Robust copyright protection scheme for digital images using the low-band characteristic

Der-Chyuan Lou
Hao-Kuan Tso
Jiang-Lung Liu
National Defense University
Chung Cheng Institute of Technology
Department of Electrical Engineering
Tahsi, Taoyuan 33509, Taiwan
E-mail: dclou@ccit.edu.tw

Abstract. A copyright protection technique without using the original image in the process of copyright verification is demanded in most applications. In addition, robustness, imperceptibility, security, and unambiguity are also essential requirements for a copyright protection technique. In this paper, a robust copyright protection scheme for digital images, based on the low-band characteristic, is proposed to meet these requirements. Experimental results show that the proposed scheme not only can clearly verify the copyright of the digital images, but also is more robust than existing schemes against several attacks such as JPEG lossy compression, noise adding, sharpening, and blurring. *© 2006 Society of Photo-Optical Instrumentation Engineers.* [DOI: 10.1117/1.2361166]

Subject terms: copyright protection; blindness; robustness; discrete wavelet transform.

Paper 050818RR received Oct. 12, 2005; revised manuscript received Mar. 7, 2006; accepted for publication Mar. 17, 2006; published online Oct. 30, 2006.

1 Introduction

Due to rapid development of the internet and multimedia techniques, duplication and distribution of digital multimedia has become easier than before. Recently, the issue of copyright protection has been widely discussed in multidisciplinary fields. Digital signatures and digital watermarking are two common techniques used to protect the copyright of digital data. However, because it is time-consuming to generate signatures,[1] they can hardly be applied to digital multimedia (such as image, video, and audio), because such media contain much larger amounts of information than text, and also because extra bandwidth is required for transmitting the signature. On the other hand, a digital watermark, which can be embedded into digital multimedia, is a more effective way to protect the copyright of digital multimedia and can be used to compensate the shortcomings of digital signatures. When a dispute happens, the embedded watermark can be retrieved to verify the copyright of digital multimedia.

For digital multimedia, a copyright protection technique should meet several requirements, including robustness, imperceptibility, security, blindness, and unambiguity.[1,2] However, almost no proposed copyright protection techniques can meet all these requirements at the same time. For example, a well-known robust technique proposed by Cox et al.[3] applies a spread-spectrum scheme to embed a watermark into the 1000 highest ac coefficients. Although the scheme strikes a good balance between robustness and imperceptibility, it has the defect that extracting the watermark needs the original image. Thus, extra space is required to store the original image.

Many researchers have proposed other copyright protection techniques to try to satisfy the preceding requirements. However, many proposed schemes[2–14] modify some pixels or coefficients of an image, which reduces the image quality. Hence, lossless data-hiding techniques have attracted lots of attention,[15,16] and have been applied in medicine and satellite imagery. Recently, Chen et al.[1] proposed a wavelet-based copyright protection technique. Their scheme is secure and robust to some attacks. Moreover, the logo retrieval does not require the original image. However, when the protected image suffers from some serious attacks, such as mixing cropping with scaling, the quality of the retrieved logo can be substantially degraded.

In this paper, a robust copyright protection scheme using the low-band characteristic in the transform domain is proposed. The proposed scheme not only can clearly verify the copyright of digital images, but also is robust against various image-processing attacks.

The rest of the paper is organized as follows. Section 2 briefly describes the concepts of the discrete wavelet transform (DWT) and torus automorphism, both of which belong to the core of the proposed scheme. Section 3 introduces the proposed scheme. The experimental results are shown in Sec. 4. Finally, conclusions are drawn in Sec. 5.

2 Discrete Wavelet Transform and Torus Automorphism

In this paper, two techniques, called the discrete wavelet transform (DWT) and torus automorphism, are adopted in our proposed scheme. We briefly described both techniques in the following subsections.

2.1 *Discrete Wavelet Transform*

The DWT has been widely used in various fields, such as image processing and electrical engineering. Its basic concept is described as follows. An image is first decomposed into four subbands, LL1, LH1, HL1, and HH1. The subband LL1 represents most of the energy of an image. The subbands LH1, HL1, and HH1 represent its detailed information. The subband LL1 can be further decomposed into four subbands LL2, LH2, HL2, and HH2. Likewise, the subband LL2 can be further decomposed into four sub-

0091-3286/2006/$22.00 © 2006 SPIE

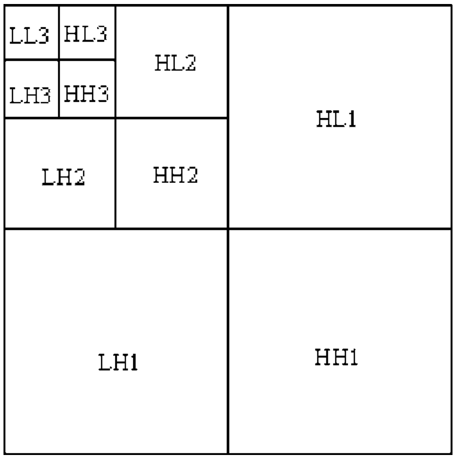


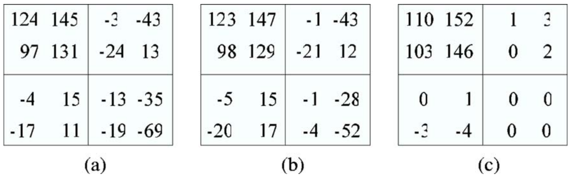
Fig. 1 Three-level wavelet decomposition of an image.

bands LL3, LH3, HL3, and HH3. Generally, LL3 is the low band, HL1, LH1, and HH1 are high bands, and the other subbands are intermediate in frequency. Figure 1 shows an example of the three-level DWT decomposition of an image.

Generally, lossy compression techniques compress an image by decreasing the energy of the high band. Figure 2 shows an example. The original image [shown as Fig. 2(a)] is first compressed by using JPEG compression. Figure 2(b) and 2(c) show the results of compression with quality factors 90 and 10. We notice that every subband coefficient changes greatly except those of the LL1 subband, which change only slightly. In other words, the low-band coefficients are more robust than the high-band ones. Hence, the proposed scheme will utilize the low-band characteristic to generate a secret image.

2.2 *Torus Automorphism*

In recent years, chaotic maps have been used for digital watermarking to increase the security.[7,12–14] A chaotic map can be considered as assigning a special state to each time point, the state changing with time. Moreover, each state is determined by the previous state.[7] The important features of a chaotic map, including its sensitivity to initial conditions and its mixing (confusion and diffusion) property, make it an excellent candidate for watermarking and encryption.[13,17] A well-known chaotic map technique, called torus automorphism,[12] can be described by the following equation:



124	145	-3	-43
97	131	-24	13
-4	15	-13	-35
-17	11	-19	-69

(a)

123	147	-1	-43
98	129	-21	12
-5	15	-1	-28
-20	17	-4	-52

(b)

110	152	1	3
103	146	0	2
0	1	0	0
-3	-4	0	0

(c)

Fig. 2 Example of an image compressed with quality factors 90 and 10.

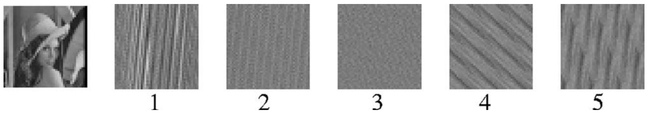


Fig. 3 Example of an image scrambled five times by torus automorphism.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod M, \tag{1}$$

where (x,y) and (x',y') denote the pixel locations before and after the transformation; a_1, a_2, a_3, and a_4 are the secret keys $(a_1,a_2,a_3,a_4 \in Z)$, and M denotes the size of an image.

We say that the equation has period T if the pixel at location (x,y) returns to its original location after being transformed T times. When the pixel location (x,y) has been transformed K times, we can make the resulting pixel at (x',y') return to its original location (x,y) by applying Eq. (1) $T-K$ times. Figure 3 shows an example of an image scrambled five times.

From the encryption perspective, if K represents an encryption key, then $T-K$ can be considered as a decryption key. When the equation and modulus M are known, the period can be determined by an exhaustive search.[7]

3 The Proposed Scheme

In general, the low frequencies are the most important component of an image that can survive common attacks. However, embedding information into low frequency will reduce the image quality. Based on the observation of Fig. 2, we propose a robust copyright protection scheme that does not embed information in an image.

3.1 *Secret Image Generation*

The original image X is a gray-level image with M by N pixels. The logo W is a binary image with O by$P$ pixels. They are defined as follows:

$$X = \{x(i,j) | 0 \le i \le M-1,\ 0 \le j \le N-1, \\ 0 \le x(i,j) \le 255\}, \tag{2}$$

$$W = \{w(l,m) | 0 \le l \le O-1,\ 0 \le m \le P-1, \\ w(l,m) \in [0,1]\}. \tag{3}$$

First, the original image and the logo are scrambled. Then we transform the scrambled image into wavelet coefficients and extract the feature value. Finally, the feature

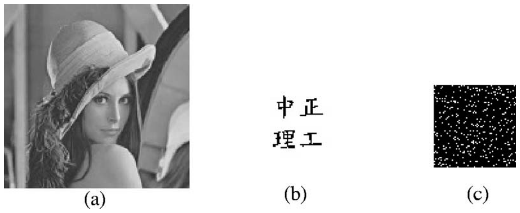
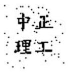
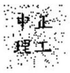
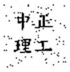


Fig. 4 (a) The test image, (b) the logo, and (c) the secret image.

Table 1 The experimental results under JPEG, noise addition, and blurring attacks.

	JPEG	Noise addition	Blurring
Attacked image			
PSNR	26.29	10.25	22.6
Retrieved logo			
NC	0.98	0.95	0.97

value is combined by an exclusive-OR (XOR) operation with the scrambled logo. The detailed steps are as follows.

Step 1. Utilize torus automorphism and secret keys (a_1, a_2, a_3, a_4, and K) to scramble the original image X and logo W:

$$X_s = \text{scramble}(X), \tag{4}$$

$$W_s = \text{scramble}(W). \tag{5}$$

Step 2. Decompose the scrambled image X_s into several subbands using l-level DWT.
Step 3. Extract the LLn subband, and generate a new LLn subband with predefined threshold value, i.e.,

$$\mathrm{LL}n_{\text{new}}(i,j) = \begin{cases} 1 & \text{if } \mathrm{LL}n(i,j) > T_1, \\ 0 & \text{if } \mathrm{LL}n(i,j) \leq T_1, \end{cases} \tag{6}$$

where T_1 represents the predefined threshold value and $T_1 = \sum_{i=1}^{M/2^l} \sum_{j=1}^{N/2^l} \mathrm{LL}n(i,j)/(M/2^l) \times (N/2^l)$.
Step 4. Divide the new LLn subband into nonoverlapping $B \times B$ blocks, and compute the sum of all blocks, i.e.,

$$\mathrm{LL}n_{\text{new}}(m,n) = \sum_{i}^{B} \sum_{j}^{B} \mathrm{LL}n_{\text{new}}(i,j). \tag{7}$$

Step 5. Generate the feature value using the following equation:

Table 2 The experimental results under sharpening, scaling, and cropping attacks.

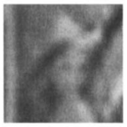
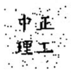
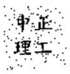
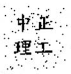
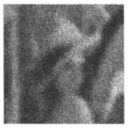
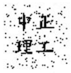
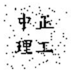
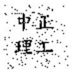
	Sharpening	Scaling	Cropping
Attacked image			
PSNR	16.31	19.03	11.2
Retrieved logo			
NC	0.98	0.97	0.97

Table 3 The experimental results under mixed attacks.

	Blurring+noise addition	Blurring+sharpening +JPEG	Scaling+cropping
Attacked image			
PSNR	18.29	16.88	15.03
Retrieved logo			
NC	0.96	0.97	0.96

$$f(m,n) = \begin{cases} 1 & \text{if } \mathrm{LL}n_{\text{new}}(m,n) \geq T_2, \\ 0 & \text{if } \mathrm{LL}n_{\text{new}}(m,n) < T_2, \end{cases} \tag{8}$$

where T_2 represents the predefined threshold value.
Step 6. Perform the XOR operation between the feature value and the scrambled logo to obtain the secret image according to

$$s(m,n) = f(m,n) \oplus w_s(m,n), \tag{9}$$

where $\oplus$ denotes the XOR operation.
Step 7. Register the secret image S and these generated keys to the trusted third party.

3.2 *Copyright Verification*

These registered keys are used to achieve the verification process. The detailed steps are similar to the secret image generation process, as follows:

Step 1. Utilize torus automorphism and secret keys (a_1, a_2, a_3, a_4, and T) to scramble the suspected image X':

$$X_s' = \text{scramble}(X'). \tag{10}$$

Step 2.Decompose the image X_s' into several subbands using l-level DWT.
Step 3. Extract the LL$'n$ subband, and generate the new LL$'n$ subband with the predefined threshold value, i.e.,

Table 4 The experimental results under print-photocopy-scan, rotation, and special attacks.

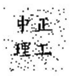
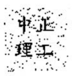
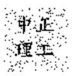
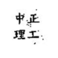
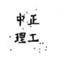
	Print-photocopy-scan	Rotation	Special attack
Attacked image			
PSNR	13.72	14.58	14.31
Retrieved logo			
NC	0.96	0.95	0.95

Table 5 The experimental results under different quality factors and threshold values.

Quality Factor	$T_2=1$		$T_2=2$		$T_2=3$	
	Image	NC	Image	NC	Image	NC
90		0.99		0.99		0.98
80		0.99		0.98		0.98
70		0.99		0.98		0.98
60		0.99		0.97		0.96
50		0.99		0.95		0.95
40		0.99		0.95		0.95
30		0.99		0.94		0.92
20		0.98		0.93		0.92
10		0.98		0.9		0.89

$$\mathrm{LL}'n_{\mathrm{new}}(i,j)=\begin{cases}1 & \text{if } \mathrm{LL}'n(i,j)>T_1',\\ 0 & \text{if } \mathrm{LL}'n(i,j)\le T_1',\end{cases}\tag{11}$$

where T_1' represents the predefined threshold value and $T_1'=\sum_{i=1}^{M/2^l}\sum_{j=1}^{N/2^l}LL'n(i,j)/[(M/2^l)\times(N/2^l)]$.
Step 4. Divide the new LL$'n$ subband into nonoverlapping $B\times B$ blocks, and compute the sum of all blocks, i.e.,

$$\mathrm{LL}'n_{\mathrm{new}}(m,n)=\sum_i^B\sum_j^B \mathrm{LL}'n_{\mathrm{new}}(i,j).\tag{12}$$

Step 5. Generate the feature value by the following equation:

$$f'(m,n)=\begin{cases}1 & \text{if } \mathrm{LL}'n_{\mathrm{new}}(m,n)\ge T_2,\\ 0 & \text{if } \mathrm{LL}'n_{\mathrm{new}}(m,n)<T_2,\end{cases}\tag{13}$$

where T_2 represents the predefined threshold value.
Step 6. Perform the XOR operation between the feature value and the secret image to obtain the scrambled logo according to

$$w_s'(m,n)=f'(m,n)\oplus s(m,n).\tag{14}$$

Step 7. Perform the operation of torus automorphism on the scrambled logo W_s':

$$W'=\mathrm{unscramble}(W_s).\tag{15}$$

Table 6 Comparison with Chen et al.'s scheme.

	Proposed scheme		Chen et al.'s scheme	
Attack	PSNR	NC	PSNR	NC
Blurring	25	0.99	29	0.99
JPEG	24	0.98	31	0.98
Noise	28	0.99	30	0.99
Sharpening	28	0.99	28	0.99
Scaling	21	0.98	29	0.99
Rotating	8	0.93	14	0.82
Print-photocopy-scan	7	0.94	19	0.9
Cropping	5	0.92	11	0.87
Cropping+scaling	9	0.93	16	0.8

Step 8. Compute the similarity NC between the original and retrieved logos by the following equation:

$$\mathrm{NC}=\frac{\sum_{i=1}^m\sum_{j=1}^n w(i,j)w'(i,j)}{\sum_{i=1}^m\sum_{j=1}^n [w(i,j)]^2}.\tag{16}$$

4 The Experimental Results

In this section, we report experiments showing the robustness of the proposed scheme. A 256×256 8-bit gray-level image named "Lena" was used as the test image. The test image was decomposed into four subbands by using one-level DWT. A 64×64 binary image was used as the logo [shown as Fig. 4(a) and 4(b)]. The selected subband is LL1, which is used to extract the feature. The predefined threshold value T_2 is 1. The secret image is shown as Fig. 4(c). Moreover, we used PhotoImpact 8.0 to simulate different attacks. The peak signal-to-noise ratio (PSNR) is used to measure the quality difference between the original image and the attacked one. The PSNR is defined as follows:

$$\mathrm{PSNR}=10\log_{10}\frac{255^2}{\mathrm{MSE}}(\mathrm{dB}),\tag{17}$$

$$\mathrm{MSE}=\frac{1}{m\times n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(X_{ij}-X_{ij}')^2,\tag{18}$$

where X_{ij} and X_{ij}' represent the original image and the attacked image, respectively. A large value for the PSNR means little difference between the original image and the attacked one. In general, it is very difficult to visually recognize the difference between the original image and the attacked one if the PSNR value is greater than 30 dB.

First, we applied JPEG compression with quality factor 5, noise addition with variance 100, and blurring attacks to the test image. Table 1 shows the results on the attacked images and the retrieved logos. Although the attacked images are seriously degraded, the retrieved logos can be still recognized.

Sharpening, scaling, and cropping are several attacks often applied to a digital image. In the scaling attack, the test image was first reduced to the size of 16×16 pixels and then restored to its original dimension. In the cropping attack, the top left corner of the test image was cut. From Table 2, it is seen that the proposed scheme can also survive these three attacks.

In our experiments, we also attacked the test image by mixing various kinds of attacks. The experimental results are shown in Table 3. It is clear that the proposed scheme is robust against the mixed attacks.

In the experiments reported in Table 4, we used other attacks (print-photocopy-scan, rotation, and special attacks) to test the robustness of the proposed scheme. In the print-photocopy-scan attack, the attacked image was obtained by using laser printing first, then photocopying, and finally scanning. In the rotation attack, the image was rotated 2 deg to the left and resized to the original dimension. Although the image qualities are greatly degraded, the retrieval results are still good.

We also used different T_2 values under different quality factors of compression to observe the retrieval results. From Table 5, it is clear that when T_2 is smaller, the retrieved results are better.

Finally, the proposed scheme is compared with Chen et al.'s scheme.[1] In the experiment, a "Lena" gray-level image with size of 512×512 was used as the test image. The comparison results are shown in Table 6. It is obvious that the proposed scheme has higher robustness than Chen et al.'s scheme.[1]

In these experiments, we use a recognizable visual image as the logo of the copyright owner. The results of the logo retrieval are unambiguous. Due to the proposed scheme utilizing the low-frequency characteristic, it is clear that the proposed scheme not only can clearly verify the copyright of the digital image, but also is robust against several attacks—in particular, print-photocopy-scan and rotation attacks that many copyright protection techniques proposed in the literature fail to resist.[1] Moreover, the proposed scheme is blind, because the logo retrieval does not require the original image. The proposed scheme adopts torus automorphism and a trusted third party to gain the benefit of security. The timestamp and digital signature techniques[1] can be also included in our scheme to enhance security further.

5 Conclusions

In this paper, we propose a robust copyright protection scheme using the low-band characteristic in the transform domain. The proposed scheme first scrambles the test image and the logo. Then it decomposes the scrambled image into wavelet coefficients and extracts the feature value. Finally, the feature value is XORed with the scrambled logo. In the verification process, the logo retrieval does not require the original image. Hence, storage space can be saved. The experimental results show that the proposed scheme meets the five essential requirements: robustness, imperceptibility, security, blindness, and unambiguity.

Acknowledgments

The authors thank the anonymous referees and the editor for their valuable suggestions and many constructive comments that improved the content and readability of this paper. This research was supported in part by the National Science Council of the Republic of China under grant NSC 93-2213-E-014-014.

References

1. T.-H. Chen, G.-B. Horng, and W.-B. Lee, "A publicly verifiable copyright-proving scheme resistant to malicious attacks," *IEEE Trans. Ind. Electron.* **52**(1), 327–334 (2005).
2. Y. Wang and A. Pearmain, "Blind image data hiding based on self reference," *Pattern Recogn. Lett.* **25**(15), 1681–1689 (2004).
3. I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.* **6**(12), 1673–1687 (1997).
4. F. Y. Shih and Y.-T. Wu, "Enhancement of image watermark retrieval based on genetic algorithms," *J. Visual Commun. Image Represent* **16**(2), 115–133 (2005).
5. Z.-M. Lu, D.-G. Xu, and S.-H. Sun, "Multipurpose image watermarking algorithm based on multistage vector quantization," *IEEE Trans. Image Process.* **14**(6), 822–831 (2005).
6. H.-C. Wu and C.-C. Chang, "Hiding digital watermarks using fractal compression technique," *Fund. Inform.* **58**(2), 189–202 (2003).
7. D.-C. Lou and C.-H. Sung, "A steganographic scheme for secure communications based on the chaos and Euler theorem," *IEEE Trans. Multimedia* **6**(3), 501–509 (2004).
8. H. Inoue, A. Miyazaki, A. Yamamoto, and T. Katsura, "A digital watermark based on the wavelet transform and its robustness on image compression," in *Proc. IEEE Int. Conf. on Image Processing*, pp. 391–395 (1998).
9. P. Bao and X. Ma, "Image adaptive watermarking using wavelet domain singular value decomposition," *IEEE Trans. Circuits Syst. Video Technol.* **15**(1), 97–102 (2005).
10. M.-S. Hsieh, D.-C. Tseng, and Y.-H. Huang, "Hiding digital watermarks using multiresolution wavelet transform," *IEEE Trans. Ind. Electron.* **48**(5), 875–882 (2001).
11. C.-T. Hsu and J.-L. Wu, "Multiresolution watermarking for digital images," *IEEE Trans. Circuits Syst., II: Analog Digital Signal Process.* **45**(8), 1097–1101 (1998).
12. G. Voyatzis and I. Pitas, "Application of toral automorphism in image watermarking," in *Proc. IEEE Int. Conf. on Image Processing*, Vol. **2**, pp. 237–240 (1996).
13. D. Zhao, G. Chen, and W. Liu, "A chaos-based robust wavelet-domain watermarking algorithm," *Chaos, Solitons Fractals* **22**, 47–54 (2004).
14. M.-J. Tsai, K.-Y. Yu, and Y.-Z. Chen, "Joint wavelet and spatial transformation for digital watermarking," *IEEE Trans. Consum. Electron.* **46**(1), 241–245 (2000).
15. M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," *IEEE Trans. Image Process.* **14**(2), 253–266 (2005).
16. J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.* **13**(8), 890–896 (2003).
17. S. Li, X. Zheng, X. Mou, and Y. Cai, "Chaotic encryption scheme for real-time digital video," *Proc. SPIE* **4666**, 149–160 (2002).

Der-Chyuan Lou received the BS degree from Chung Cheng Institute of Technology (CCIT), National Defense University, Taiwan, R.O.C., in 1987, and the MS degree from National Sun Yat-Sen University, Taiwan, R.O.C., in 1991, both in electrical engineering. He received the PhD degree in 1997 from the Department of Computer Science and Information Engineering at National Chung Cheng University, Taiwan: Since 1987, he has been with the Department of Electrical Engineering at CCIT, where he is currently a professor and the director of the Computer Center of CCIT. His research interests include cryptography, steganography, algorithm design and analysis, computer arithmetic, and parallel and distributed systems.

Hao-Kuan Tso received the BS and MS degrees in the Department of Electrical Engineering at the Chung-Cheng Institute of Technology, Taiwan, R.O.C., in 1995 and 2000, respectively. He is currently pursuing the PhD degree in the Department of Electrical Engineering at CCIT, National Defense University, Taiwan, R.O.C. His research interests include information hiding, image processing, and cryptography.

Jiang-Lung Liu received his PhD in electronics engineering from Chung Cheng Institute of Technology (CCIT), National Defense University, Taiwan. He is an assistant professor in the Department of Electrical Engineering at CCIT. His research interests include cryptology, information hiding, multimedia security, and image processing.