Multimedia Tools and Applications (2019) 78:16887–16906
https://doi.org/10.1007/s11042-018-6879-3

Robust watermarking in curvelet domain for preserving cleanness of high-quality images

Wook-Hyung Kim[1] · Seung-Hun Nam[1] · Ji-Hyeon Kang[1] · Heung-Kyu Lee[1]

Received: 12 December 2017 / Revised: 31 October 2018 / Accepted: 13 November 2018 /
Published online: 2 January 2019

Abstract
Watermarking inserts invisible data into content to protect copyright. The embedded information provides proof of authorship and facilitates the tracking of illegal distribution, etc. Current robust watermarking techniques have been proposed to preserve inserted copyright information from various attacks, such as content modification and watermark removal attacks. However, since the watermark is inserted in the form of noise, there is an inevitable effect of reducing content visual quality. In general, most robust watermarking techniques tend to have a greater effect on quality, and content creators and users are often reluctant to insert watermarks. Thus, there is a demand for a watermark that maintains maximum image quality, even if the watermark performance is slightly inferior. Therefore, we propose a watermarking technique that maximizes invisibility while maintaining sufficient robustness and data capacity to be applied in real situations. The proposed method minimizes watermarking energy by adopting curvelet domain multi-directional decomposition to maximize invisibility and maximizes robustness against signal processing attacks with a watermarking pattern suitable for curvelet transformation. The method is also robust against geometric attacks by employing the watermark detection method utilizing curvelet characteristics. The proposed method showed very good results of a 57.65 dB peak signal-to-noise ratio in fidelity tests, and the mean opinion score showed that images treated with the proposed method were hardly distinguishable from the originals. The proposed technique also showed good robustness against signal processing and geometric attacks compared with existing techniques.

Keywords Content copyright protection · Digital content watermark · Curvelet transform · High-quality content · Blind detection

1 Introduction

With widespread digitalization, anyone can easily copy and distribute content without high cost, but this causes the significant problem of copyright infringement. Therefore, watermarking has

✉ Heung-Kyu Lee
heunglee@kaist.ac.kr

Extended author information available on the last page of the article

emerged as a method to prevent copyright infringement. Invisible copyright information is inserted into the content as noise, so it is not easily noticeable. However, because of the noise form, the watermark degrades content quality. In particular, watermarking methods that are robust against various attacks can significantly degrade image quality due to the high watermark embedding energy. Figure 1 shows that the watermarked image (Fig. 1b) is visually compromised compared with the original image (Fig. 1a). Any reader who can distinguish small image changes, and the actual content producers, would notice this level of degradation, and content producers and users of high-quality content are reluctant to insert watermarks in images. High-resolution and high-quality images, such as ultra-high definition (UHD), have become popular, and image quality has become more important. Consequently, there has been high demand for watermarking technology focusing on image quality rather than robustness and data capacity.

This paper maximizes invisibility by adopting the curvelet domain [6] for watermark embedding. The curvelet transform can decompose an image in more than eight directions, depending on the domain configuration, so it is advantageous to insert a watermark of lower energy. Several studies have previously considered the curvelet domain.

Zhang et al. [26] proposed a method to embed and extract watermarks in the amplitude of curvelet coefficients using quantization index modulation (QIM) [8]. The method was able to detect watermarks blindly and robust against various filter, compression, and noise attacks when the embedded watermark energy was high. However, the approach did not consider curvelet filter characteristics to cut frequency components in a specific direction during curvelet transform; thus, the detection rate was somewhat lower than the embedded watermark energy.

Tao et al. [22] proposed a method for embedding watermarks into the curvelet coefficients using the spread spectrum [9]. The method was capable of blind detection and robust to signal distortion. However, it also failed to consider curvelet filter characteristics; therefore, it also had a lower detection rate than the watermark embedding energy and was vulnerable to geometric attacks, such as image scaling and rotation.

Channapragada et al. [7] proposed a curvelet watermarking method using magic squares. This method resized the watermark to the same size as the image using the magic square method [24] and embedded the resized watermark into the curvelet image using the spread spectrum. The resultant watermark had excellent invisibility and robustness to various attacks, but the method was impractical because it is non-blind and requires the original image to detect the watermark.

Nguyen et al. [17] proposed a method of inserting a watermark after dividing the curvelet coefficients into sub-blocks. After a predetermined number of coefficients of each block are

Fig. 1 Image quality degradation due to watermark embedding: enlarged (**a**) original and (**b**) watermarked image

sampled, a watermark is inserted using a spread spectrum method. This method is robust to signal processing attacks, but is also vulnerable to geometric attacks.

Kim et al. [13] achieved high robustness with low watermarking energy with a watermark design that considered curvelet filter characteristics. However, their method was vulnerable to geometric attacks due to inadequate use of the curvelet coefficient characteristic in the detection process.

Zebbiche et al. [25] proposed a blind watermarking technique that inserts a watermark into the DT-CWT domain and determines the presence of the watermark with the Rao-detector. Although this technique achieves high invisibility by applying new perceptual masking, it is susceptible to some filtering or noise attacks and lacks consideration of geometric attacks.

This paper proposes a watermarking method that maximizes invisibility while maintaining robustness against attacks that occur frequently in real conditions. To achieve this, we adopted a curvelet domain to minimize the watermark embedding energy. However, due to inherent curvelet filter characteristics, watermark signals are distorted in the forward and inverse curvelet transformation processes when a watermark is embedded with conventional watermarking methods. To prevent this, we adopt a particular pattern generation method suitable for curvelets. We also present robust detection methods and templates for geometric attacks.

The paper makes the following contributions:

1. High invisibility that does not significantly impair image quality.
2. Blind watermarking, i.e., the original image is not required for watermark detection.
3. Robustness against various signal attacks with low watermarking energy.
4. Robustness against geometric attacks, such as scaling and rotation.

The remainder of this paper is organized as follows. Section 2 provides a brief introduction of the curvelet transform, and Section 3 discusses the proposed watermarking algorithm. Section 4 presents the experimental results, and Section 5 concludes the paper.

2 Curvelet transform

In contrast to conventional domain watermarking methods, curvelet domain watermarks are distorted during forward and inverse curvelet transform**.** This section provides a brief description of the curvelet domain and explains why the watermark is corrupted during the curvelet transform.

2.1 A brief overview of curvelet transform

Curvelet transform is a multiscale and multi-directional decomposition method that was proposed by Candès [3–6, 15, 16] and designed to compensate for wavelet disadvantages. Curvelets can represent various angles, in contrast to wavelets, and can compensate for not covering all the frequencies as some other directional multiscale decompositions do, such as the Gabor and Ridgelet transform [21]. Curvelet coefficients can be obtained from the inner product of the original image f and a curvelet φ,

$$\begin{aligned} c(j,l,k) = \left\langle f, \varphi_{j,l,k} \right\rangle &= \int_{R^2} f(x)\overline{\varphi_{j,l,k}(x)}dx \\ &= \frac{1}{(2\pi)^2}\int \hat{f}(\omega)\overline{\hat{\varphi}_{j,l,k}(\omega)}d\omega = \frac{1}{(2\pi)^2}\int \hat{f}(\omega)U_j(R_{\theta_l}\omega)e^{i\langle x_k^{(j,l)},\omega\rangle}d\omega, \end{aligned} \tag{1}$$

$$U_j(r,\theta) = 2^{-\frac{3j}{4}} W\left(2^{-j} r\right) V\left(\frac{2^{\left\lfloor \frac{j}{2} \right\rfloor} \theta}{2\pi}\right), \tag{2}$$

where j is a scale parameter; l is a rotation parameter; $k = (k_1, k_2)$ is a translation parameter, with k_1 and k_2 as the curvelet horizontal and vertical axes, respectively; U_j is a wedge-shaped frequency window; R_θ is the rotation operator; r and $\theta_l = 2\pi \cdot 2^{-\lfloor j/2 \rfloor} \cdot l$ are the polar coordinates in the frequency domain; and W and V are the radial and angular windows, respectively.

Figure 2 shows the decomposition of the frequency domain using Eqs. 1 and 2. The frequency is divided into various directions and scales, which simplifies minimizing the watermark embedding energy.

2.2 Problem of watermarking in the curvelet domain

Figure 3 is a diagram of forward curvelet transform. The inverse transform is similar to the forward transform, and the image passes through the curvelet filter in both the forward and inverse transform. The curvelet filter consists of frequency components in a specific direction, as shown in Fig. 4a. On the other hand, watermarks embedded by the spread spectrum and QIM include all the frequency components, as shown in Fig. 4b and c.

The inserted watermark passes through the filter during the curvelet transform, and the frequency components outside the filter are removed. This causes the embedded watermark in the curvelet image to be corrupted during transformation, which reduces the detection rate. A specific watermarking technique for the curvelet domain is required to prevent this corruption.

3 Proposed method

This section describes the proposed watermarking algorithm. Figure 5 shows the proposed embedding and detection process. We designed a watermark pattern that is not damaged during curvelet transformation, and watermark embedding and detection were performed using this pattern.

3.1 Watermark pattern design for the curvelet domain

To address the problems discussed in Section 2.2, we adopt a watermark pattern that undergoes curvelet filtering without distortion. To avoid confusion, $\overline{S}$ is defined as the spatial domain, $\overline{T}$

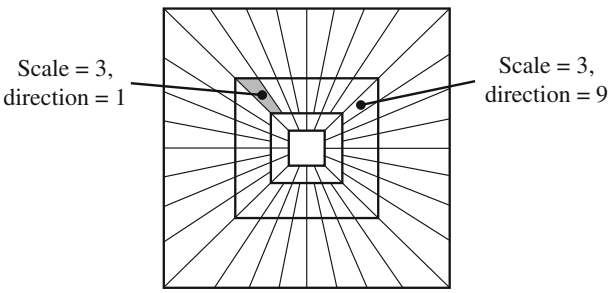


Fig. 2 Frequency spectrum coverage of curvelet transform. The grey shape is a sub-band with scale $j = 3$ and direction $l = 1$

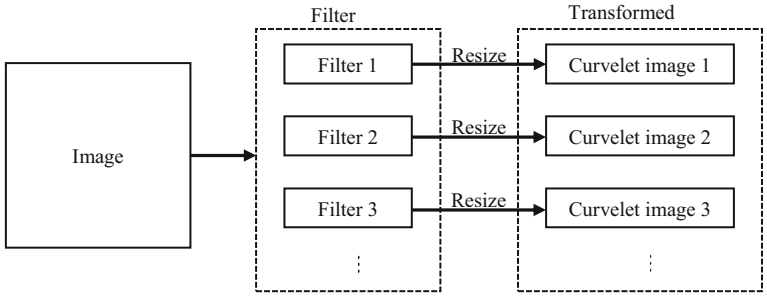


Fig. 3 Diagram of curvelet transform

is the frequency domain of the spatial domain, and $\overline{C}$ is the curvelet domain. $\overline{C}$ is composed of frequency and spatial components, but when the discrete Fourier transform (DFT) is applied, the transformed domain, $\overline{F}$, only includes frequency components. The symbols are summarized in Table 1.

To pass through the curvelet filter without damage, the watermark pattern must be designed using only internal frequencies of the curvelet filter. We present two methods to design such a watermark pattern.

1. **Simultaneous equation**. We solved the simultaneous equation to obtain a watermark pattern incorporating only frequency components inside the curvelet filter

$$\sum_{(u,v)\in A} k_{u,v} \cdot F_{u,v} = W, \tag{3}$$

where k is the DFT coefficient in the $\overline{F}$ domain, $\boldsymbol{F}$ is the inverse DFT matrix from the $\overline{F}$ to the $\overline{C}$ domain, (u, v) is the coordinate of the $\overline{F}$ domain, and $\boldsymbol{A}$ is the set of coordinates inside the curvelet filter on $\overline{F}$ (i.e., the bright part of Fig. 4a). Equation 3 is the same as the inverse discrete Fourier transform (IDFT), but uses limited frequency components. Since this simultaneous equation is overdetermined, there is often no solution, so we find a solution, $\tilde{W}$, that is close to W. This method can insert a watermark in a desired position for a desired embedding method (such as spread spectrum or QIM), but has the disadvantage of requiring significant

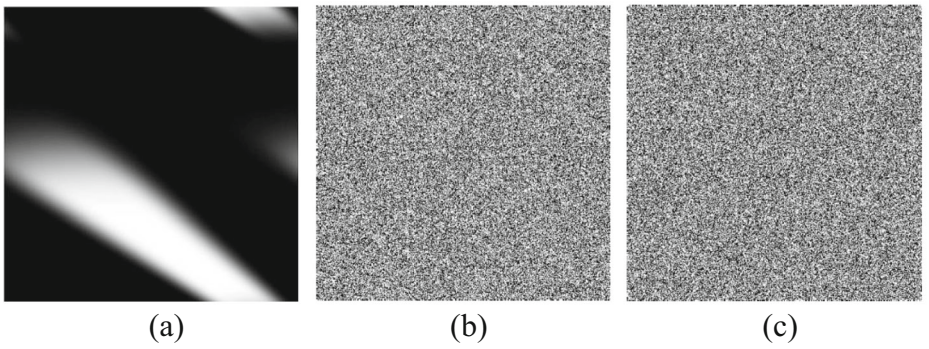


Fig. 4 Frequency components of **a** curvelet filter, **b** spread spectrum watermark, **c** quantization watermark (scale = 3 and direction = 1)

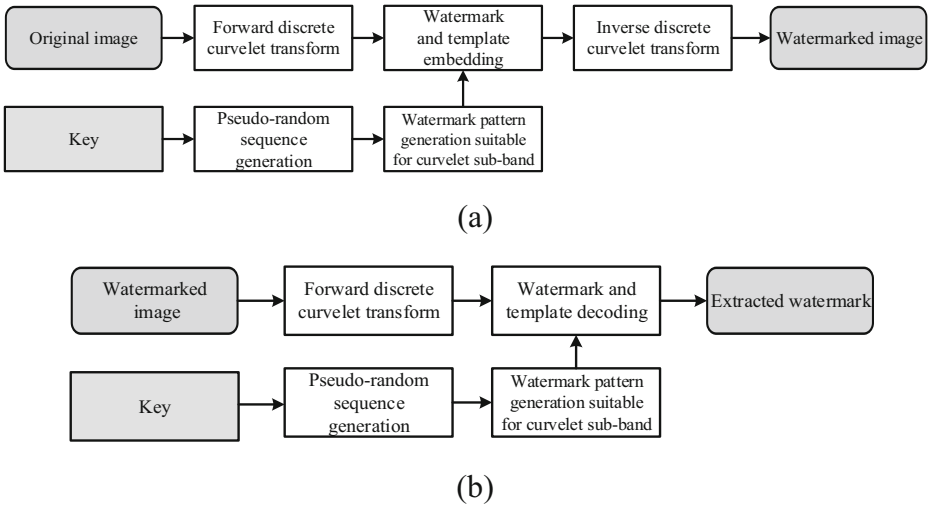


Fig. 5 Proposed curvelet domain watermarking method: **a** embedding and **b** detection procedures

computational overhead. To obtain the watermark pattern following this method, several thousand dimensional simultaneous equations must be solved for a full high-definition image.

2. **Random sequence**. A random sequence is scattered inside the filter of the $\overline{F}$ domain, and the pattern is obtained by applying IDFT to the scattered random sequence. First, a random sequence is generated, equal in length to the number of coordinates in the curvelet filter (i.e., the number of elements in $\boldsymbol{A}$). The generated sequence is then substituted into the curvelet filter in order. Finally, applying IDFT to the sequences generates a watermark pattern that is not corrupted by the curvelet filter. Since the mean value of the generated watermark pattern is approximately 0, only the variance needs to be amplified to 1. This method has the disadvantages of only inserting a watermark using the spread spectrum method and cannot select the watermark position, but it has the advantage of requiring relatively little computation

The first method is impractical due to its high computational complexity. It is also necessary to solve additional problems, such as finding an optimal $\tilde{W}$ similar to W, to minimize the watermark signal being filtered. Therefore, this paper uses the second method for simplicity and practicality.

3.2 Embedding method

Figure 5a shows the watermark embedding process. The original image is transformed into the curvelet domain. A random sequence is generated using the key, and the watermark pattern is

Table 1 Domain symbol definitions

	Spatial domain	Frequency domain of spatial domain	Curvelet domain	Frequency domain of curvelet domain[a]
Symbol	$\overline{S}$	$\overline{T}$	$\overline{C}$	$\overline{F}$

[a] The frequency domain of the curvelet domain is the DFT of $\overline{C}$

generated as described in Section 3.1. The generated watermark pattern is then inserted into the curvelet image using the spread spectrum method [2]. The process can be represented as

$$C'_{s,d}(m,n) = C_{s,d}(m,n) + \alpha \left| C_{s,d}(m,n) \right| W_{s,d}(m,n), \tag{4}$$

where $1 \le m \le i$, $1 \le n \le j$; C is the curvelet coefficient of the original; C 'is a watermarked curvelet coefficient; s and d are the scale and direction, respectively, for the watermark to be inserted; m and n are the horizontal and vertical coordinates, respectively, of the curvelet domain; W is the watermark; i and j are the horizontal and vertical size, respectively, of the curvelet image; and α is the watermark embedding strength.

Equation 4 is for a single scale and direction, and it is possible to embed multiple watermarks by repeating Eq. 4 for various scales and directions. We also embed the template in the other direction, in the same way as the watermark, as shown in Algorithm 1. Algorithm 1 describes a situation where a watermark is inserted into scale 3 and direction 1 and a template is inserted into scale 3 and direction 9. This provides robustness against rotation attacks and explains in detail the role of templates in decoding methods.

Algorithm 1 Rotation template embedding method

Step 1. Select a direction other than the direction in which the watermark is inserted (direction 1).

Step 2. Rotate the template by the difference between the selected direction and direction 1. For example, if direction 9 shown in Fig. 2 is selected, then directions 1 and 9 are 90° apart, so the template is rotated 90°.

Step 3. Insert the rotated template in the selected direction.

3.3 Detection method

Figure 5b shows the watermark detection process. The curvelet transformation is applied to the test image. Then, the watermark pattern is generated and correlated with the curvelet image. When the correlation exceeds a pre-defined threshold value, it is determined that the watermark has been detected. The correlation is expressed as

$$Correlation = \frac{C' \cdot W}{L} = \frac{1}{L} \sum_{m=1}^{i} \sum_{n=1}^{j} C(m,n) W(m,n), \tag{5}$$

where the notation is the same as the embedding process and L is the image size ($i \times j$). Since curvelet coefficients are robust to signal processing attacks, the watermark can be detected after such attacks as noise addition and compression.

However, it is difficult to detect the watermark after geometric distortion because the curvelet coefficients are significantly damaged. For this case, the problem can be solved with an extraction method based on the absolute value of the curvelet coefficients, which are robust to geometric attacks. The most common geometric transformations, scaling and rotation, translate and rotate the embedded watermark, respectively, as shown in Fig. 6. When the image is scaled small, high frequencies are removed, and the watermark spans scales 3 and 4, as shown in Fig. 6b. If the image is rotated, the frequencies rotate together, so the watermark spans directions 1 and 2, as shown in Fig. 6c.

If the image (and hence the watermark) has undergone a scaling attack, the effects are similar to translating an undistorted watermark in the $\overline{F}$ domain, as shown in Fig. 6d and e. Since the watermark is inserted into the $\overline{C}$ domain and $\overline{F}$ is the DFT of $\overline{C}$, DFT translation

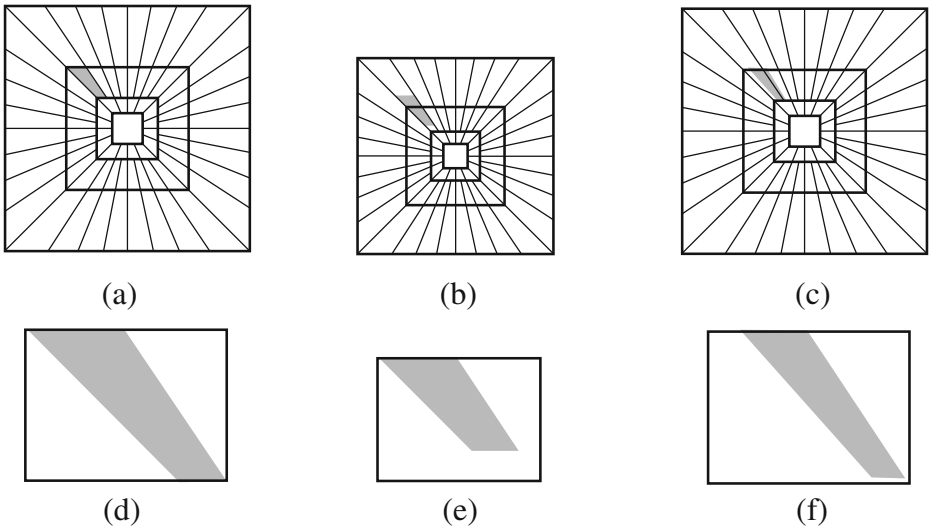


Fig. 6 Different embedded watermark positions by image scaling and rotation; $\overline{T}$ domain: **a** no attack, **b** scaling, **c** rotation; $\overline{F}$ domain: **d** no attack, **e** scaling, **f** rotation

invariance can be exploited. Thus, even if the coefficients are translated in the $\overline{F}$ domain, the coefficient magnitudes in the $\overline{C}$ domain are invariant. Therefore, if the absolute value of the curvelet is applied to Eq. 5, the watermark can be detected even after a scaling attack. Since the image signal and the watermark signal are complex in the $\overline{C}$ domain, the embedded absolute value of watermark W_{abs} is

$$W_{abs} = |C + W| - |C|. \tag{6}$$

However, for blind detection, the original C is not available; thus, C and $|C|$ are unknown in Eq. 6. Therefore, W_{abs} can be estimated as.

$$W_{abs} \simeq \tilde{W}_{abs} = |\overrightarrow{C}^{''}| - |\overrightarrow{C}^{'}| = |\overrightarrow{C}^{'} + \overrightarrow{W}| - |\overrightarrow{C} + \overrightarrow{W}| = |\overrightarrow{C} + 2\overrightarrow{W}| - |\overrightarrow{C} + \overrightarrow{W}|, \tag{7}$$

where $\overrightarrow{C}^{'} = \overrightarrow{C} + \overrightarrow{W}$ and $\overrightarrow{C}^{''} = \overrightarrow{C}^{'} + \overrightarrow{W}$. Figure 7 shows the vectors and absolute values. Since C' and C'' can be obtained in the detection step, W_{abs} can be estimated. The estimated absolute value of the watermark is $0 \le \tilde{W}_{abs} \le W_{abs}$ because the direction of $\overrightarrow{C}$ is distorted by the geometric attack. However, the error due to estimation is within the allowable range, and the watermark can be detected robustly against scaling attack.

Rotation attack can be addressed using a template. The rotation attack rotates the watermark in the $\overline{F}$ domain, as shown in Fig. 6d and f, and the inserted watermark and template undergo the same degree of rotation. Therefore, the degree of rotation can be inferred from the correlation between the watermark embedded direction and the template embedded direction. The correlation between these directions will be larger than the correlation in the other two directions. For example, if the watermark and template are inserted in directions 1 and 9, respectively, a peak will occur at the correlation of these directions. If the image rotates by $360^{\circ}/n_s$, where n_s is the number of directions in scale s, the watermark and template will move to directions 2 and 10, respectively, and a peak will appear at the correlation of directions 2 and 10. Using this information, we can estimate the degree of rotation attack at a resolution of $360^{\circ}/$

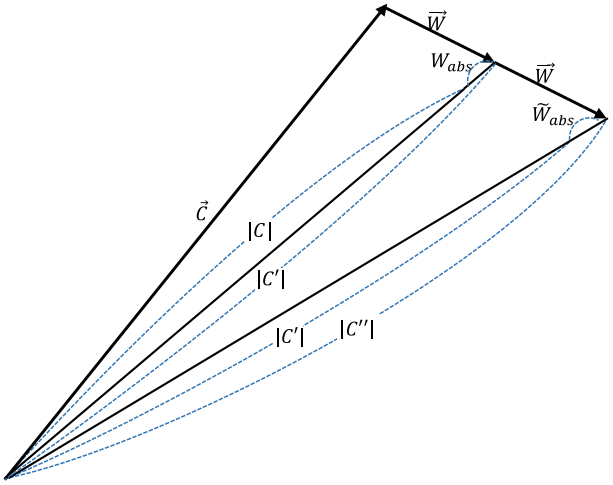


Fig. 7 Estimating the absolute value of the embedded watermark

n_s. Then, the image is inversely rotated the estimated number of degrees and watermark detection is performed using $\tilde{W}_{abs}$. This template decoding method is shown in Algorithm 2.

Algorithm 2 Rotation template decoding method

Step 1. Pairing directions. If the template is inserted with a difference of 8, the paired directions are (1, 9), (2, 10), (3, 11), ….

Step 2. Inversely rotate the second direction of the pair by the difference between the first and second directions of the pair. This is the inverse step of *Step 2* in Algorithm 1.

Step 3. Obtain correlations for all pairs and find the pair with the highest correlation.

Step 4. Rotate the image using information from that pair. For example, if the pair found in step 3 is (3, 11), inversely rotate the image by $360°/n_s \times 2$.

Step 5. Extract the watermark using $\tilde{W}_{abs}$ from the inversely rotated image.

4 Experimental results

This section shows the proposed method's invisibility and robustness to various attacks. The test image sets were obtained from the Heinrich Hertz Institute [11], Microsoft Research 3D Video Datasets [27], and Middlebury [12, 18–20]. The test sets consisted of approximately 800 images with resolutions from 720×576 to 1800×1500. Figure 8 shows typical example images. We then compared the proposed method with Tao's [22], Zebbiche's [25], Zhang's [26], and Nguyen's [17] blind curvelet domain watermarking techniques. We also compared it with Makbol's method [14], a watermarking technique that uses discrete wavelet transform-singular value decomposition.

Tao's method is a zero-bit watermarking method that uses a spread spectrum, and the watermark is inserted into only one wedge. For a fair comparison, the proposed method also inserted a watermark into only one wedge, and we have labeled these results Proposed-c. In both methods, the watermark was inserted into the first wedge among 32 wedges of scale 3, and the template for the proposed method was inserted into the 9th wedge.

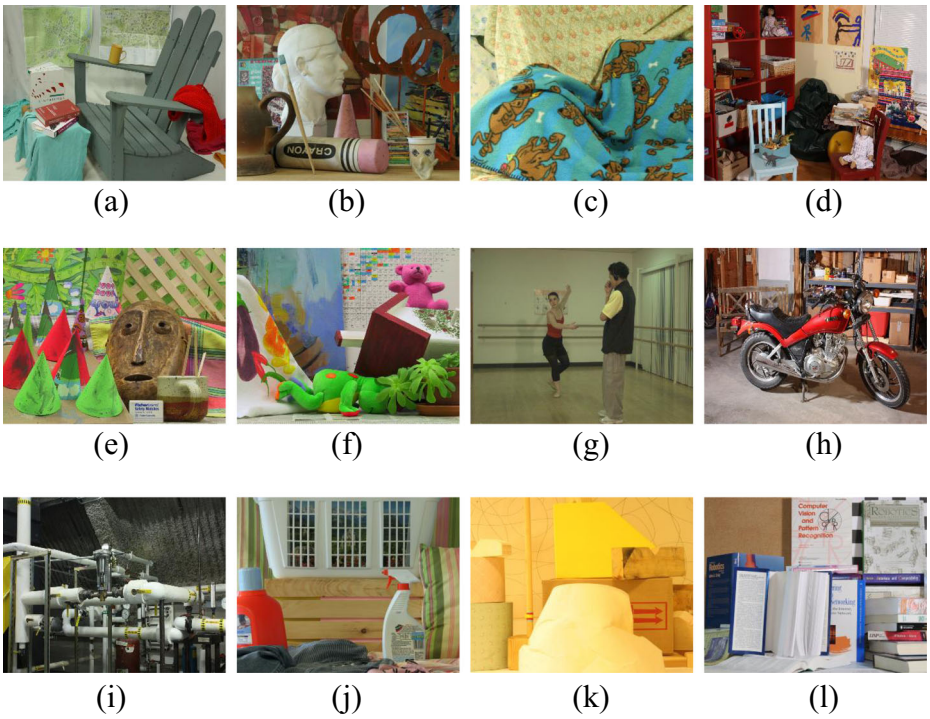


Fig. 8 Example test sets: **a** Adirondack, **b** Art, **c** Cloth, **d** Playroom, **e** Cones, **f** Teddy, **g** Ballet, **h** Motorcycle, **i** Pipes, **j** Laundry, **k** Lampshade, **l** Books

Zebbiche's method is also a zero-watermarking technique. However, this technique inserts a watermark in the DT-CWT domain and measures the watermark response using a Rao-detector instead of a correlation. To adjust the response's scale to a level similar to the correlation, we adjusted the overall scale so that the fake watermark response is equal to the fake watermark correlation.

Zhang's method is a multi-bit watermark that uses a QIM method, inserts one bit per wedge, and uses six wedges to insert a total of six bits. For a fair comparison, the proposed method also inserted watermarks in six wedges, and we have labeled these results Proposed-m. In both methods, the watermark was inserted into wedges 1–3 and 6–8 among the 32 wedges of scale 3, and the template for the proposed method was inserted into the 9th wedge. In the proposed method, a direct message coding method [10] was used to insert and detect bits using the spread spectrum method.

Nguyen's and Makbol's methods were also set to have the same bit capacity as other watermarking methods. Nguyen's method inserted a watermark at scales 3 and 1 of the curvelet coefficients and divided the coefficients into six sub-blocks. Makbol's method divided the low-low band of the DWT into 24 sub-blocks and selected six sub-blocks for inserting the watermark.

4.1 Invisibility test

Figure 9a and b shows typical original and watermarked images. The quality difference can hardly be distinguished by the eye. Figure 9c shows the difference between the watermarked

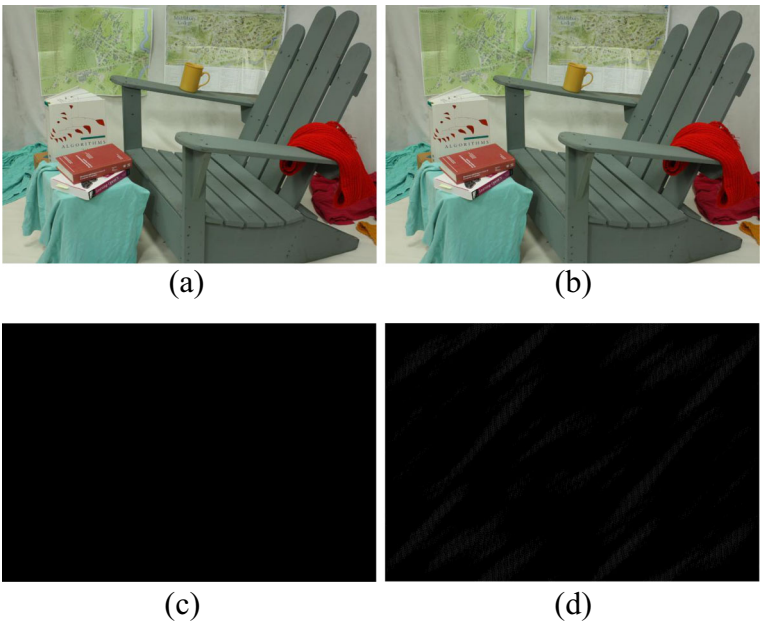


Fig. 9 Original and watermarked images: **a** original image, **b** watermarked image, **c** subtraction of original and watermarked images, **d** contrast-enhanced subtraction image

and original image and Fig. 9d applies 50× the contrast to Fig. 9c. The maximum pixel intensity difference between the watermarked and original image was only 2, which is unnoticeable without increasing the contrast.

We also tested invisibility subjectively and objectively. Subjective assessments were measured by the mean opinion score (MOS), and objective assessments were measured by the peak signal-to-noise ratio (PSNR) and structural similarity (SSIM) [23]. MOS was measured by 10 image/watermark experts using the double-stimulus continuous quality-scale method (ITU-R [1]) with the experimental environment of a 49-in. UHD TV (model 49UF8570).

Table 2 shows that the MOS of the proposed method is superior to that of previous works. In particular, the Proposed-c method had a near-perfect score (4.9), which means it was difficult to distinguish between the original and watermarked images. Table 3 shows that for the objective assessments, PSNR and SSIM, the proposed method was more invisible than previous methods. In particular, the Proposed-c exhibited very high invisibility of >57 dB PSNR. The SSIM of Proposed-c was also the highest, so the structure of the image was best-preserved. In the multi-bit watermarking method, Proposed-m also showed better results than Zhang's, Makbol's, and Nguyen's methods, which were the same multi-bit watermarking methods, in the subjective and objective invisibility evaluations.

Table 2 Average MOS

	Proposed-c	Tao [22]	Zebbiche [25]	Proposed-m	Zhang [26]	Makbol [14]	Nguyen [17]
MOS	4.9	4.8	4.8	4.6	4.4	4.3	4.3

Table 3 Average PSNR and SSIM

	Proposed-c	Tao [22]	Zebbiche [25]	Proposed-m	Zhang [26]	Makbol [14]	Nguyen [17]
PSNR	57.65	56.47	56.91	51.76	49.18	51.07	51.41
SSIM	0.9984	0.9977	0.9979	0.9946	0.9807	0.9939	0.9944

4.2 Robustness to signal distortion

Figure 10 shows the robustness of Proposed-c, Tao's and Zebbiche's methods, which are zero-bit watermarking methods, for signal distortion. The results of Proposed-c, Tao's and Zebbiche's methods showed the average response value between the watermarked images and "True" watermark. The "Fake" showed the highest correlation value among the correlation between 1000 fake watermarks and watermarked

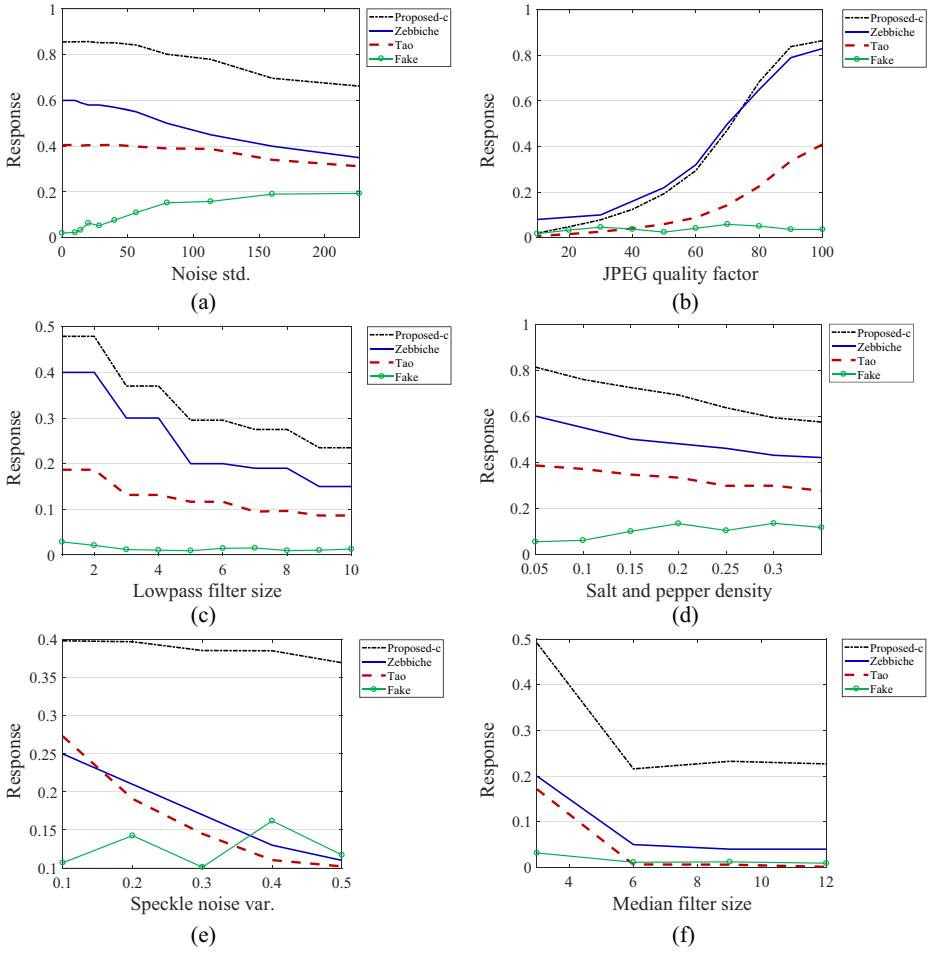


Fig. 10 Robustness of Proposed-c, Tao's and Zebbiche's methods to signal distortion: **a** Gaussian noise addition, **b** JPEG compression, **c** low-pass filtering, **d** salt and pepper noise addition, **e** speckle noise addition, and **f** median filtering

Table 4 Robustness of Proposed-c and Tao's methods to histogram equalization

	Proposed-c	Tao [22]	Zebbiche [25]	Fake
Watermark response	2.95	1.40	2.46	0.09

images. As the results show, Proposed-c was robust to compression, filtering, and several noise additions. The correlation of Proposed-c was almost twice that of Tao's method. In addition, Proposed-c also showed high robustness against histogram equalization, as shown in Table 4. The watermark was inserted by the same spread spectrum method, but the proposed method was more robust against signal distortion because it was not damaged by the curvelet filter. Zebbiche's method shows the best performance in JPEG, but shows slightly weaker results in other signal distortions.

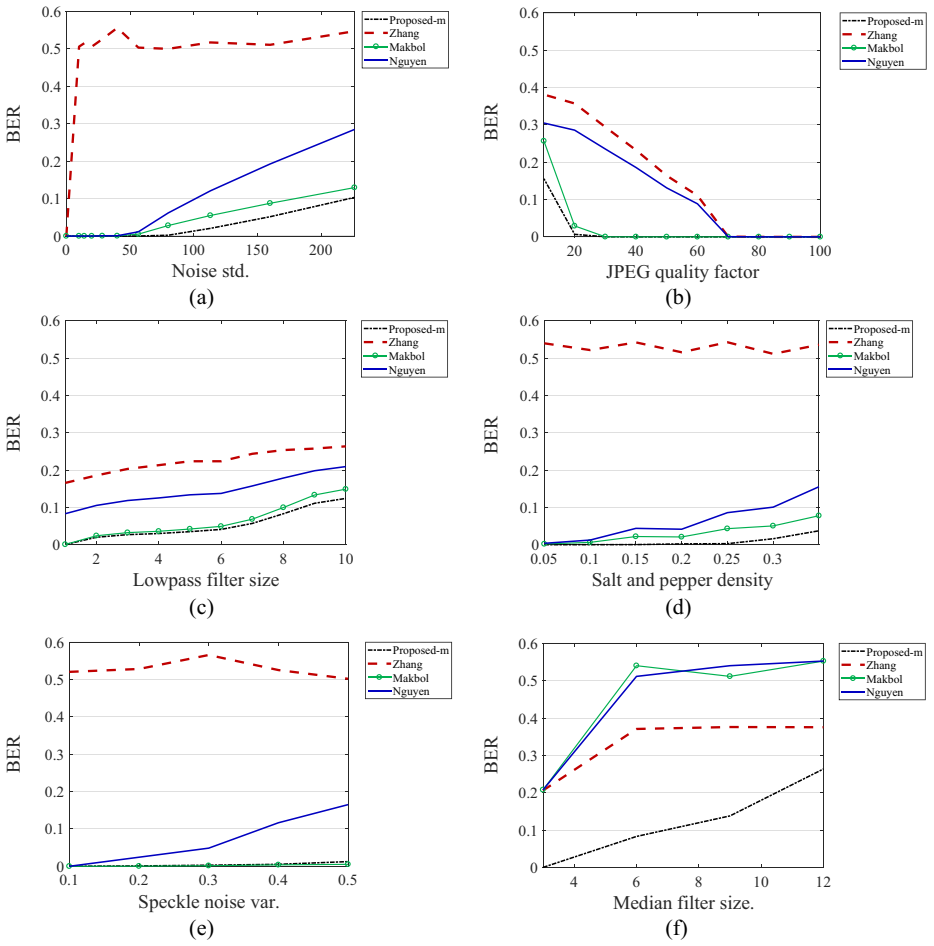


Fig. 11 Robustness of Proposed-m, Zhang's, Makbol's, and Nguyen's methods to signal distortion: **a** Gaussian noise addition, **b** JPEG compression, **c** low-pass filtering, **d** salt and pepper noise addition, **e** speckle noise addition, and **f** median filtering

Table 5 Robustness of Proposed-m, Zhang's, Makbol's, and Nguyen's methods to histogram equalization

	Proposed-m	Zhang [26]	Makbol [14]	Nguyen [17]
BER	0.02	0.38	0.04	0.02

Figure 11 shows the robustness of the Proposed-m and Zhang's methods, which are multi-bit watermarking methods, for signal distortion. Robustness was measured using the bit error rate (BER), which is defined as

$$BER = \frac{b_e}{b_c + b_e} = \frac{b_e}{b_t}, \tag{8}$$

where b_e is the number of error bits, b_c is the number of correctly decoded bits, and b_t is the total number of decoded bits. Zhang's method exhibited significantly higher BER than the Proposed-m method. In particular, Zhang's method showed vulnerability to Gaussian and salt and pepper noise attacks. This is because the coefficient impairments from curvelet filtering and the quantization step were relatively low compared with the noise size. In addition, Makbol and Nguyen's methods showed weaknesses in median filtering, but the proposed method showed robustness in median filtering.

As shown in Table 5, Zhang's method was also vulnerable to histogram adjustments. This is because the step size of the quantized coefficients was modified during histogram equalization. However, since there was no information on the modified step size in the decoding step, the bits could not be decoded correctly. On the other hand, the proposed method, Makbol's method, and Nguyen's method could detect the bits reliably even after the histogram equalization attack. This is because the correlation method and the magnitude comparison method of coefficients were robust to histogram equalization.

4.3 Robustness to geometric distortion

Figures 12 and 13 show the robustness of Proposed-m, Tao's, Zebbiche's, Zhang's, Makbol's, and Nguyen's methods to scaling and rotation. Tao's method used a complex number of curvelet coefficients vulnerable to geometric attacks; therefore, it was not robust against geometric attacks. In contrast, Zhang's method exhibited high robustness to geometric attacks, since the watermark was inserted into the absolute value of the curvelet coefficients, which were less deformed in geometric attacks. Proposed-m also exhibited high robustness against

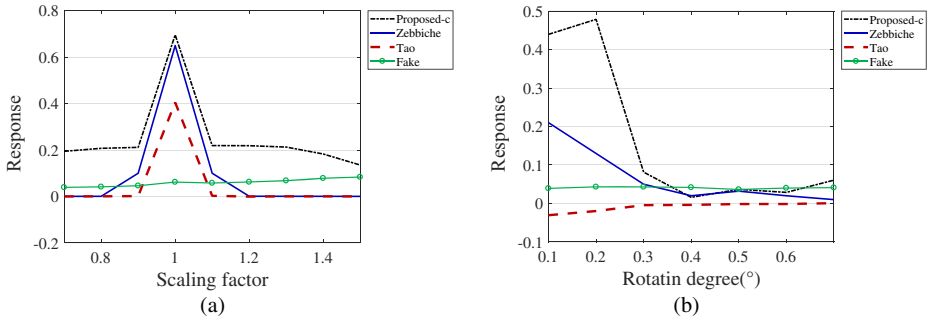


Fig. 12 Robustness of Proposed-c, Tao's and Zebbiche's methods to geometric distortion: **a** scaling and **b** rotation

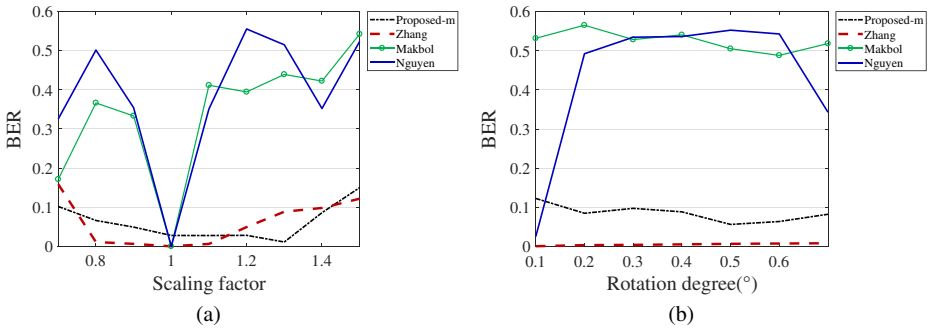


Fig. 13 Robustness of Proposed-m, Zhang's, Makbol's, and Nguyen's methods to geometric distortion: **a** scaling and **b** rotation

geometric attacks and would be sufficient for practical use. However, Zebbiche, Makbol and Nguyen's methods showed vulnerability to geometric attacks because these methods did not take into account the geometric attacks.

Larger rotations can be addressed using the proposed template method. The template was inserted at scale 3, which was composed of 32 directions. Therefore, image rotation can be detected at a resolution of 360°/32 = 11.25°. Figure 14a shows that template accuracy was low where the template spanned two directions (e.g. 5.625°, 16.875°, 28.125°, …). If the "True" range was expanded to the spanned direction, it showed high accuracy in all sections, as shown in Fig. 14b. After restoring the image with resolution 11.25° using the template, the watermark could be found through a heuristic search, which requires an acceptable amount of computation to detect the watermark.

However, it is still impossible for the proposed method to cope with all geometric attacks. The proposed watermark is easily damaged by geometric attacks, such as affine transformation attacks and image cropping, so additional research is needed.

4.4 Visual results of extracted watermark

Figure 15 shows the visual results of the extracted watermark. We used "Adirondack" to show the results, and since the correlation-based methods cannot be shown as visual results, we only show visual results for the multi-bit methods.

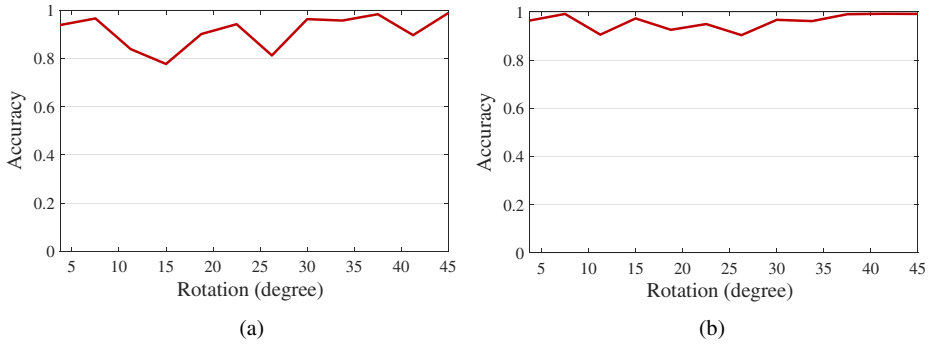


Fig. 14 Template accuracy against rotation attacks: **a** True only if the template embedded direction is exactly found or **b** the "True" range is expanded to the spanned direction

	Proposed-m	Zhang	Makbol	Nguyen
No attack				
Noise (std. 110)				
JPEG (quality factor 20)				
Low-pass filter (3×3)				
Salt and pepper (density 0.25)				
Speckle noise (variance 0.4)				
Median filtering (6×6)				
Scaling (factor 0.8)				
Rotation (0.5 degrees)				

Fig. 15 Visual results comparison of the extracted watermark for "Adirondack"

5 Conclusions

This paper proposed a blind watermarking technique based on curvelet transformation. Watermarking techniques have been widely applied to protect copyright, but quality degradation is inevitable, and many people are reluctant to embed watermarks. To overcome these shortcomings of watermarking, the proposed watermarking method minimizes quality degradation and maximizes invisibility using the curvelet domain while maintaining robustness against various attacks. With a watermark generation technique suitable for curvelets, the proposed method maximizes robustness against signal processing attacks with low watermarking energy, and robustness against scaling and rotation was obtained by a template and watermark detection method using the absolute value of curvelet coefficients. The experimental results showed that the proposed method's invisibility was superior to that of previous methods and its robustness against signal and geometric attacks was reliable and suitable for real-world applications. However, additional research is needed because it is not yet possible to deal with affine attacks, such as shearing, and geometric attacks, such as image cropping. Furthermore, the number of scales and directions of the curvelet used in the proposed method was determined by intuition, which is not the best method. This also needs to be supplemented. A future study will expand this research into video content, minimizing video quality degradation due to embedding watermarks while maintaining robustness to video compression and various other attacks that occur in the video environment.

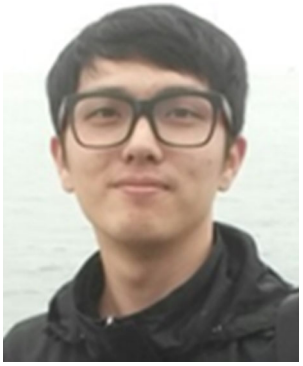
Acknowledgements This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT)

References

1. ASSEMBLY, ITU Radiocommunication (2003) Methodology for the subjective assessment of the quality of television pictures. International telecommunication Union, Geneva
2. Barni M, Bartolini F, Cappellini V, Piva A (1998) A DCT-domain system for robust image watermarking. Signal Process 66(3):357–372
3. Candès EJ, Donoho DL (2000) Curvelets: a surprisingly effective nonadaptive representation for objects with edges. Stanford Univ Ca Dept of Statistics, California
4. Candès EJ, Donoho DL (2004) New tight frames of curvelets and optimal representations of objects with piecewise C2 singularities. Commun Pure Appl Math 57(2):219–266
5. Candès EJ, Guo F (2002) New multiscale transforms, minimum total variation synthesis: applications to edge-preserving image reconstruction. Signal Process 82(11):1519–1543
6. Candès E, Demanet L, Donoho D, Ying L (2006) Fast discrete curvelet transforms. MMS 5(3):861–899
7. Channapragada RSR, Prasad MV (2015) Watermarking techniques in curvelet domain. In: Channapragada RSR, Prasad MVNK (eds) Computational intelligence in data mining-Volume 1 (pp 199–211). Springer, New Delhi
8. Chen B, Wornell GW (2001) Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. IEEE Trans Inf Theory 47(4):1423–1443
9. Cox IJ, Kilian J, Leighton FT, Shamoon T (1997) Secure spread spectrum watermarking for multimedia. IEEE Trans Image Process 6(12):1673–1687
10. Cox I, Miller M, Bloom J, Fridrich J, Kalker T (2007) Digital watermarking and steganography. Morgan Kaufmann, Burlington
11. Fehn C (2004) Depth-image-based rendering (DIBR), compression, and transmission for a new approach on 3 D-TV. *Proc SPIE* 5291(2):93–104
12. Hirschmuller H, Scharstein D (2007) Evaluation of cost functions for stereo matching. IEEE 2007 conference on computer vision and pattern recognition, 1–8
13. Kim WH, Nam SH, Lee HK (2017) Blind curvelet watermarking method for high-quality images. Electron Lett 53(19):1302–1304
14. Makbol NM, Khoo BE, Rassem TH (2016) Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. IET Image Process 10(1):34–52
15. Nayak DR, Dash R, Majhi B, Prasad V (2017) Automated pathological brain detection system: a fast discrete curvelet transform and probabilistic neural network based approach. Expert Syst Appl 88:152–164
16. Nayak DR, Dash R, Majhi B (2018) Pathological brain detection using curvelet features and least squares SVM. Multimed Tools Appl 77(3):3833–3856
17. Nguyen SC, Ha KH, Nguyen HM (2015) An improved image watermarking scheme using selective curvelet scales. In Advanced Technologies for Communications (ATC), 2015 International conference on (pp 445–450). IEEE
18. Scharstein D, Pal C (2007) Learning conditional random fields for stereo. IEEE 2007 conference on computer vision and pattern recognition, 1–8
19. Scharstein D, Szeliski R (2003) High-accuracy stereo depth maps using structured light. IEEE 2003 computer society conference on computer vision and pattern recognition, 1, I-I
20. Scharstein D, Hirschmüller H, Kitajima Y, Krathwohl G, Nešić N, Wang X, Westling P (2014) High-resolution stereo datasets with subpixel-accurate ground truth. German conference on pattern recognition, 31–42
21. Sumana IJ, Islam MM, Zhang D, Lu G (2008) Content based image retrieval using curvelet transform. IEEE 10th workshop on multimedia signal processing, 11–16
22. Tao P, Dexterb S, Eskicioglub AM (2008) Robust digital image watermarking in curvelet domain. Methods 14:15
23. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 13(4):600–612
24. Xie T, Kang L (2003) An evolutionary algorithm for magic squares. *IEEE 2003 Congress on*. Evol Comput 2:906–913
25. Zebbiche K, Khelifi F, Loukhaoukha K (2018) Robust additive watermarking in the DTCWT domain based on perceptual masking. Multimed Tools Appl 77:1–24
26. Zhang C, Cheng LL, Qiu Z, Cheng LM (2008) Multipurpose watermarking based on multiscale curvelet transform. TIFS 3(4):611–619
27. Zitnick CL, Kang SB, Uyttendaele M, Winder S, Szeliski R (2004) High-quality video view interpolation using a layered representation. ACM Trans Graph 23(3):600–608

Wook-Hyung Kim received his B.S. degree in electrical engineering from Hanyang University, Seoul, Korea in 2012, and M.S. degree in electrical engineering from Korea Advanced Institute of Science and Technology (KAIST), Daejon, Republic of Korea in 2014. He is currently working toward his Ph.D. degree in Multimedia Computing Lab., School of Computing, KAIST. His current research interest include multimedia security.

Seung-Hun Nam is received the B.S. degree in Information Communication Engineering from Dongguk University, Seoul, Republic of Korea, in 2013, and the M.S. degree in School of Computing from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Republic of Korea, in 2015. He is currently pursuing the Ph.D. degree in Multimedia Computing Lab., School of Computing, KAIST. His research interest include digital watermarking and image forensics.



Ji-Hyeon Kang is received the B.S. degree in school of computer science and electrical engineering from Handong University, Pohang, Republic of Korea, in 2015, and the M.S. degree in School of Computing from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Republic of Korea, in 2017. He is currently pursuing the Ph.D. degree in Multimedia Computing Lab., School of Computing, KAIST. His research interest include digital watermarking and 360 spherical panorama image.

Heung-Kyu Lee received a BS degree in electronics engineering from Seoul National University, Seoul, Korea, in 1978, and MS and PhD degrees in computer science from Korea Advanced Institute of Science and Technology, Korea, in 1981 and 1984, respectively. Since 1986 he has been a professor in the Department of Computer Science, KAIST. He has authored/coauthored over 200 international journal and conference papers. He has been a reviewer of many international journals, including Journal of Electronic Imaging, Real-Time Imaging, and IEEE Trans. on Circuits and Systems for Video Technology. His major interests are digital watermarking, digital fingerprinting, and digital rights management.

Affiliations

Wook-Hyung Kim [1] · Seung-Hun Nam [1] · Ji-Hyeon Kang [1] · Heung-Kyu Lee [1]

Wook-Hyung Kim
whkim@mmc.kaist.ac.kr

Seung-Hun Nam
shnam@mmc.kaist.ac.kr

Ji-Hyeon Kang
jhkang@mmc.kaist.ac.kr

[1] School of Computing, Korea Advanced Institute of Science and Technology, 291 Daehak-ro Yuseong-gu, Daejeon 34141, Republic of Korea