 1/a_3$.

- a_3 : This parameter determines the values of $f_1(x)$ and $f_0(x)$ functions for larger coefficients, when the exponential function is vanished. We decided to find this parameter dependent to the image as in some images we may be able to apply more or less strength in large coefficients while preserving transparency. Thus, using an optimization algorithm, as shown in Section V, we determine this parameter.

In summary, we relate the parameters in $f_1(x)$ and $f_0(x)$ to each other through

$$\begin{aligned} a_1 &= 1.3 - a_3 & b_1 &= -\frac{a_1}{a_3^2} \\ b_2 &= a_2 = -0.05 & b_3 &= \frac{1}{a_3}. \end{aligned} \quad (15)$$

In addition, we restrict a_3 to be larger than 1.3.

We can see that a_3 is the only degree of freedom for defining $f_1(x)$ and $f_0(x)$. As shown in Fig. 6 for different values of a_3 , $f_1(x)$ has an exponentially ascending trend for $x > 0$ and is larger than unity. On the other hand, $f_0(x)$ has an exponentially descending trend for $x > 0$ and is smaller than unity. These functions are selected exponentially in order that larger coefficients change more than smaller ones during the watermarking process since the larger coefficients are related to the strong edges in the supposed directional subband.

Moreover, as mentioned in Section III, these functions must be defined such that $xf(x)$ is monotonic. As shown in Fig. 6, $f_1(x)$ is a monotonically ascending function for $x > 0$; thus, $xf_1(x)$ is also monotonically ascending for all xs . However, as $f_0(x)$ is a monotonically descending function for $x > 0$, the monotonicity of $xf_0(x)$ must be investigated.

If we write $w(x) = xf_0(x)$ in terms of a_3 parameter for $x > 0$, we have

$$w(x, a_3) = xf_0(x) = \frac{x}{a_3} \left[(a_3 - 1.3)e^{-\frac{x}{20}} + 1 \right]. \quad (16)$$

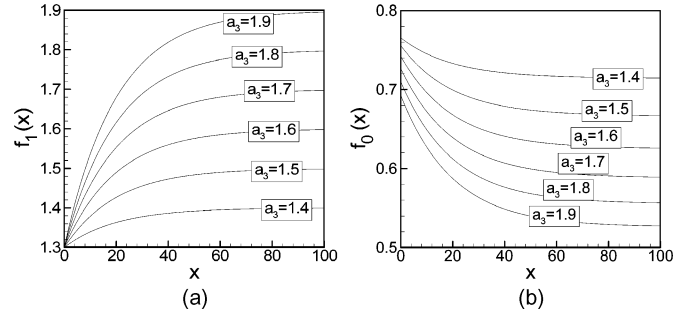


Fig. 6. Strength functions (a) $f_1(x)$ and (b) $f_0(x)$ for different values of a_3 .

Calculating the derivative of $w(x, a_3)$ with respect to x , we have

$$y(x, a_3) = \frac{\partial w(x, a_3)}{\partial x} = \frac{1}{a_3} \left[(a_3 - 1.3) \left(1 - \frac{x}{20} \right) e^{-\frac{x}{20}} + 1 \right]. \quad (17)$$

If we let $z = 1 - (x/20)$ and $c = a_3 - 1.3$, (17) can be rewritten as

$$y(z, c) = cz e^{z-1} + 1. \quad (18)$$

Since $a_3 > 1.3$ and $x > 0$, we have $c > 0$ and $z < 1$. Calculating the derivative of $y(z, c)$ with respect to z , we have

$$\frac{\partial y(z, c)}{\partial z} = c(z + 1)e^{z-1}. \quad (19)$$

This function is negative for $z < -1$ and positive for $z > -1$. Thus, $y(z, c)$ is minimum at $z = -1$ with the value of $1 - ce^{-2}$, which is positive for $c < e^2 = 7.39$. In other words, for $a_3 < 8.69$, $y(z, c)$ is positive and as a consequence, $w(x, a_3) = xf_0(x)$ is monotonically ascending for all xs . Since the practical range of a_3 is between 1.3 and 2, we are sufficiently far from the maximum acceptable value of $a_3 = 8.69$. Therefore, the proposed functions in (13) and (14) satisfy the monotonicity of $xf(x)$, and, thus, they are invertible as required in Section III.

Applying the inverse contourlet transform, we reconstruct the watermarked block. Repositioning each block in its position in the image, we create the watermarked image. The block positions and the GGD parameters (σ_x and β) should be sent along with the watermarked image. The block diagram of the proposed watermarking method is shown in Fig. 7(a).

B. Watermark Detection

For detecting the watermark data in each block, we suggest a detection scheme based on an optimum detector. Fig. 7(b) shows the block diagram of the proposed detector.

Suppose that x_i represents the contourlet coefficients of the most energetic directional subband of a specific block. We assume these coefficients to be independently and identically distributed (i.i.d.) as $GG(\sigma, \beta)$. Besides, we approximate the distribution of the watermarked coefficients attacked by AWGN from (10).

In order to have ML decision, we must have

$$P(y_1, y_2, \dots, y_m | 1) \geq_0^1 P(y_1, y_2, \dots, y_m | 0) \quad (20)$$

where the left term is the distribution of the coefficients in a specific block with m coefficients for “1” embedding and the right

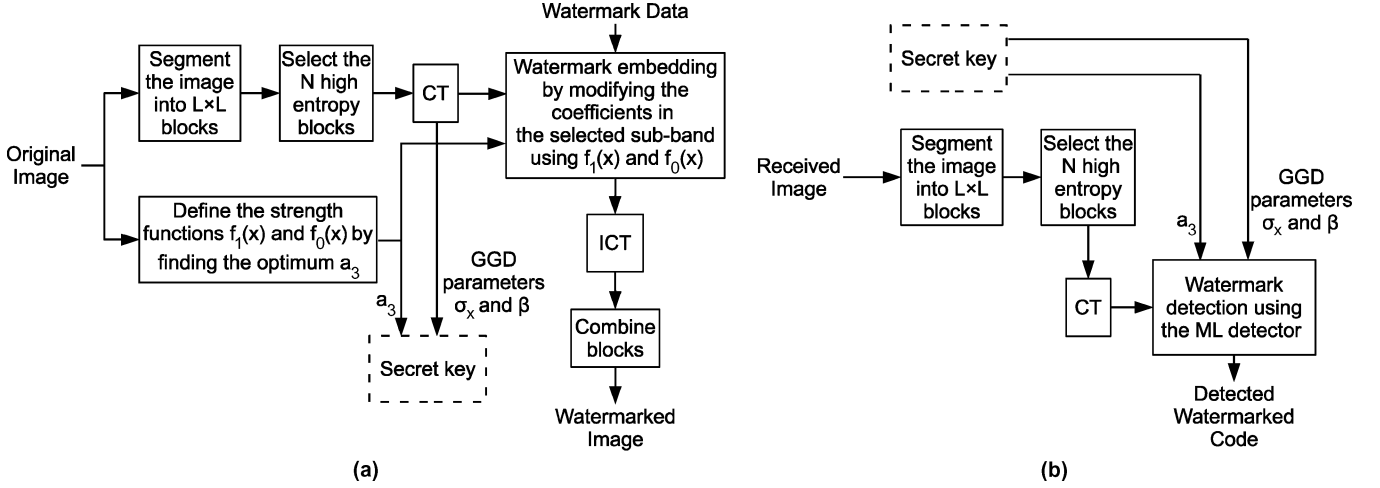


Fig. 7. Block diagram of the proposed watermarking scheme: (a) embedding; (b) detecting.

term is the same distribution for “0” embedding. By considering the i.i.d. distribution of the contourlet coefficients, these distributions are defined as

$$\begin{aligned}
 P(y_1, \dots, y_m | 1) &= \prod_{i=1}^m \frac{K_1(y_i - \frac{3\sigma_n}{2}) + 2K_1(y_i) + K_1(y_i + \frac{3\sigma_n}{2})}{4} \\
 P(y_1, \dots, y_m | 0) &= \prod_{i=1}^m \frac{K_0(y_i - \frac{3\sigma_n}{2}) + 2K_0(y_i) + K_0(y_i + \frac{3\sigma_n}{2})}{4} \quad (21)
 \end{aligned}$$

where $K_1(y)$ and $K_0(y)$ are computed from (9) using the strength functions $f_1(x)$ and $f_0(x)$, respectively.

Inserting (21) in (20), we can find the watermarked bit using the optimum detector.

As we can see, the best decision depends on the noise standard deviation in the watermarked directional subband, σ_n . To estimate this parameter, we can use a Monte-Carlo method as suggested in [37].

For the noise free environment, (20) and (21) can be simplified as

$$\sum_{i=1}^N \left[(\alpha |g_0(y_i)|)^\beta - (\alpha |g_1(y_i)|)^\beta \right] \geq \frac{1}{2} T \quad (22)$$

where

$$T = \sum_{i=1}^N \ln \frac{g_1(y_i) f_1'(g_1(y_i)) + f_1(g_1(y_i))}{g_0(y_i) f_0'(g_0(y_i)) + f_0(g_0(y_i))}$$

where $g_1(y)$ and $g_0(y)$ are the inverse functions of $w_1(x) = x f_1(x)$ and $w_0(x) = x f_0(x)$, respectively.

Considering (3), we need to have the standard deviation σ_x and the shape parameter β of the GGD function for the supposed directional subband in each block.

There are two approaches to find these parameters. First, we can use the kurtosis of the GGD coefficients to find the β parameter. To do so, we first compute kurtosis as

$$k_x = \frac{1}{\left(\frac{1}{N} \sum_{i=1}^N x_i^2\right)^2} \frac{1}{N} \sum_{i=1}^N x_i^4.$$

Then, we use the method to find β from the kurtosis discussed in [40]

$$k_x = \frac{\Gamma\left(\frac{1}{\beta}\right) \Gamma\left(\frac{5}{\beta}\right)}{\Gamma^2\left(\frac{3}{\beta}\right)}. \quad (23)$$

To find the σ_x parameter, we suggest an estimator which is fitted for our ML detector. Suppose we have N GGD coefficients in the current subband. Then, the distribution of these coefficients can be defined as

$$P(\beta, \sigma_x; x) = \prod_{i=1}^N GG(x_i). \quad (24)$$

By applying a logarithmic function to both sides, we have

$$L(\beta, \sigma_x; x) = N \ln C(\sigma_x, \beta) - \alpha(\sigma_x, \beta)^\beta \sum_{i=1}^N |x_i|^\beta. \quad (25)$$

Computing the root of $\partial L(\beta, \sigma_x; x) / \partial \sigma_x = 0$, we have

$$\hat{\sigma}_x = \left[\frac{\Gamma\left(\frac{3}{\beta}\right)}{\Gamma\left(\frac{1}{\beta}\right)} \right]^{\frac{1}{2}} \left(\frac{\beta}{N} \sum_{i=1}^N |x_i|^\beta \right)^{\frac{1}{\beta}}. \quad (26)$$

Besides, we can utilize another scheme discussed in [41] to find GGD parameters. In this idea, we use an approach called the method of moments estimator (MME) suggested to find the shape parameter β . The MME to find β is given as

$$\beta = M^{-1}(\bar{M}(x)) \quad (27)$$

where

$$M(\beta) = \frac{\Gamma^2\left(\frac{2}{\beta}\right)}{\Gamma\left(\frac{1}{\beta}\right)\Gamma\left(\frac{3}{\beta}\right)}$$

and

$$\bar{M}(x) = \frac{\left(\frac{1}{N} \sum_{i=1}^N |x_i|\right)^2}{\frac{1}{N} \sum_{i=1}^N |x_i|^2}.$$

Using this approach, we can simply find the shape parameter β and then use it in (26) to estimate the ML parameter.

We can use both of these approaches to estimate GGD parameters. However, we use the first one in our simulations.

V. PARAMETER OPTIMIZATION

The strength functions $f_1(x)$ and $f_0(x)$ have critical role on the performance of the watermarking scheme. These functions can affect two factors in the watermarked image: visibility and robustness. Since $f_0(x)$ can be calculated from $f_1(x)$ through (15), we only consider the effect of $f_1(x)$. First, larger values of $f_1(x)$ can cause more distortions in the image due to the watermark. On the other hand, larger values of $f_1(x)$ increase the robustness of the watermarked image against various attacks. Therefore, there is a trade-off between visibility and robustness. We utilize a multi-objective optimization technique to select an appropriate strength functions ensuring imperceptibility with acceptable robustness.

As we see in (15), there is one degree of freedom, a_3 , in defining the strength functions $f_1(x)$ and $f_0(x)$. We thus seek for an appropriate value of a_3 satisfying the requirement of imperceptibility and robustness.

We model the effect of the strength function on the visibility using the image quality index Q suggested in [42], [43]. In this quality assessment method, any image distortion is modeled as a combination of three factors considering the properties of the HVS: 1) loss of correlation, 2) luminance distortion, and 3) contrast distortion. This image quality index outperforms traditional quality assessment methods such as MSE due to its conformity to HVS and subjective tests.

If we denote the original and the manipulated watermarked images with X and Y , respectively, the quality index Q is defined as

$$Q = \frac{(2\hat{X}\hat{Y} + C_1)(2\sigma_{XY} + C_2)}{\left[(\hat{X})^2 + (\hat{Y})^2 + C_1\right](\sigma_X^2 + \sigma_Y^2 + C_2)} \quad (28)$$

where \hat{X} , \hat{Y} , σ_X^2 , and σ_Y^2 are the mean values and variances of X and Y , respectively. Moreover, parameters C_1 and C_2 are defined as

$$C_1 = (K_1L)^2, \quad C_2 = (K_2L)^2$$

where L is the dynamic range of the pixel values (255 for 8-bit grayscale images), and $K_1, K_2 \ll 1$ are small constants (we

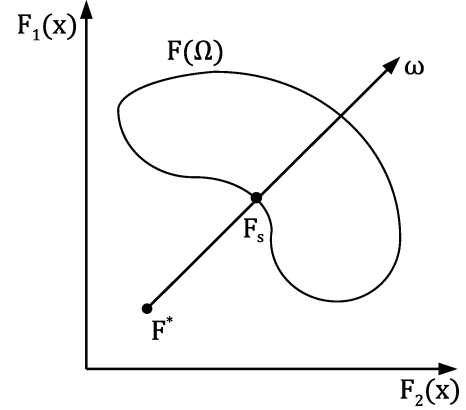


Fig. 8. Goal attainment optimization method.

choose $K_1 = 0.01$ and $K_2 = 0.03$ throughout this paper as suggested in [42]). The best value for Q is achieved if and only if $X_i = Y_i$ for all $i = 1, 2, \dots, N$.

Since image signals are generally nonstationary and image quality is often spatially variant, it is reasonable to measure statistical features locally and then combine them together. Wang *et al.* [42] suggested to apply the quality measurement to nonoverlapping $B \times B$ block segments of the image, calculate a local index Q_j for each block, and find the overall quality index for M blocks by arithmetic averaging.

However, as humans judge the image quality based on the worse blocks, we decided to use the geometric averaging instead. This way a single low-quality block can effectively reduce the overall Q . Thus, we calculate the quality index as

$$Q = \left(\prod_{j=1}^M Q_j \right)^{\frac{1}{M}}. \quad (29)$$

Thus, to show the effect of the strength function on the visibility, we define an objective function $h_D(a_3) = 1 - Q(a_3)$, where $Q(a_3)$ is the quality index factor calculated in (29) for the image watermarked by the strength functions $f_0(x)$ and $f_1(x)$. This objective function reveals the effect of a_3 on the distortion introduced in the image.

Another factor which is necessary in the watermarking scheme is the robustness. We define another objective function $h_E(a_3)$, which is calculated as the average BER (Bit-Error-Rate) against two typical attacks which are common in our application, for example JPEG compression with quality factor of 10% and AWGN attack with $\sigma_n = 30$. In other words, for each value of a_3 parameter, we watermark the image with the proposed scheme using the strength functions $f_0(x)$ and $f_1(x)$.

As we can see in Fig. 6, increasing the a_3 parameter increases the strength of the proposed watermarking scheme by amplifying $f_1(x)$ and attenuating $f_0(x)$. Thus, it increases the distortion $h_D(a_3)$, while $h_E(a_3)$ decreases. Our goal is to find an optimum value of a_3 which minimizes both these objective functions simultaneously. Therefore, we treat it as a multi-objective optimization problem. To solve this problem, we use the goal attainment method of Gembicki [44].



Fig. 9. Original, watermarked and difference images using the proposed method: *Baboon*, *Barbara*, *Map*, *Bridge*, and *Couple*. For each image, the top one is the original test image, the middle one is the watermarked image, and the bottom one is the five times scaled of the absolute difference between the watermarked and the original image.

In this method, to optimize a set of l objective functions $F(x) = [F_1(x), F_2(x), \dots, F_l(x)]$ which have some trade-offs, a set of design goals, $F^* = [F_1^*, F_2^*, \dots, F_l^*]$ and a set of weights, $W = [W_1, W_2, \dots, W_l]$ are considered. Then, the goal attainment problem can be formulated as

$$\min_{\lambda \in \mathbb{R}} \lambda \quad \text{subject to} \quad F_i(x) - W_i \lambda \leq F_i^* \\ i = 1, 2, \dots, m, \quad x \in \Omega \quad (30)$$

where Ω is the feasible region in the parameter space x , and λ is an auxiliary variable unrestricted in sign. The weight vector, W , enables the designer to select trade-offs between the objectives. That is, if we can tolerate an objective to be under-attained, a smaller weight is assigned to it; conversely, if we require an objective to be over-attained, then a larger weight must be assigned to it.

Fig. 8 illustrates geometrically the goal attainment method for two objective functions. In this figure, $F(\Omega)$ is the feasible region in the objective function space. The minimum value of λ occurs in F_s where $F^* + W\lambda$ vector intersects the lower boundary of the objective space $F(\Omega)$.

In our problem, we have two competitive objective functions $h_D(a_3)$ and $h_E(a_3)$. Using the goal attainment method, we can find the optimum value of a_3 for this multi-objective optimization problem that offers an imperceptible robust result.

VI. SIMULATION RESULTS

We have performed several experiments to test the proposed algorithms and evaluate its performance against several attacks which are common in our application. For the contourlet transform as suggested in [19], we use the 9–7 biorthogonal filters with three levels of pyramidal decomposition for the multiscale decomposition stage and the ladder filters introduced by Phoong *et al.* [45] (referred to as PKVA filters) for the multidirectional decomposition stage. We partition the finest scale to eight directional subbands. The results are obtained by averaging over 20 runs with 20 different pseudorandom binary sequences as the watermarking signal.

For this study, we use five natural images (*Baboon*, *Barbara*, *Map*, *Bridge*, and *Couple*) of size 512×512 . The original test images and their watermarked version using the proposed method with 16×16 block size and 128 bits message length as well as the five times scaled of the absolute difference between the watermarked and the original image are shown in Fig. 9. As we can see, the watermark invisibility is satisfied. The mean Peak-Signal-to-Noise-Ratio (PSNR) between the original and the watermarked images are 39.53, 36.63, 39.87, 42.40, and 42.48 dB, respectively.

We have also tested other block sizes and bit rates as well but here we show the results for the block size of 16×16 which delivers us suitable robustness against different attacks along with an appropriate transparency of the watermark data. Besides, we have studied the performance of the proposed contourlet base

method over similar DWT based approach for different block sizes to find the efficiency of implementation of contourlet. Experimental results revealed that as we have expected even for the small block size of 16×16 there is a notable difference between the performance of contourlet and wavelet transform. In fact, wavelet as a separable 2-D multi resolution transform just follows the curves as horizontal-vertical lines and essentially cannot represent 2-D directional discontinuity which is common in as image edges. Thus, contourlet has advantage over the wavelet transform in our proposed method, in which the great performance is obtained where the transform coefficients are sparse.

For the proposed semi-blind approach, a typical side information bit budget needed for an image of size 512×512 and assuming 16×16 block size and 128-bit message length is as follows:

- i) block positions: 1 bit/block = $(512/16)^2 = 1024$ bits (we send "1" if a block is among the high entropy blocks and "0" otherwise);
- ii) 4-bit words for the shape parameter (β) and 8 bit words for the ML parameter as mentioned in (26): $12.128 = 1536$ bits;
- iii) a_3 : 8 bits.

Thus, the raw side information necessitates 2568 bits/image. The block positions, however, can be compressed to near 512 bits on the average using Arithmetic coding as a lossless coding. Other block parameters also can be reduced with lossy coding to near 1024 bits using Vector Quantization (VQ) with negligible loss in the performance. Thus, in total the side information is reduced to near 1.5 Kbits on the average per image.

A. Capacity

To show the capacity of the proposed scheme, a graph of capacity versus noise standard deviation is shown in Fig. 10. In this graph, we have considered a fixed BER of 1% as a typical sufficiently small error rate and investigated the maximum message length in bits for 16×16 block size which obtains this error rate. The average message length over five test images is shown in Fig. 10. As shown in this figure, even for heavy noise powers of $\sigma_n = 30$, the capacity of the proposed method in obtaining the BER of less than 1% is near 60 bits.

B. Performance Under Attacks

Here, we test the performance of the proposed technique against several common watermarking attacks such as JPEG compression, AWGN, salt&pepper noise, rotation, and scaling attacks.

1) *AWGN Attack*: In the first experiment, we investigate the effect of AWGN to the proposed watermarking scheme. Fig. 11(a) shows the BER of the proposed method for various images versus different noise power. As we expect, the method has a great resistance even against heavy AWGN attack. This is because the receiver is optimized for the noisy environment.

2) *JPEG Attack*: In the second experiment, the proposed technique is tested against JPEG compression with different quality factor. As demonstrated in Fig 11(b), the proposed method is highly robust against JPEG with different quality factor up to 10%.

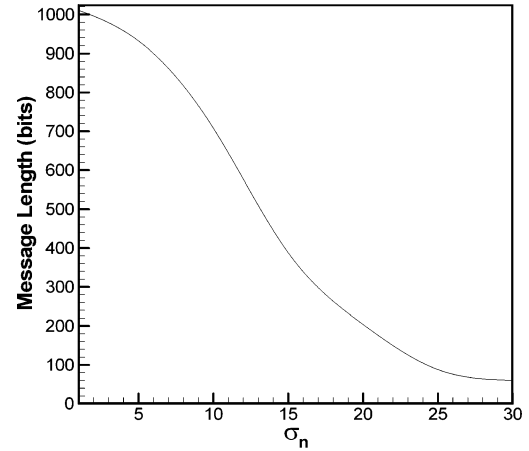


Fig. 10. Capacity of the proposed method for BER less than 1%.

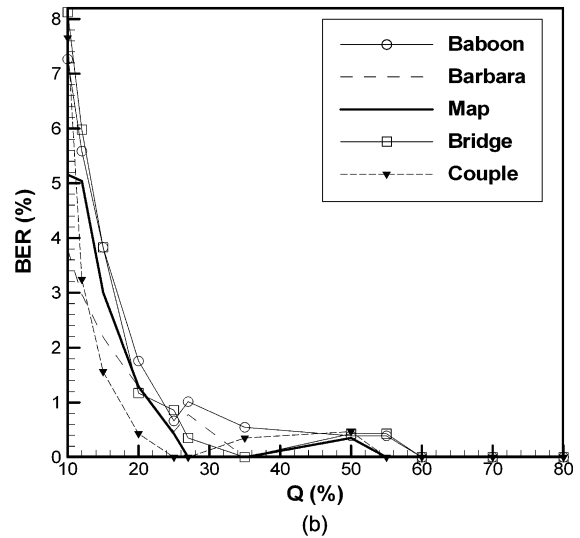
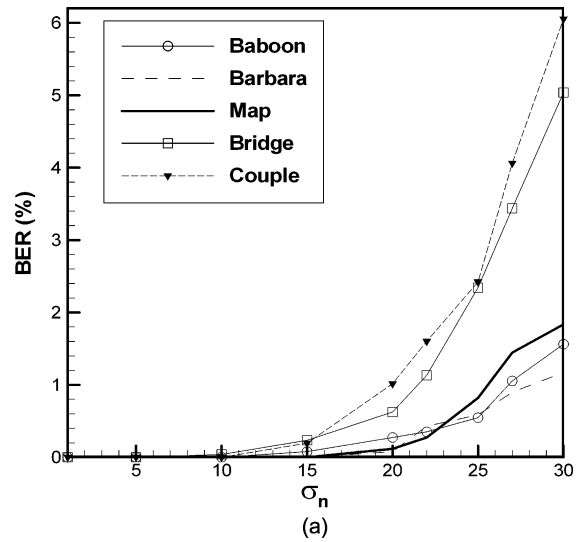


Fig. 11. (a) AWGN attack for various test images with different noise variances. (b) JPEG compression attack for various quality factors.

3) *Salt&Pepper Noise Attack*: In the third experiment, the proposed technique is tested against salt&pepper noise attack. The BER results for different densities of salt&pepper noise

TABLE I
BER(%) RESULTS OF EXTRACTED WATERMARK UNDER
SALT&PEPPER NOISE ATTACK

Image	salt&pepper noise percentage				
	1%	2%	3%	4%	5%
Baboon	0.63	0.31	0.63	1.56	2.89
Barbara	0.00	0.04	0.35	0.94	1.48
Map	0.27	0.90	1.99	3.24	6.05
Bridge	0.43	1.29	2.50	4.92	8.32
Couple	0.59	0.98	3.05	5.20	8.71

are given in Table I. We can see that the proposed method is highly robust against salt&pepper noise attack even for high salt&pepper noise percentage up to 5%.

4) *Rotation Attack*: In the next experiment, we investigate the robustness against rotation attack. The proposed embedding approach is robust to rotation provided that one can compensate for the loss of synchronization. Thus, we propose a synchronization technique to estimate the rotation angle, rotate back the image and then detect the watermark code. In this synchronization method, we estimate the rotation angle in two steps consisting a coarse estimation and a fine tuning step. We use the side information available in our semi-blind approach for the synchronization purpose: the coarse estimation uses the indices of block positions and then the fine estimation is performed using the shape and ML parameters.

Step 1) *Coarse Estimation*: In the coarse estimation step, we divide all the possible rotation angles in $[-90^\circ, 90^\circ]$ to 18 segments of 10° width and consider 18 coarse angles of $\theta_c \in \{-85^\circ, -75^\circ, \dots, -15^\circ, -5^\circ, 5^\circ, 15^\circ, \dots, 75^\circ, 85^\circ\}$. For each of these angles, we rotate the received image reversely with $-\theta_c$ and find the N high entropy blocks of the image. Then we count the number of the high entropy blocks that matches with the high entropy blocks of the original images which has been used for watermark embedding. The angle θ_c , which yields the most number of matched blocks, is considered as the coarse estimated angle of rotation. Fig. 12(a) illustrates the corresponding number of matched blocks after angle correction versus several rotation angles for two test cases of *Barbara* image rotated by 27° and *Couple* image rotated by -31° . As it is clear from the figures, the number of matched block is maximized when the attacked image is rotated by -25° for *Barbara* and -35° for *Couple* which corresponds to the nearest possible coarse angles.

Step 2) *Fine Tuning*: The rotation angle estimated in the previous step is a coarse estimation of the true values. To find the exact rotation angle, we divide the detected segment of the coarse estimation $[\theta_c - 5^\circ, \theta_c + 5^\circ]$ to 20 small segments to find the rotation angle with the accuracy of 0.5° . To this aim, we search in the fine tuning angles of $\theta_f \in \{\theta_m - 5^\circ, \theta_m - 4.5^\circ, \dots, \theta_m - 0.5^\circ, \theta_m, \theta_m + 0.5^\circ, \dots, \theta_m + 4.5^\circ, \theta_m + 5^\circ\}$. For each fine estimation angle θ_f , we first rotate the received image

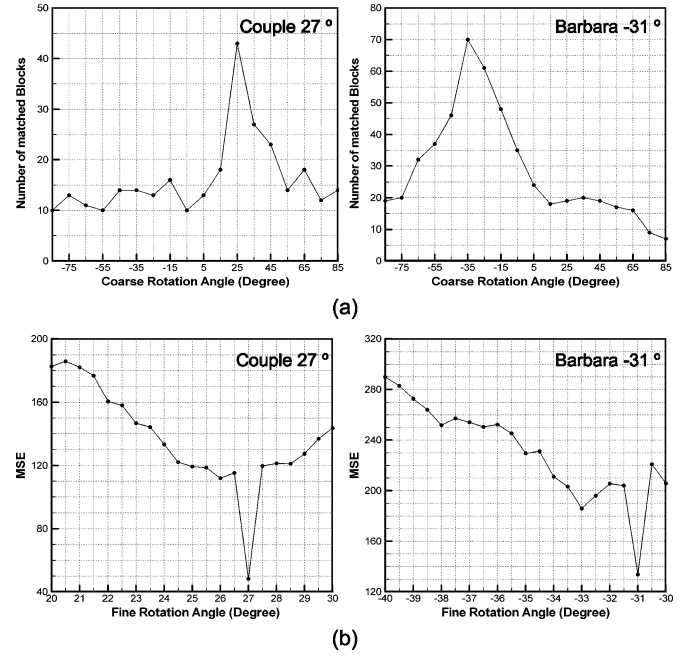


Fig. 12. Estimation of the rotation angle for Couple image rotated by 27° and Barbara image rotated by -31° : (a) coarse estimation and (b) fine estimation.

reversely with $-\theta_f$ and then compute the following factor:

$$MSE = \frac{1}{N} \sum_1^N |\hat{\sigma}_x - \hat{\sigma}_w|^2 \quad (31)$$

where $\hat{\sigma}_x$ and $\hat{\sigma}_w$ are the standard deviation of the contourlet coefficients in each block of the original image and the reversely rotated image, respectively. $\hat{\sigma}_x$ is available at the receiver as a secret key and $\hat{\sigma}_w$ is calculated in the receiver as

$$\hat{\sigma}_w = \min \left(\hat{\sigma}_{x|\hat{f}_0}, \hat{\sigma}_{x|\hat{f}_1} \right). \quad (32)$$

The angle θ_f yielding the smallest MSE is considered as the estimated angle of rotation. Fig. 12(b) illustrates the corresponding MSE after angle correction versus several rotation angles for two test cases discussed in step 1. It is clear in these figures that the estimated angles are an accurate indication of how much the image has been rotated.

Using the proposed two step estimation approach, we find the rotation angle. Then, we reversely rotate the received image by the estimated angle and use the ML detector to extract the watermark code. The resulted performance is reported in Table II. The high robustness of the proposed method is obvious.

5) *Scaling Attack*: The last attack we study is the scaling attack. The BER results are reported in Table III. It is clear that the proposed method is highly robust against attacks with different scaling factors. It must be noted that for scaling factors less than one this attack can be considered as a low pass filtering attack. Besides, for scaling attack, we assumed that the detector knows the original size of the image, for example, all the tested images are 512×512 . The detector also can find the image size utilizing the side information. For instance, the first part of the side

TABLE II
BER(%) RESULTS OF EXTRACTED WATERMARK UNDER ROTATION ATTACK

Image	Rotation Angle (Degree)															
	-90	-60	-30	-10	-5	-2	-1	-0.5	0.5	1	2	5	10	30	60	90
Baboon	0.00	16.06	16.37	5.16	2.85	0.55	0.55	0.00	0.00	0.00	0.00	1.52	4.30	16.06	16.37	0.00
Barbara	0.00	4.57	5.78	1.29	0.59	0.51	0.27	0.27	0.00	0.00	0.00	0.00	0.27	4.57	5.78	0.00
Map	0.00	11.29	9.53	6.68	5.59	6.13	5.63	4.88	4.73	5.43	5.00	6.76	7.89	11.29	9.53	0.00
Bridge	0.00	8.01	6.29	2.89	1.72	0.27	0.00	0.00	1.76	3.83	3.67	5.74	7.42	8.01	6.29	0.00
Couple	0.00	2.30	2.54	2.15	0.86	0.27	0.00	0.00	0.90	0.90	1.25	0.74	0.74	2.30	2.54	0.00

TABLE III
BER(%) RESULTS OF EXTRACTED WATERMARK UNDER SCALING ATTACK

Image	Scaling Factor					
	0.75	0.8	0.9	1.1	1.5	2
Baboon	10.39	3.20	1.17	0.00	0.00	0.00
Barbara	31.02	2.34	0.31	0.00	0.00	0.00
Map	10.82	9.30	4.77	0.00	0.00	0.00
Bridge	7.85	8.20	3.13	0.00	0.00	0.00
Couple	13.28	9.92	5.47	0.00	0.00	0.00

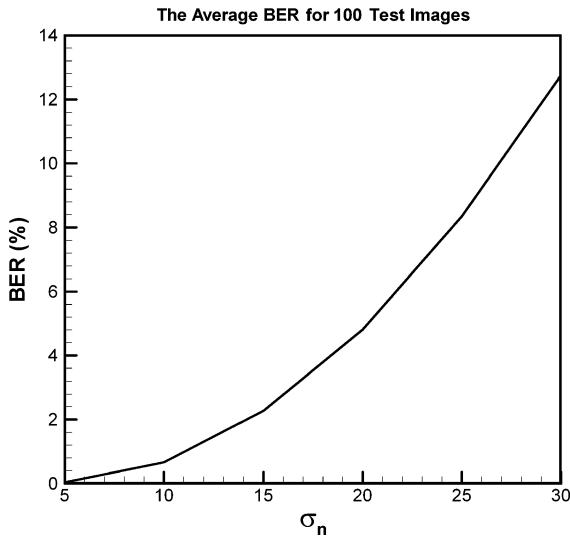


Fig. 13. BER averaged results for the AWGN attacks over 100 different test images watermarked with the proposed scheme.

information, the block positions, reveals the image size. Thus, knowing the size of the original image, we can resize the attacked image to its original size and then decode the watermark code. In fact, the distortion after this resizing is the distortion of (downsampling-upsampling) or vice versa.

6) *Testing the Performance for Various Images:* Here, we test the performance of the proposed technique for 100 different test images selected from different categories of natural images. The average BER for AWGN attack is given in Fig. 13. As we can see, we have a good robustness for these test images and this shows the significance of other method and its generality for various test images.

C. Comparison With Other Watermarking Schemes

In this section, to compare our watermarking algorithm with other watermarking schemes, we use the same bit rate and PSNR

TABLE IV
COMPARISON BETWEEN OUR WATERMARKING METHOD AND MWT-EMD METHOD [46]: BER (%) UNDER JPEG COMPRESSION ATTACK FOR *Baboon* IMAGE. IN THIS EXPERIMENT, THE MESSAGE LENGTH IS 64 bits AND PSNR OF THE WATERMARKED IMAGE IS 42 dB AS USED IN [46]

Method	JPEG Quality Factor			
	5	10	15	20
MWT-EMD [46]	4.69	0.00	0.00	0.00
Proposed	6.30	4.69	0.00	0.00

TABLE V
COMPARISON BETWEEN OUR WATERMARKING METHOD AND MWT-EMD METHOD [46]: BER (%) UNDER ROTATION ATTACK FOR *Baboon* IMAGE. IN THIS EXPERIMENT, THE MESSAGE LENGTH IS 64 bits AND PSNR OF THE WATERMARKED IMAGE IS 42 dB AS USED IN [46]

Method	Rotation Angle (Degree)					
	-2	-1	-0.5	0.5	1	2
MWT-EMD [46]	56.3	54.7	43.8	45.3	53.1	43.8
Proposed	0.00	0.00	0.00	0.00	0.00	0.00

as the bit rate and PSNR used in other techniques. The simulation results are shown in Tables IV and V and Figs. 14 and 15.

In Tables IV and V and Fig. 14, we compare our watermarking scheme with the MWT-EMD method [46] for JPEG compression, rotation, and AWGN attacks. In this experiment, we use the message length of 64 bits and PSNR (42 dB) for the watermarked image as used in [46] with the *Baboon* image. We see that the robustness of our method against JPEG compression attack is slightly lower than MWT-EMD method. However, in AWGN attack, our results are considerably better as our detector is optimized for the noisy environment. Moreover, we see that, unlike the MWT-EMD method, our scheme is highly robust against rotation attack due to the synchronization technique we used in the detector to estimate the rotation angle.

The comparison with the Ergodic Chaotic Parameter Modulation (ECPM) method [47] is shown in Fig. 15. In this experiment, we embed the watermark code with different message length in the host image and attack the watermarked image by AWGN with $\sigma_n^2 = 5$ for different message lengths. As we can see in Fig. 15, our method considerably outperforms the EPCM method.

D. Extension to a Blind Technique

Here, we will suggest a blind extension of the proposed watermarking technique. To make our system blind we should estimate two parameters of the GGD distribution function parameters: σ_x and β at the receiver. For this purpose, we make a slight change in our embedding strategy. So far, we have used (12) to

TABLE VI
BER(%) RESULTS OF THE SUGGESTED BLIND WATERMARKING TECHNIQUE UNDER ROTATION ATTACK

Image	Rotation Angle (Degree)									
	-10	-5	-2	-1	-0.5	0.5	1	2	5	10
Baboon	9.69	6.88	3.98	2.62	3.52	3.20	3.55	3.91	4.41	7.15
Barbara	9.69	8.87	8.44	8.13	8.01	8.13	8.13	8.55	7.11	8.59
Map	12.31	11.99	11.45	11.60	11.02	10.00	9.65	9.92	11.29	11.84
Bridge	3.13	2.30	2.11	0.39	0.39	1.64	2.73	2.93	5.59	6.99
Couple	3.95	2.62	2.89	2.03	1.68	2.03	2.38	2.81	3.16	1.88

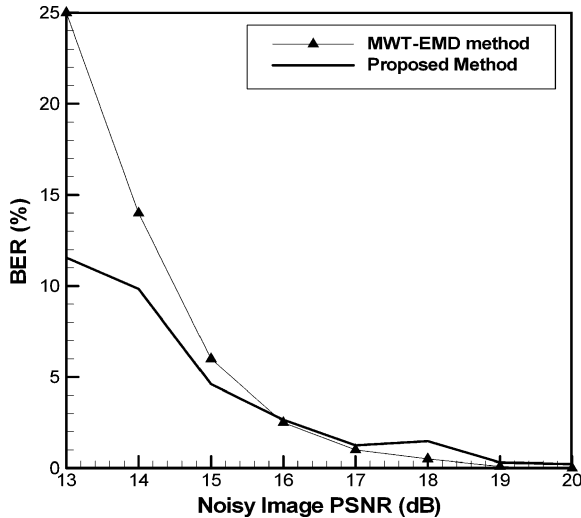


Fig. 14. Comparison between our watermarking method and MWT-EMD method [46] for different images: BER (%) under AWGN attack.

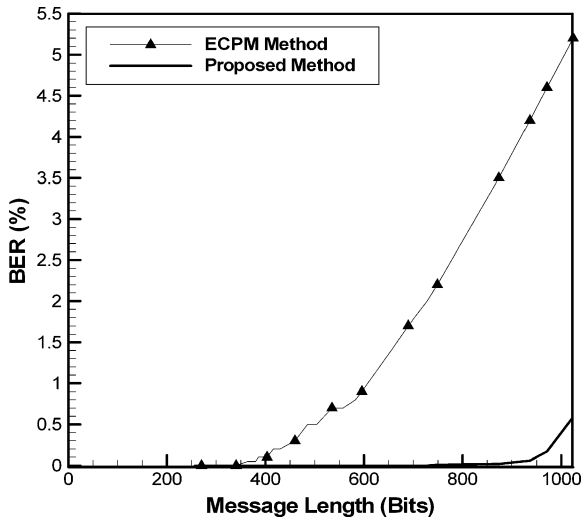


Fig. 15. Comparison between our watermarking method and the ECPM method [47]: BER (%) under AWGN attack for the noise variance of $\sigma_n^2 = 5$ with different message lengths.

hide data in the contourlet coefficients. Now, we only change half of the coefficients. In other words, we use two random subsets of coefficients and only embed data in the coefficients of one subset, like the patchwork idea [48]. The indices of these subsets are produced by a random generator and the seed is sent to the decoder side through a secure channel. Besides, we maintain the other half of the coefficients unchanged. If we put the coefficients in the selected subband in a vector and show them

by x_i , the embedding process is performed using the following strategy:

$$w_i = \begin{cases} x_i \cdot f_1(x_i), & \text{for embedding 1} \\ x_i \cdot f_0(x_i), & \text{for embedding 0} \end{cases} \quad \begin{matrix} i \in S \\ i \notin S \end{matrix} \quad (33)$$

where S is the random subset mentioned above.

On the receiver end, we use these unchanged coefficients to estimate the GGD parameters σ_x and β . Therefore, we do not need to send these parameters as the secret key and our scheme is blind. β is estimated by solving

$$\hat{k}_x = \frac{\Gamma\left(\frac{1}{\beta}\right)\Gamma\left(\frac{5}{\beta}\right)}{\Gamma^2\left(\frac{3}{\beta}\right)} \quad (34)$$

where \hat{k}_x is the kurtosis of the unchanged coefficients (in other subset). If we call these coefficients x_u , \hat{k}_x is computed as

$$\hat{k}_x = \frac{1}{(\sigma_{x_u}^4)^{\frac{1}{2}}} \frac{1}{N} \sum_{i=1}^{\frac{N}{2}} x_{u_i}^4 \quad (35)$$

where N is the number of coefficients in the selected subband.

To estimate the σ_x parameter, we use our ML estimator given in (26); however, we only use unchanged coefficients x_u . Thus, σ_x is estimated by

$$\hat{\sigma}_x = \left[\frac{\Gamma\left(\frac{3}{\beta}\right)}{\Gamma\left(\frac{1}{\beta}\right)} \right]^{\frac{1}{2}} \left(\frac{\beta}{N} \sum_{i=1}^{\frac{N}{2}} |x_{u_i}|^\beta \right)^{\frac{1}{\beta}} \quad (36)$$

Thus, for this blind version, no side information is needed because the value of the a_3 is already set as an agreement between the coder and decoder, the shape parameter β and the ML value are estimated from the unchanged subset of contourlet coefficients, and the indices of high entropy blocks are estimated using error correction codes as proposed in [49].

The results of the suggested blind watermarking technique for JPEG and AWGN attack are shown in Fig. 16. Performance under salt&pepper noise, rotation, and scaling attack are also provided in Tables VII and VIII. It is found that although the performance of the suggested blind technique is slightly lower than the semi-blind scheme, it has still acceptable robustness against various attacks. It should be noted that for the rotation attack in the blind version on the contrary to the semi-blind version, we just have the fine estimation using the error correction coding [49] and parameter estimation simultaneously. This is why the results have a lower performance in this case in comparison with the results of semi-blind version.

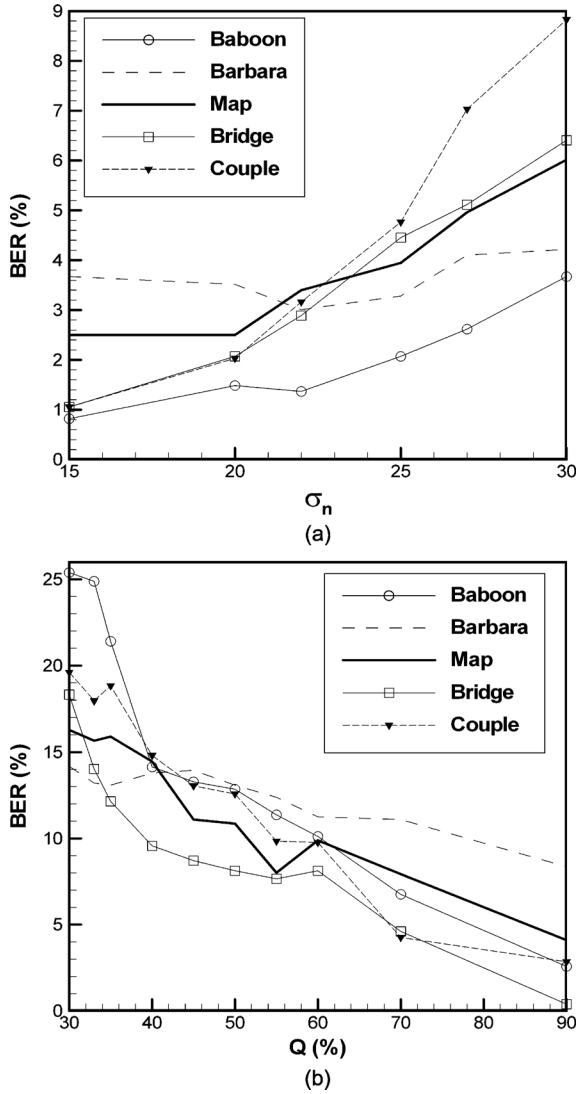


Fig. 16. Performance of the suggested blind watermarking technique under (a) AWGN and (b) JPEG compression attack for various test images.

TABLE VII

BER(%) RESULTS OF THE SUGGESTED BLIND WATERMARKING TECHNIQUE UNDER SALT&PEPPER NOISE ATTACK

Image	salt&pepper noise percentage				
	1%	2%	3%	4%	5%
Baboon	1.91	2.66	2.81	3.52	3.79
Barbara	3.28	3.59	4.18	4.41	4.80
Map	7.70	8.44	9.26	10.27	10.98
Bridge	5.43	6.64	7.27	7.89	9.10
Couple	6.72	8.36	8.55	9.61	10.35

TABLE VIII

BER(%) RESULTS OF THE SUGGESTED BLIND WATERMARKING TECHNIQUE UNDER SCALING ATTACK

Image	Scaling Factor				
	0.8	0.9	1.1	1.5	2
Baboon	21.37	9.53	3.05	3.05	3.05
Barbara	10.39	9.84	8.28	8.28	8.28
Map	12.07	8.16	2.62	2.62	2.62
Bridge	7.85	3.98	0.47	0.47	0.47
Couple	7.19	4.69	1.88	1.88	1.88

VII. CONCLUSION

In this paper, we have introduced a robust multiplicative image watermarking technique in the contourlet transform domain. The proposed algorithm is presented in both semi-blind and blind versions. Since the contourlet transform concentrates the image energy in the limited number of edge coefficients, using multiplicative approach in this domain yields high robustness accompanied by great transparency. To have better control on both imperceptibility and robustness, the strength functions are selected optimally by multi-objective optimization approach. We model the distribution of contourlet coefficients by GGD. Then, the distribution of watermarked noisy coefficients is calculated analytically. Using ML decision rule, the optimum detector has been proposed. The optimal detector guarantees the suggested method is well suited for high noisy environment. Experimental results over several images confirm the excellent resistance against common attacks in the semi-blind version. In the blind version the proposed method outperforms recently proposed techniques in AWGN and rotation attacks, while it has competitive results in JPEG attacks.

REFERENCES

- [1] J. Seitz, *Digital Watermarking for Digital Media*. Arlington, VA: Information Science Publishing, 2005.
- [2] C. S. Lu, *Multimedia Security: Stenography and Digital Watermarking Techniques for Protection of Intellectual Property*. Hershey, PA: Idea Group Publishing, 2004.
- [3] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data: A state-of-the-art overview," *IEEE Trans. Signal Process. Mag.*, vol. 17, no. 5, pp. 20–46, May 2000.
- [4] P. Moulin and J. A. O'Sullivan, "Information-theoretic analysis of information hiding," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 563–593, Mar. 2003.
- [5] A. Maor and N. Merhav, "On joint information embedding and lossy compression in the presence of a stationary memoryless attack channel," *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3166–3175, Sep. 2005.
- [6] C. T. Hsu and J. L. Wu, "Multiresolution watermarking for digital images," *IEEE Trans. Circuit Syst.*, vol. 45, no. 8, pp. 1097–1101, Aug. 1998.
- [7] D. Kundur and D. Hatzinakos, "Towards robust logo watermarking using multiresolution image fusion principles," *IEEE Trans. Image Process.*, vol. 6, no. 1, pp. 185–198, Jan. 2004.
- [8] M. Barni and F. Bartolini, *Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications*. Boca Raton, FL: CRC, 2004.
- [9] M. A. Akhatee, S. M. E. Sahraeian, B. Sankur, and F. Marvasti, "Robust scaling-based image watermarking using maximum-likelihood decoder with optimum strength factor," *IEEE Trans. Multimedia*, vol. 11, no. 5, pp. 822–833, May 2009.
- [10] E. P. Simoncelli, W. T. Freeman, E. H. Adelson, and D. J. Heeger, "Shifttable multiscale transforms," *IEEE Trans. Inf. Theory*, vol. 38, no. 2, pp. 587–607, Feb. 1992.
- [11] F. G. Meyer and R. R. Coifman, "Brushlets: A tool for directional image analysis and image compression," *J. Appl. Comput. Harmon. Anal.*, vol. 5, pp. 147–187, 1997.
- [12] N. Kingsbury, "Complex wavelets for shift invariant analysis and filtering of signals," *J. Appl. Comput. Harmon. Anal.*, vol. 10, pp. 234–253, 2001.
- [13] I. W. Selesnick, R. G. Baraniuk, and N. G. Kingsbury, "The dual-tree complex wavelet transform," *IEEE Signal Process. Mag.*, vol. 22, pp. 123–151, Nov. 2005.
- [14] V. Velisavljevic, P. L. Dragotti, and M. Vetterli, "Directional wavelet transforms and frames," in *Proc. IEEE Int. Conf. Image Processing*, 2002, vol. 3, pp. 589–592.
- [15] L. Demanet and L. Ying, "Wave atoms and sparsity of oscillatory patterns," *Appl. Comput. Harmon. Anal.*, vol. 23, p. 368, 2007.
- [16] E. Le Pennec and S. Mallat, "Sparse geometric image representations with bandelets," *IEEE Trans. Image Process.*, vol. 14, no. 4, pp. 423–438, Apr. 2005.

- [17] E. J. Candes and D. L. Donoho, "Ridgelets: A key to higher-dimensional intermittency?," *Philos. Trans. Roy. Soc. London A*, vol. 357, no. 1760, pp. 2495–2509, 1999.
- [18] E. J. Candes and D. L. Donoho, "Curvelets—a surprisingly effective non-adaptive representation for objects with edges," in *Curve and Surface Fitting*, C. R. A. Cohen and L. Schumaker, Eds. Nashville, TN: Vanderbilt Univ. Press, 2000.
- [19] M. N. Do and M. Vetterli, "The contourlet transform: An efficient directional multiresolution image representation," *IEEE Trans. Image Process.*, vol. 14, no. 12, pp. 2091–2106, Dec. 2005.
- [20] D. D.-Y. Po and M. N. Do, "Directional multiscale modeling of images using the contourlet transform," *IEEE Trans. Image Process.*, vol. 15, no. 6, pp. 1610–1620, Jun. 2006.
- [21] M. Jayalakshmi, S. N. Merchant, and U. B. Desai, "Digital watermarking in contourlet domain," in *Proc. 18th Int. Conf. Pattern Recognition*, 2006, vol. 3, pp. 861–864.
- [22] M. Jayalakshmi, S. N. Merchant, and U. B. Desai, "Blind watermarking in contourlet domain with improved detection," presented at the Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06), .
- [23] L. Xueqiang, D. Xinghao, and G. Donghui, "Digital watermarking based on non-sampled contourlet transform," in *Proc. IEEE Int. Workshop Anti-counterfeiting, Security, Identification*, 2007, pp. 138–141.
- [24] H. Li, W. Song, and S. Wang, "A novel blind watermarking algorithm in contourlet domain," in *Proc. 18th Int. Conf. Pattern Recognition*, 2006, vol. 3, pp. 639–642.
- [25] S. Xiao, H. Ling, F. Zou, and Z. Lu, "Adaptive image watermarking algorithm in contourlet domain," in *Proc. Japan-China Joint Workshop on Frontier of Computer Science and Technology*, 2007, pp. 125–130.
- [26] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoan, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.
- [27] Q. Cheng and T. S. Huang, "Robust optimum detection of transform domain multiplicative watermarks," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 906–924, Apr. 2003.
- [28] M. Barni, F. Bartolini, A. De Rosa, and A. Piva, "A new decoder for the optimum recovery of nonadditive watermarks," *IEEE Trans. Image Process.*, vol. 10, no. 5, pp. 755–766, May 2001.
- [29] M. Barni, F. Bartolini, A. De Rosa, and A. Piva, "Optimum decoding and detection of multiplicative watermarks," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 1118–1123, Apr. 2003.
- [30] T. Ng and H. Garg, "Maximum likelihood detection in image watermarking using generalized gamma model," in *Proc. 39th Asilomar Conf. Signals, Systems and Computer*, 2005, pp. 1680–1684.
- [31] J. Wang, G. Liu, Y. Dai, and J. Sun, "Locally optimum detection for Barni's multiplicative watermarking in DWT domain," *Signal Process.*, vol. 88, pp. 117–130, 2008.
- [32] V. Solachidis and I. Pitas, "Optimal detector for multiplicative watermarks embedded in the DFT domain of non-white signals," *EURASIP J. Appl. Signal Process.*, vol. 2004, no. 16, pp. 2522–2532, 2004.
- [33] T. M. Ng and H. K. Garg, "Maximum-likelihood detection in DWT domain image watermarking using laplacian modeling," *IEEE Signal Process. Lett.*, vol. 12, no. 4, pp. 285–288, 2005.
- [34] P. J. Burt and E. H. Adelson, "The Laplacian pyramid as a compact image code," *IEEE Trans. Commun.*, vol. COM-31, no. 4, pp. 532–540, Apr. 1983.
- [35] R. H. Bamberger and M. J. T. Smith, "A filter bank for the directional decomposition of images: Theory and design," *IEEE Trans. Signal Process.*, vol. 40, no. 4, pp. 882–893, Apr. 1992.
- [36] M. N. Do and M. Vetterli, "Framing pyramids," *IEEE Trans. Signal Process.*, vol. 51, no. 9, pp. 2329–2342, Sep. 2003.
- [37] A. L. Da Cunha, J. Zhou, and M. N. Do, "The nonsubsampling contourlet transform: Theory, design, and applications," *IEEE Trans. Image Process.*, vol. 15, no. 10, pp. 3089–3101, Oct. 2006.
- [38] A. Populis, *Probability, Random Variables and Stochastic Processes*, 3rd ed. New York: McGraw-Hill, 1991.
- [39] M. A. Akhaee, S. M. E. Sahraeian, and F. Marvasti, "Contourlet based image watermarking using optimum detector in a noisy environment," in *Proc. IEEE Int. Conf. Image Processing*, Oct. 2008, pp. 429–432.
- [40] S. G. Chang, B. Yu, and M. Vetterli, "Adaptive wavelet thresholding for image denoising and compression," *IEEE Trans. Image Process.*, vol. 9, no. 9, pp. 1532–1546, Sep. 2000.
- [41] J. A. Dominguez-Molina, G. Gonzalez-Farias, and R. M. Rodriguez-Dagnino, A Practical Procedure to Estimate the Shape Parameter in the Generalized Gaussian Distribution.
- [42] Z. Wang and A. C. Bovik, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.
- [43] Z. Wang and A. C. Bovik, "A universal image quality index," *IEEE Signal Process. Lett.*, vol. 9, no. 3, pp. 81–84, Mar. 2002.
- [44] F. Gembicki and Y. Haimes, "Approach to performance and sensitivity multiobjective optimization: The goal attainment method," *IEEE Trans. Autom. Control*, vol. 20, no. 6, pp. 769–771, Jun. 1975.
- [45] S.-M. Phoong, C. W. Kim, P. P. Vaidyanathan, and R. Ansari, "A new class of two-channel biorthogonal filter banks and wavelet bases," *IEEE Trans. Signal Process.*, vol. 43, no. 3, pp. 649–665, Mar. 1995.
- [46] N. Bi, Q. Sun, D. Huang, Z. Yang, and J. Huang, "Robust image watermarking based on multiband wavelets and empirical mode decomposition," *IEEE Trans. Image Process.*, vol. 16, no. 8, pp. 1956–1966, Aug. 2007.
- [47] S. Chen and H. Leung, "Ergodic chaotic parameter modulation with application to digital image watermarking," *IEEE Trans. Image Process.*, vol. 14, no. 10, pp. 1590–1602, Oct. 2005.
- [48] I. K. Yeo and H. J. Kim, "Generalized patchwork algorithm for image watermarking," *Multimedia Syst.*, vol. 9, no. 3, pp. 261–265, 2003.
- [49] K. Solanki, N. Jacobsen, U. Madhoo, B. S. Manjunath, and S. Chandrasekaran, "Robust image-adaptive data hiding based on erasure and error correction," *IEEE Trans. Image Process.*, vol. 13, no. 12, pp. 1627–1639, Dec. 2004.



Mohammad Ali Akhaee (S'07–M'10) was born in Tehran, Iran, in 1982. He received the B.S. degree in both electronic and communication engineering from the Amirkabir University of Technology and the M.S. degree from the Sharif University of Technology, Tehran, Iran, in 2003 and 2005, respectively. He received the Ph.D. degree from the Sharif University of Technology in 2009.

His research interest includes multimedia security, statistical signal processing, and speech and image processing.



S. Mohammad Ebrahim Sahraeian (S'08) was born in Shiraz, Iran, in 1983. He received the B.S. and M.S. degrees in electrical engineering from the Sharif University of Technology, Tehran, Iran, in 2005 and 2008, respectively. He is currently pursuing the Ph.D. degree in electrical and computer engineering at Texas A&M University, College Station.

His research interests include image and multidimensional signal processing, genomic signal processing, and bioinformatics.



Farokh Marvasti (S'72–M'74–SM'83) received the B.Sc., M.Sc., and Ph.D. degrees, all in electrical engineering, from Rensselaer Polytechnic Institute, Troy, NY, in 1970, 1971, and 1973, respectively.

He was an Associate Professor at the Illinois Institute of Technology, Chicago, during 1987–1991, and from 1992 to 2003, he was an instructor at King's College, London, U.K. He was granted several research grants. Currently, he is a Professor at the Sharif University of Technology, Tehran, Iran. His general research interests lie in signal processing, multiple

access, MIMO techniques, and information theory.