International Journal of Innovative Computing, Information and Control
Volume **9**, Number **9**, September **2013**

 ISSN 1349-4198
pp. 3549–3560

IMAGES TAMPER SELF-DETECTION AND SELF-RECOVERY USING SPIHT TECHNIQUE

Ji-Hong Chen[1], Wen-Yuan Chen[2] and Chin-Hsing Chen[1]

[1]Institute of Computer and Communication Engineering
National Cheng Kung University
No. 1, Dasyue Rd., East Dist., Tainan City 70101, Taiwan
jihong@ee.ncku.edu.tw; chench@eembox.ee.ncku.edu.tw

[2]Department of Electronic Engineering
National Chin Yi University of Technology
No. 57, Sec. 2, Zhongshan Rd., Taiping Dist., Taichung City, Taiwan
cwy@ncut.edu.tw

Received August 2012; revised December 2012

Abstract. *This paper presents a high quality image recovery technique as a highly efficient means for image tamper detection and recovery. A region of importance (ROI) in an image is firstly compressed by a set partitioning in hierarchical tree (SPIHT) technique and then embedded into a host image. In this way, the aim of self-detection and self-recovery for a tampered image can be achieved without extra information. Higher levels of security and secrecy are reached by embedding the image data into the discrete cosine transform (DCT) frequency domain through a nested structure technique. Accordingly, a high quality recovered image is ensured. This proposal is experimentally demonstrated to provide two clear advantages, that is, 1) the aim of a high quality and highly efficient image recovery from a tempered region is reached through an ROI image compression by an SPIHT technique, and 2) a higher level of security is achieved by use of a nested embedding structure. The proposed scheme can be applied to anti-counterfeiting for archives, digital right management, protection of crime scene photos, etc.*
Keywords: Self-detection, Self-recovery, Set partition in hierarchical trees (SPIHT), Region of importance, Discrete cosine transform (DCT)

1. **Introduction.** The tremendous progress made over recent years in both science and technology has led to the development of powerful multimedia tools, and has permitted imperceptible image modification in digital images as well. Thus, the protection of intellectual property rights is becoming an issue of increasing significance, and multimedia authentication and verification have turned into a popular discipline.

The authenticity and integrity of digital images can be ensured using a digital watermarking technique, a commonly seen technique when embedding a digital signature into a cover image. As a data stream, this digital signature can be either a small logo [1], a barcode [2] or even verification data [3] when employed for various purposes. A watermark can be extracted by use of an extraction scheme for a range of purposes, such as content integrity verification, ownership authentication and secret message transfer.

There have been a great number of watermarking schemes developed for various or specific purposes. In most cases, a watermark can be classified as a fragile, a semi-fragile, or a robust watermark in terms of its nature. Fragile watermarks [4-6] are commonly used for tamper detection or verifying the integrity of received images. These watermarks can be destroyed easily by rotating, cropping, scaling and other malicious operations. Semi-fragile watermarks [7,8] resist against benign transformations, and can identify modified

regions in a tampered image and extract the remaining watermark from the undamaged regions. Thus, semi-fragile watermarks are commonly used to detect malignant transformations. Robust watermarks [9-11] are designed to resist against various attacks that destroy the watermark in an image, and are typically used to protect digital rights or in varied digital signatures that prevent hackers or attackers from changing the ownership or infringing the copyrights.

On the basis of a hierarchical structure, the detection approach proposed by Lin et al. [12] requires a secret key together with a public chaotic mixing algorithm to recover a tampered image. The algorithm further proposed by Lin et al. [13] is a one that divides a watermarked image into non-overlapping blocks, each mapped to another block using toral automorphism. This method uses the three least significant bits of each original image pixel as the recovery information. Lee and Lin [14] proposed an effective dual watermark and look-up table method for image tamper detection and recovery, where two copies of the watermark are employed for each non-overlapping block in an image. Lin and Huang [15] used a hash function and an XOR operation to acquire an authentic sequence that is embedded into one of the sub-blocks in an image that recovers the tampered region. Song and Zhang [16] proposed a watermark embedding technique in the wavelet domain. Recovered information is compressed by an SPIHT algorithm, and then embedded into a host image in the wavelet domain. Lin et al. [17] proposed an ROI-based semi-fragile watermarking method to achieve image tamper detection and recovery. This information recovery approach is to define a region of importance (ROI) that is then embedded into the region of background (ROB). In case a tampering is detected in the ROI, the image can be recovered from the information embedded in the ROB.

This proposal uses a watermarking technique to hide a selected region into the region of importance (ROI) based on human visual perception, and uses a set partitioning in hierarchical tree (SPIHT) high-quality compression technique to ensure a high-quality image recovery from a tampered image. The remainder of this paper is outlined as follows. Section 2 describes the proposed secret recovery information embedding algorithm. Section 3 describes the proposed image tampering detection and recovery algorithm. Section 4 presents experimental results, and finally Section 5 concludes this paper.

2. Embedding Algorithm.

As illustrated in Figure 1, the overall embedding process involves a number of steps. Firstly, an ROI image was selected out of the cover image for image tamper detection and recovery. For security concern, a private key was used to generate the pseudo random number sequences (PRNS) PN_1 and PN_2. For an enhanced secrecy, a toral automorphism [18] associated with PN_1 is hired to hash the ROI data. an SPIHT technique is then used to reduce the size of data protected and elevate the data security. In an attempt to improve the robustness, the cover image was transformed to the frequency domain by DCT and PN_2 is adopted to hash embedded blocks to intensify data security. Finally, the image was watermarked by converting the embedded image from the frequency domain back to the spatial domain after taking the inverse DCT.

2.1. Set partitioning in hierarchical tree compression.

To conceal a secret image into a cover image, a high reconstructed image quality and a low bit rate property must be held by an image compression technique. The set partitioning in hierarchical (SPIHT) [19] method can meet the data hiding requirements, for the reason that it is developed based on the discrete wavelet transform (DWT) frequency domain with a high reconstruction image quality and a low bit rate property as stated above. Illustrated in Figure 2 is a comparison of peak signal-to-noise ratio (PSNR) versus compression ratio between SPIHT and JPEG. The encoding process uses a list of significant pixels (LSP) to store all the

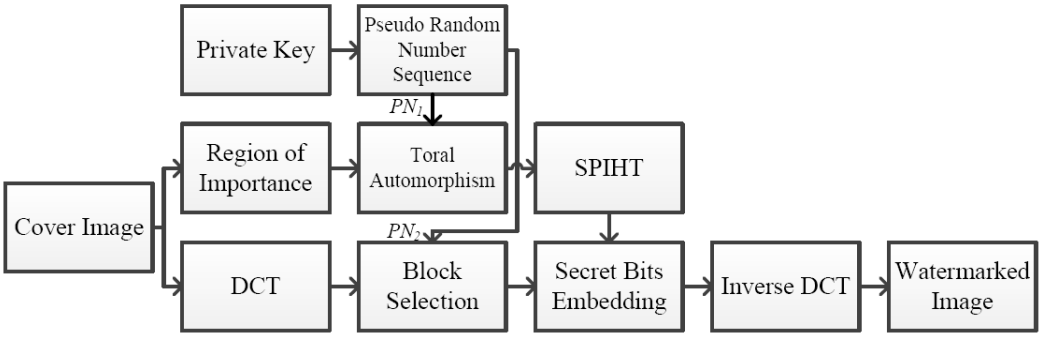


FIGURE 1. Flow chart of the proposed embedding process

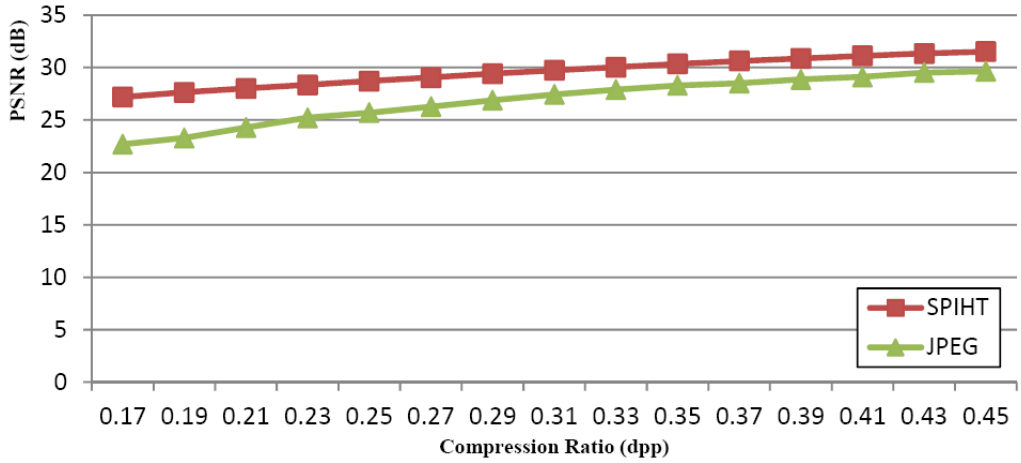


FIGURE 2. PSNR comparison between SPIHT and JPEG

significant coefficients, while a list of insignificant pixels (LIP) is composed of an unprocessed coefficients stream waiting for checking and encoding, and a list of insignificant set (LIS) temporarily stores the un-treated sub-tree coefficients. The SPIHT method also classifies the coefficients into type A or B. If an LIS entry is significant, then it belongs to type A. Conversely, if an LIS entry is a partition of type A, then it is considered as type B. Illustrated in Figure 3 is the relationship between types A and B. The SPIHT encoding algorithm can be described as follows:

1. Initialization: output the threshold $N = \lfloor \log_2 \left(\max_{(i,j)} \{|c_{i,j}|\} \right) \rfloor$ to the decoder, where $c_{i,j}$ is the coefficient of the DWT.
2. Sorting Pass: output μ_n and its sign, followed by the pixel coordinate $\eta_{(k)}$ such that $2^N \leq \left| c_{\eta_{(k)}} \right| < 2^{N+1}$, where u_n denotes the encoding bits stream of the coefficient $c_{i,j}$.
3. Refinement Pass: output the refinement bits of the nth most significant bit of all the coefficients.
4. Quantization-step Update: decrease N by $N/2$, and repeat Step 2.

2.2. **Region of importance.** In most cases, the region of interest is the area occupied by an image, and hence the protection for such region can lead to a reduction in the secret data size as well as an improvement in secret data quality. Owing to this feature, the part of the image is chosen as the embedding area and an ROI, as illustrated in Figure 4, which is the only region compressed by use of the SPIHT compression algorithm. In

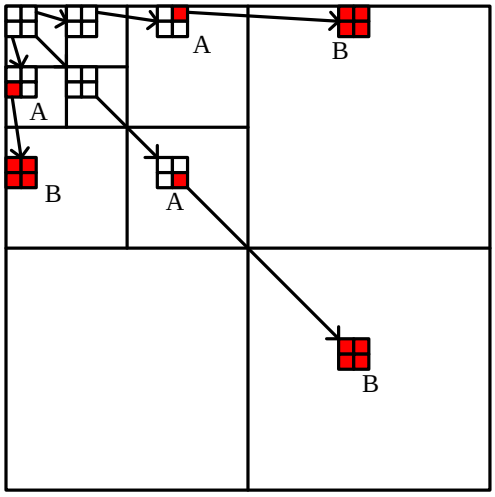


FIGURE 3. The relationship between types A and B sets in an SPIHT algorithm

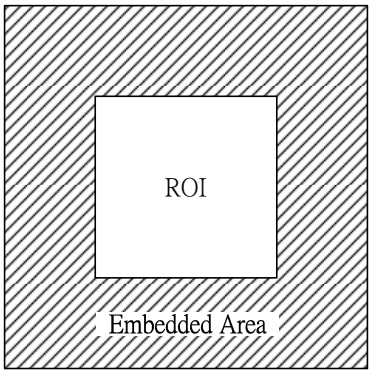


FIGURE 4. A graphic illustration of a region of importance (ROI)

FIGURE 5. ROI image comperess by SPIHT: (a) ROI of an original image, (b) a compressed image by SPIHT at a compression ratio of 0.25 bpp and with a PSNR of 28.70 dB

this way, not merely the compression size is reduced but also a high image quality of the recovered region is ensured. Figure 5 shows the compression results using the SPIHT compression algorithm. The image in Figure 5(a) is compressed into that in Figure 5(b) at a compression ratio of 0.25 bpp, and a PSNR up to 28.70 dB is reached in the decompressed image.

2.3. **Toral automorphism.** For security concern, a watermarked image is pre-permuted into noises using toral automorphism with a users key. Toral automorphism is a type of dynamic system that scatters the image shape by iterative operations until a specified number of iterations are performed, and then recovers the image to the original shape. The number of iterations is determined by the toral automorphism parameters and the image size. The proposed method uses toral automorphism to transform the original image into a chaotic form to protect the watermark. The transformation formula is represented as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod n, \tag{1}$$

where $(x', y') \in [0, n] \times [0, n]$, $(x, y) \in [0, n] \times [0, n]$, and $k \in [0, n]$. The terms $[x, y]$ and $[x', y']$ represent the pixel locations of the original and confused images, respectively, the parameter k denotes the control parameter, and n the size of the given image.

2.4. **Block selection of DCT.** Taking the discrete cosine transform (DCT), an image is transformed from the spatial to the frequency domain. The DCT can be expressed as

$$D(p,q) = \frac{1}{\sqrt{2n}} \alpha(p)\, \alpha(q) \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} f(m,n) \cos \frac{(2m+1)\, p\pi}{2M} \cos \frac{(2n+1)\, q\pi}{2N}, \tag{2}$$

where

$$\alpha(p) = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \tag{3}$$

$$\alpha(q) = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases} \tag{4}$$

f denotes the original image and D the DCT-transferred image, M and N the row and column sizes of the image f, respectively, and the terms p, q, m, and n represent the images D and f coordinates, respectively.

The proposal employs a host image of 8×8 blocks whose coefficients are the values corresponding to the DCT basis. As illustrated in Figure 6, the coefficient located at the upper-left corner is the DC value, which is affected by the luminance, while those, marked as B1-B5, in the vicinity of the DC value are the low-frequency components, over which the energy is concentrated, and are suitable for concealing secret data in this work.

2.5. **Secret bits embedding.** The data hiding approach in this proposal ensures that the secret information is not destroyed and the security is enhanced by scrambling the data into a chaotic state. Therefore, a chaotic mechanism is required to hash a bitstream m_s, and a fast pseudo-random number traversing method is employed as a chaotic mechanism to permute the bitstream m_s. The relationship between the bit sequences after and before permutation is given as

$$m_c(i) = m_s(i'), \quad i \ge 1,\ i' \le F, \tag{5}$$

$$i = permutation(i'), \tag{6}$$

where F symbolizes the length of the bit sequence. The permutation operation was performed through Equation (5) with a pseudo-random sequence.

This embedding process adopts a bit replacement technique to conceal the secret data. In this way, the secret image is of the size 256×256 and a compression rate of 0.25 bpp is reached by the SPIHT compression algorithm. Thereby, a bitstream of length 15,360 bits is generated, and bit 5 is selected out of the DCT coefficients for secret bit replacement, while the coefficients B1-B5 of the DCT block are employed for secret bits embedding.

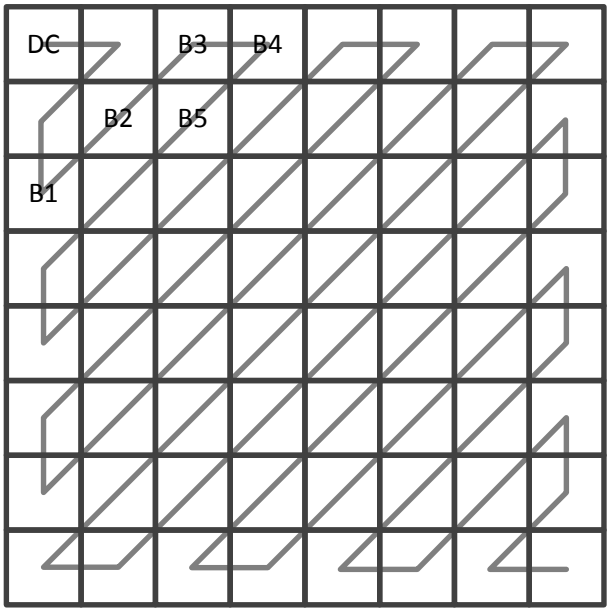


FIGURE 6. Coefficients corresponding to DCT blocks

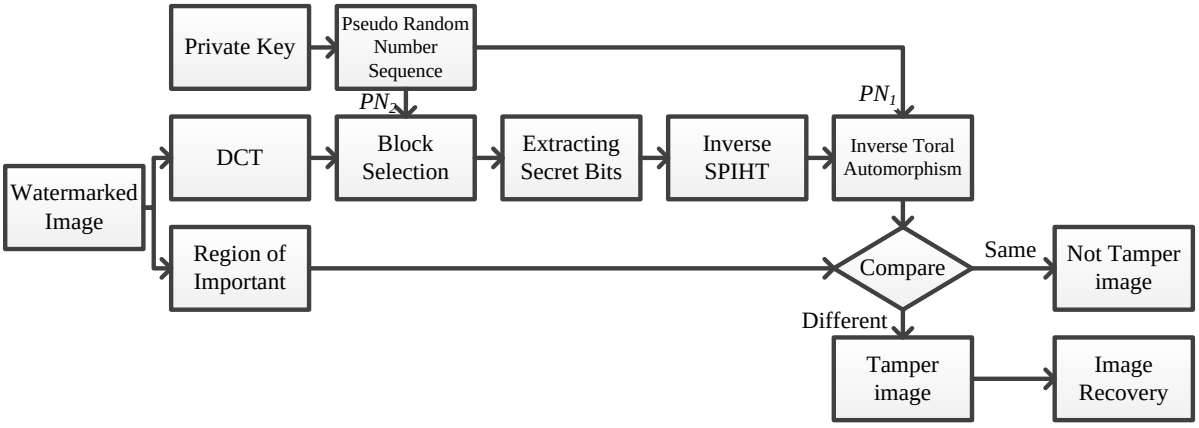


FIGURE 7. Flowchart of the proposed self-detection and self-recovery process

3. **Detection and Recovery Algorithm.** As illustrated in Figure 7, the detection process is exactly the inverse of the aforementioned embedding process. As the first step, a watermarked image was transformed to the frequency domain by a DCT technique. As in the embedding procedure, the block selection and the inverse toral automorphism necessitate the PN sequences PN_1 and PN_2 to recovery the hash order. Following the extraction of the secret bits, an inverse SPIHT algorithm was used to restore an ROI data. Finally, a comparison is made between the extracted ROI data and the watermarked image, as an efficient way to tell whether the image is tampered or not. Once the ROI image was found tampered, the self-recovery processing will be enabled to restore the image automatically.

3.1. **Extracting the bitstream.** The secret data embedding process employs a pseudo number traversing method as a chaotic mechanism to permute the bitstreams. As referred to previously, the relationship is revealed in Equations (5) and (6) between the bit sequences after and before permutation. The secret data extraction process adopts an

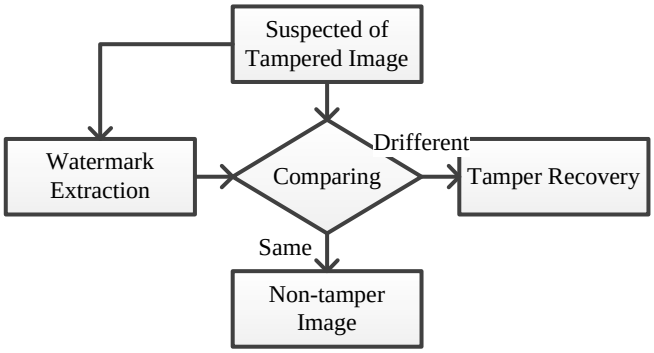


FIGURE 8. Flowchart of the proposed image tamper detection and recovery procedure

inverse fast pseudo-random number traversing method as the inverse chaotic mechanism to rearrange the bitstream. The rearrangement operation is given by

$$m_s(i') = m_c(i), \quad i \geq 1,\ i' \leq F, \tag{7}$$

$$i' = permutation(i), \tag{8}$$

where F denotes the length of the bit sequence.

3.2. **Set partitioning in hierarchical tree decompression.** An SPIHT encoder compresses an image into a linear bitstream using a zigzag scan order, and the encoding operation is detailed in Section 2. The SPIHT decoding follows the inverse process of the encoding, but excluding Step 4, that is, Step 1 checks the bitstream and assigns corresponding values to the coefficients of the DWT in a zigzag scan order, Step 2 modifies the corresponding values of the DWT coefficients according to the refined bits, and Step 3 repeats the steps above until all the bit streams have been handled.

3.3. **Inverse toral automorphism.** Toral automorphism scatters the image shape into a hashed state, and the inverse toral automorphism returns the chaotic image to the original shape. According to the theory of toral automorphism, a hashed image returns to its original shape when it is iterated a specified number of times. Thus, the hashed image returns to its original shape in the event that a specified number of iterations are performed first in the embedding process and then in the extracting process.

3.4. **Tampering self-detection and self-recovery.** Illustrated in Figure 8 is a flowchart of the proposed tamper self-detection and self-recovery process. Firstly, extract the watermark out of a suspected tampered image, and then use the SPIHT decompression algorithm to produce a detected image. Next, compare the suspected tampered image with an uncompressed image produced by SPIHT. If both data are found to be distinct, identify the uncompressed part of the data and the recovered part of the tampered image. Figure 9 shows a crimes scene photo that was tampered deliberately and recovered subsequently. As can be seen, the linchpin point disappeared in the tampered image (Figure 9(b)) as opposed to the original (Figure 9(a)). Demonstrated in Figure 9(c) is the image produced by this proposed tamper detection approach, by which the tampered image is self-recovered with a PSNR up to 39 dB, as shown in Figure 9(d).

4. **Experimental Results.** Imperceptibility is a crucial factor in hiding recovered secret information. The quantity PSNR is commonly adopted as a quality measure for the reconstruction from compressed images and for watermarked images. Therefore, a quantitative measure is required to provide an objective judgment of the extraction fidelity.

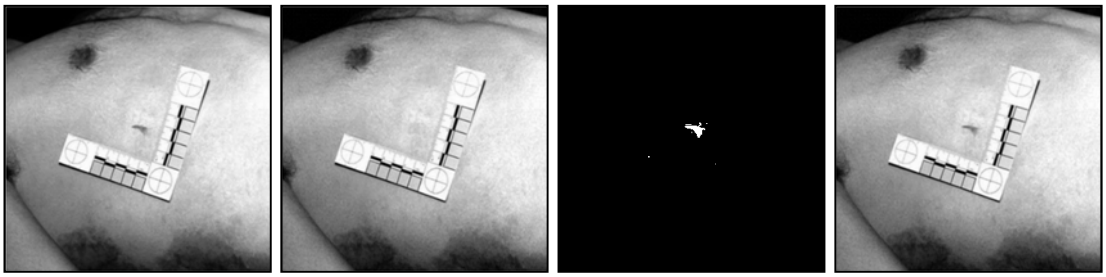


FIGURE 9. The crime scene image: (a) the original image, (b) image tampered with a PSNR of 39.26 dB, (c) the tampered location, (d) recovered image with a PSNR of 39.00 dB

FIGURE 10. Crime scene: (a) a watermarked image with a PSNR of 39.72 dB, (b) a tampered image of (a), (c) the detected tampered region of (a), (d) the recovered image of (b) with a PSNR of 37.91 dB

Most easily defined by the mean squared error (MSE), the degree of transparency in this work is evaluated in terms of the peak signal-to-noise ratio (PSNR), defined as

$$PSNR = 20\log_{10}\frac{255}{MSE}, \tag{9}$$

$$MSE = \frac{1}{M \times N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\|I(x,y) - I'(x,y)\|^2, \tag{10}$$

where $I(x,y)$ and $I'(x,y)$ denote the $M \times N$ grayscale values of the cover image I and the watermarked image I', respectively. Images Crime Scene, Mona Lisa, F-16, and Painting of size 512×512 were used as the test objects in this proposed scheme.

Simulation result. In this study, a number of experiments are conducted as a way to validate the effectiveness of this proposal. Pictured in Figure 10(a) is crime scene photo, where an evidence marker is placed next to a bullet shell, which was a recovery of embedded secret data with a PSNR of 39.72 dB. The bullet shell, as seen in Figure 10(a), was removed in Figure 10(b), as a consequence of malicious tampering, but is precisely located in Figure 10(c). In Figure 10(d), the image is recovered with a PSNR of 37.91 dB. Accordingly, this algorithm is proven able to precisely locate the tampered region which can be recovered back to the original, i.e., a reliable protection of crime scene photos against falsification.

Figure 11(a) shows Mona Lisa, a masterpiece of Leonardo da Vinci, which was a recovery of embedded secret data with a PSNR of 40.03 dB. Her face is tempered deliberately

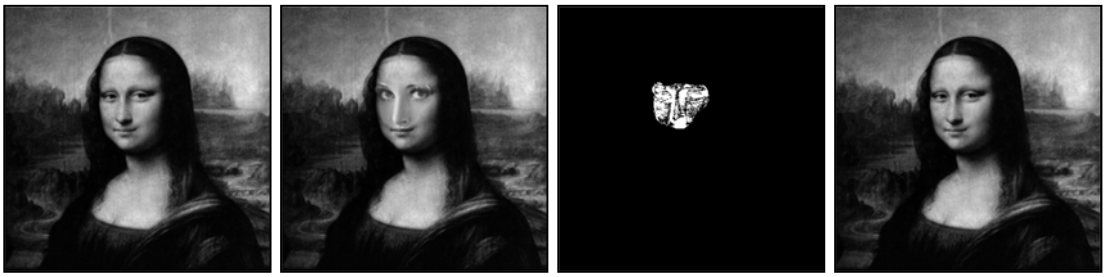


FIGURE 11. Mona Lisa: (a) a watermarked image with a PSNR of 40.03 dB, (b) a tamperd image of (a), (c) the detected tampered region of (a), (d) the recovered image of (b) with a PSNR of 38.17 dB

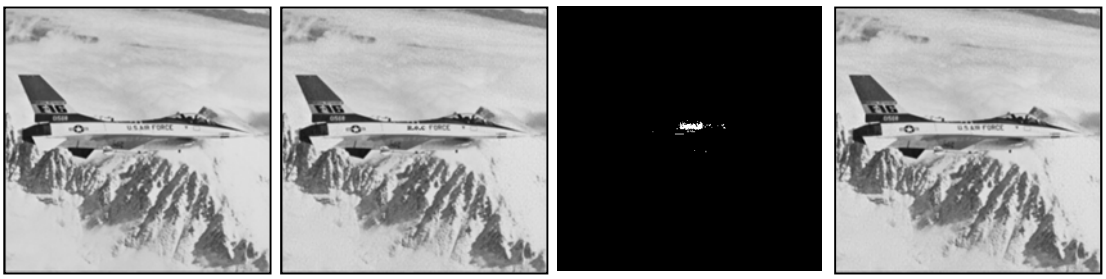


FIGURE 12. F-16 fighter: (a) a watermarked image with a PSNR of 39.00 dB, (b) a tamperd image of (a), (c) the detected tampered region of (a), (d) the recovered image of (b) with a PSNR of 38.34 dB

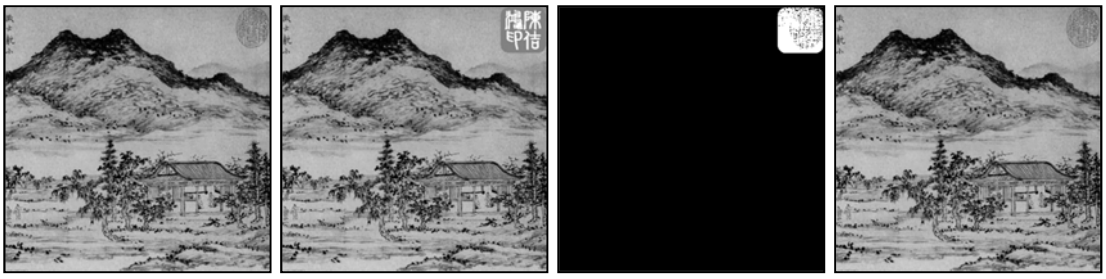


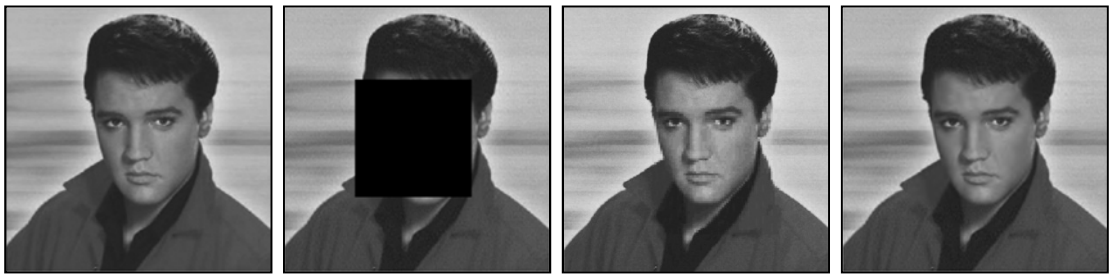
FIGURE 13. Landscape painting: (a) a watermarked image with a PSNR of 39.13 dB, (b) a tamperd image of (a), (c) the detected tampered region of (a), (d) the recovered image of (b) with a PSNR of 38.78 dB

(Figure 11(b)), the tampered area is located precisely (Figure 11(c)), and is recovered (Figure 11(d)) with a PSNR of 38.17 dB. As in the previous case, this proposal is proven again able to precisely detect the tampered region and then acquire a satisfactory image recovery.

Presented in Figure 12(a) is a watermarked photo of an F-16 fighter aircraft with a PSNR of 39.00 dB, and exhibited in Figure 12(b) is a tempered photo. The tampered area was identified in Figure 12(c), and then a fully recovered image with a PSNR of 38.34 dB is shown in Figure 12(d), that is, the characters R.O.C on the F16 body are corrected into US AIR as intended.

TABLE 1. PSNR values of the watermarked and the recovered images

Sample Image	Crime Scene	Mona Lisa	F-16	Painting
Watermarked Image	39.72	40.03	39.00	39.13
Recovered Image	37.91	38.17	38.34	38.78



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

FIGURE 14. Comparison between Lee's method and this proposal: (a) an original image of Elvis, (b) a 22% cropped image of (a), (c) the recoverd image through Lee's algorithm with a PSNR of 36.39 dB, (d) the recoverd image through this proposal with a PSNR of 38.58 dB

TABLE 2. Performance comparison between Lee's method and this proposal

Item	Lee's method	Propose method
Security	–	High
Embedding location	Watermark embedded in LSB	Watermark embedded in DCT
Detection and recovery speed	Quickly	Quickly
Quality	High	Very high

Presented in Figure 13(a) is a watermarked and sealed traditional Chinese landscape painting with a PSNR of 39.13 dB. In Figure 13(b), the painting's seal is falsified. As seen in Figures 13(c) and 13(d), this proposal is found again able to successfully locate the tampering at the upper right corner and acquire a recovered image with a PSNR of 38.78 dB.

Tabulated in Table 1 is a PSNR comparison between all the watermarked images and all the recovered images. It is seen that the recovered images provide comparable PSNR values relative to the watermarked counterparts.

Presented in Figure 14(a) is an original Elvis photo, while the facial features of Elvis are padded with a black window in Figure 14(b), and the face is recovered in Figure 14(c) using Lee's method [13] with a PSNR of 36.39 dB. In contrast, significantly improved image quality is seen in Figure 14(d) by use of this proposal. A comparison between Lee's method and this proposal is tabulated in Table 2. For security concern, this proposal employs a chaotic algorithm to embed secret data in the frequency domain, ensuring that that recovered data cannot be found easily. In terms of detection and recovery capacity, this proposal provides an efficient detection and a high quality image recovery.

5. **Conclusion.** This paper employs a pseudo random number sequence generator (PRN SG), toral automorphism, an SPIHT technique, DCT and a secret bit embedding algorithm to achieve the aim of self-detection and self-recovery for an ROI image. In secret

data embedding, a private key was used to generate two sequences and through PRNSG. Accordingly, the blocks selected by DCT and toral automorphism are hashed in such a way that the system security is enhanced. In order to achieve a high-quality as well as a highly efficient tampered image recovery, an SPIHT technique is adopted to compress the ROI area which is embedded into the cover image. The image data are transformed from the spatial to the frequency domain by DCT and the secret data is embedded into the frequency domain for a higher robustness of the watermarked image. This study is demonstrated experimentally as an automatically enabled effective self-detection and self-recovery algorithm. Furthermore, this scheme can be applied to anti-counterfeiting for archives, digital rights management, protection of crime scene photos, etc.

REFERENCES

[1] Y. Lee, J. Nah and J. Kim, Digital image watermarking using bidimensional empirical mode decomposition in wavelet domain, *International Symposium on Multimedia*, pp.583-588, 2009.

[2] W. Y. Chen and J. W. Wang, Nested image steganography scheme using QR-barcode technique, *Optical Engineering*, vol.48, vol.5, pp.057004-1-10, 2009.

[3] S. L. Hsieh, C. P. Yeh and I. J. Tsai, An image copyright protection scheme with tamper detection capability, *Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing*, pp.342-349, 2009.

[4] C. W. Wu, D. Coppersmith, F. C. Mintzer, C. P. Tresser and M. M. Yeung, Fragile imperceptible digital watermark with privacy control, *SPIE Security Watermarking Multimedia Contents*, vol.3657, pp.79-84, 1999.

[5] D. Kunder and D. Hatzinakos, Digital watermarking for telleable tamper proofing and authentication, *Journals & Magazines*, vol.87, pp.1167-1180, 1999.

[6] G. J. Yu, C. S. Lu and H. Y. M. Liao, Mean quantization-based fragile watermarking for image authentication, *Optical Engineering*, vol.40, no.7, pp.1396-1408, 2001.

[7] K. Maeno, Q. Sun, S. F. Chang and M. Suto, New semi-fragile image authentication watermarking techniques using random bias and nonuniform quantization, *IEEE Trans. on Multimedia*, vol.8, pp.32-45, 2006.

[8] D. Zou, Y. Q. Shi, Z. Ni and W. Su, A semi-fragile lossless digital watermarking scheme based integer wavelet transform, *IEEE Trans. on Circuits and System for Video Technology*, vol.16, pp.1294-1300, 2006.

[9] W. Y. Chen and C. H. Chen, Robust watermarking scheme for still images using frequency shift keying high-variance block selection, *Optical Engineering*, vol.42, no.6, pp.1826-1835, 2003.

[10] W. Y. Chen and C. H. Chen, A robust watermarking scheme using phase shift keying with the combination of amplitude boost and low amplitude block selection, *Pattern Recognition*, vol.38, pp.587-598, 2005.

[11] X. Huang and B. Zhang, Statistically robust detection of multiplicative spread-spectrum watermarks, *IEEE Trans. on Information Forensics and Security*, vol.2, pp.1-13, 2007.

[12] P. L. Lin, C. K. Hsieh and P. W. Huang, A hierarchical digital watermarking method for image tamper detection and recovery, *Pattern Recognition*, vol.38, pp.2519-2529, 2005.

[13] S. D. Lin, Y. Kuo and M. Yao, An image watermarking scheme with tamper detection and recovery, *International Journal of Innovative Computer, Information and Control*, vol.3, no.6(A), pp.1379-1387, 2007.

[14] T. Y. Lee and S. D. Lin, Dual watermark for image tamper detection and recovery, *Pattern Recognition*, vol.41, pp.3497-3506, 2008.

[15] S. D. Lin and Y.-H. Huang, An integrated watermarking technique with tamper detection and recovery, *International Journal of Innovative Computer, Information and Control*, vol.5, no.11(B), pp.4309-4316, 2009.

[16] Q. Song and H. Zhang, Image tamper detection and recovery using dual watermark, *Conf. on Wireless Communications Networking and Mobile Computing*, pp.1-4, 2010.

[17] S. D. Lin, J.-H. Lin and C.-Y. Chen, A ROI-base semi-fragile watermarking for image tamper detection and recovery, *International Journal of Innovative Computer, Information and Control*, vol.7, no.12, pp.6875-6888, 2011.

[18] G. Voyatzis and I. Pitas, Application of toral automorphism in image watermarking, *IEEE Conf. on Image Processing*, vol.2, pp.237-240, 1996.

[19] A. Sad and W. A. Pearlman, A new, fast, and efficient image codec based on set partitioning in hierarchical trees, *IEEE Trans. on Circuit and Systems for Video Technology*, vol.6, no.3, pp.243-250, 1996.