IEICE TRANS. FUNDAMENTALS, VOL.E92–A, NO.3 MARCH 2009

LETTER *Special Section on Latest Advances in Fundamental Theories of Signal Processing*

Asymmetric Fragile Watermarking Using a Number Theoretic Transform

Hideaki TAMORI[†a)], ***Student Member and*** **Tsuyoshi YAMAMOTO**[†], ***Member***

SUMMARY We propose an asymmetric fragile watermarking technique that uses a number theoretic transform (NTT). Signature data is extracted from a watermarked image by determining correlation functions that are computed using the NTT. The effectiveness of the proposed method is evaluated by simulated detection of altering.

key words: *number theoretic transform, asymmetric watermarking, fragile watermarking, image authentication*

1. Introduction

Since digital data, such as images, can be easily modified, it is necessary to guarantee its originality when using it as an official document or evidence. Therefore, fragile watermarking techniques are researched for meeting this need. Digital images are divided into small blocks, and fragile watermarks are embedded into each block. Altered blocks are detected by searching for destroyed watermarks.

Conventional techniques for fragile watermarking were mainly categorized as spatial-domain methods based on a hashing function. We have proposed a different technique based on the fact that NTTs have no round-off error [1]. This is categorized as a transform-domain method. Compared to spatial-domain methods, transform-domain ones offer greater security [1]. However, [1] is a secret key scheme, so an attacker can update the signature data after altering images if the secret key is known. Therefore, this method is more cumbersome because the secret key must be sent through a secure channel. Also, only the user who possesses the secret key can carry out the extraction procedure [2]. In this paper, we propose an asymmetric fragile watermarking technique using the NTT. This technique can release a public key, which cannot be used to update the watermarking [3]. A simulation experiment was conducted to examine the effectiveness of the proposed method.

2. Number Theoretic Transform

The transform pairs of the NTT are as follows:

$$X(k) = \sum_{n=0}^{N-1} x(n)\alpha^{kn} \pmod{P}, \tag{1}$$

$$x(n) = \frac{1}{N}\sum_{k=0}^{N-1} X(k)\alpha^{-kn} \pmod{P}, \tag{2}$$

where $X(k)$ is the spectrum of a signal $x(n)$, P and α are integers, and N is the smallest nonzero integer for which $\alpha^N = 1 \pmod{P}$. N is the transformation length referred to as the *order*, while α is the kernel of the transforms referred to as the *root of N*. Since all NTT calculations are performed in a Galois field, no round-off errors are observed. The NTT supports convolution, and has been used for filtering, calculating the correlation function, and cryptography [4], [5].

3. Proposed Method

The procedure for our embedding process is shown in Fig. 1(a). First, we determine the block size N and modulus P, which are the NTT parameters. Note that $P = aN + 1$ is a prime number and larger than the highest pixel value of the original image, where a is a nonzero integer [1].

The original image of size $IN \times JN$ pixels is divided into blocks of $N \times N$ pixels, and we denote the value of pixel(x, y) in block(i, j) as $f_{i,j}(x, y)$, where $0 \le i \le I-1, 0 \le j \le J-1$, and $0 \le x, y \le N-1$. Let $r_{i,j}(x, y)$ be a pseudo-random integer sequence, and $g_{i,j}(x, y)$ be the value of pixel(x, y) in watermarked block(i, j). $g_{i,j}(x, y)$ is computed by

$$g_{i,j}(x, y) = f_{i,j}(x, y) + r_{i,j}(x, y). \tag{3}$$

Note that the seed for $r_{i,j}(x, y)$ is generated using $f_{i,j}(x, y)$ and $sign_{i,j}(x, y)$ which is the embedded signature bit in block(i, j). Also, $r_{i,j}(x, y)$ which is the (x, y)-th secret key in block(i, j) should be composed of very small absolute values compared to the pixel value.

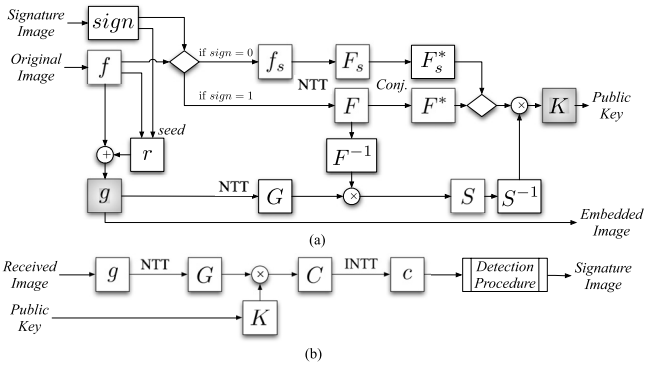

Fig. 1 Proposed method: (a) embedding and (b) extraction procedure.

Manuscript received July 4, 2008.
Manuscript revised October 16, 2008.

[†]The authors are with the Graduate School of Information Science and Technology, Hokkaido University, Sapporo-shi, 060-0814 Japan.
a) E-mail: tamori@ime.ist.hokudai.ac.jp

DOI: 10.1587/transfun.E92.A.836

Let $F_{i,j}(u,v)$ and $G_{i,j}(u,v)$ be the NTT of $f_{i,j}(x,y)$ and $g_{i,j}(x,y)$, respectively, where $0 \le u,v \le N-1$, and $S_{i,j}(u,v)$ be

$$S_{i,j}(u,v) = F_{i,j}^{-1}(u,v)G_{i,j}(u,v), \tag{4}$$

where $F_{i,j}^{-1}(u,v)$ is the inverse of $F_{i,j}(u,v)$, i.e.,

$$F_{i,j}(u,v)F_{i,j}^{-1}(u,v) = 1 \pmod{P}. \tag{5}$$

Note that $S_{i,j}(u,v)$ is the product of each element of $F_{i,j}^{-1}(u,v)$ and $G_{i,j}(u,v)$. Let $K_{i,j}(u,v)$ be the (u,v)-th public key in block(i,j). $K_{i,j}(u,v)$ is generated as follows:

$$K_{i,j}(u,v) = \begin{cases} F^*_{i,j}(u,v)S^{-1}_{i,j}(u,v) & \text{if } sign_{i,j} = 1, \\ F^*_{si,j}(u,v)S^{-1}_{i,j}(u,v) & \text{if } sign_{i,j} = 0, \end{cases} \tag{6}$$

where $F_{si,j}(u,v)$ is the NTT of $f_{si,j}(x,y)$, which is obtained by exchanging the parts of $f_{i,j}(x,y)$ between quadrant I and IV and between II and III, as shown in Fig. 2. $F^*{}_{i,j}(u,v)$ and $F^*{}_{si,j}(u,v)$ are the conjugate of $F_{i,j}(u,v)$ and $F_{si,j}(u,v)$, which are denoted as

$$F^*{}_{i,j}(u,v) = F_{i,j}(-u,-v), \tag{7}$$

$$F^*{}_{si,j}(u,v) = F_{si,j}(-u,-v), \tag{8}$$

respectively, and $S^{-1}_{i,j}(u,v)$ is the inverse of $S_{i,j}(u,v)$.

The extraction procedure is shown in Fig. 1(b). The received image of size $IN \times JN$ pixels is divided into blocks of $N \times N$ pixels, which are denoted as $g_{i,j}(x,y)$. Let $C_{i,j}(u,v)$ be the product of each element of $G_{i,j}(u,v)$ and $K_{i,j}(u,v)$, i.e., the convolution between $G_{i,j}(u,v)$ and $K_{i,j}(u,v)$ (Eqs. (4) and (6)), which is expressed as

$$C_{i,j}(u,v) = \begin{cases} F_{i,j}(u,v)F^*{}_{i,j}(u,v) & \text{if } sign_{i,j} = 1, \\ F_{i,j}(u,v)F^*_{si,j}(u,v) & \text{if } sign_{i,j} = 0, \end{cases} \tag{9}$$

if $g_{i,j}(x,y)$ has not been altered.

Let $c_{i,j}(x,y)$ be the inverse NTT (INTT) of $C_{i,j}(u,v)$. If $sign_{i,j} = 1$, $c_{i,j}(x,y)$ is the autocorrelation function of $f_{i,j}(x,y)$. Also, if $sign_{i,j} = 0$, $c_{i,j}(x,y)$ is the cross-correlation function between $f_{i,j}(x,y)$ and $f_{si,j}(x,y)$. Therefore, our extractor is

$$sign_{i,j} = \begin{cases} 1 & \text{if } \max c_{i,j}(x,y) = c_{i,j}(N/2, N/2), \\ 0 & \text{if } \max c_{i,j}(x,y) = c_{i,j}(0,0). \end{cases} \tag{10}$$

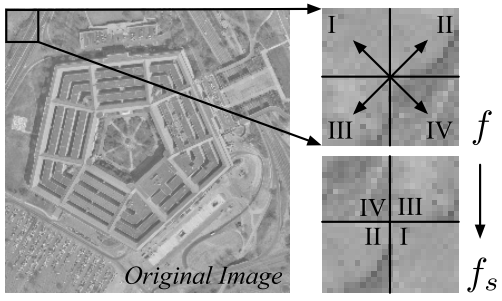

Fig. 2 $f_{si,j}(x,y)$ is obtained by exchanging the parts of $f_{i,j}(x,y)$ between quadrant I and IV and between II and III.

No computational errors occur in this embedding and extraction process because the NTT has no round-off error. Therefore, the block(i,j) is considered to be altered when $sign_{i,j}$ in Eq. (10) is neither 0 nor 1.

4. Experimental Results

We preformed simulations in which a watermarked image was altered artificially. The target image, shown in Fig. 3(a), was an 8-bit gray-scale image of size 256×256 pixels. The original signature image, as shown in Fig. 3(b), was a binary image of size 32×32 pixels. $P = 16,337,592,495,324,680,449$, $N = 8$, and $r_{i,j}(x,y)$ was uniformly distributed in $\{-1,1\}$.

The watermarked image, as shown in Fig. 3(c), had a peak signal-to-noise ratio (PSNR) of 50.2 (dB), and the extracted signature image from Fig. 3(c) is shown in Fig. 3(d). The original signature image was exactly extracted thanks to the features of the NTT.

Figure 3(c) was altered by a copy-and-paste attack as shown in Fig. 3(e), and the extracted signature image from Fig. 3(e) is shown in Fig. 3(f). We can detect the altered area visually.

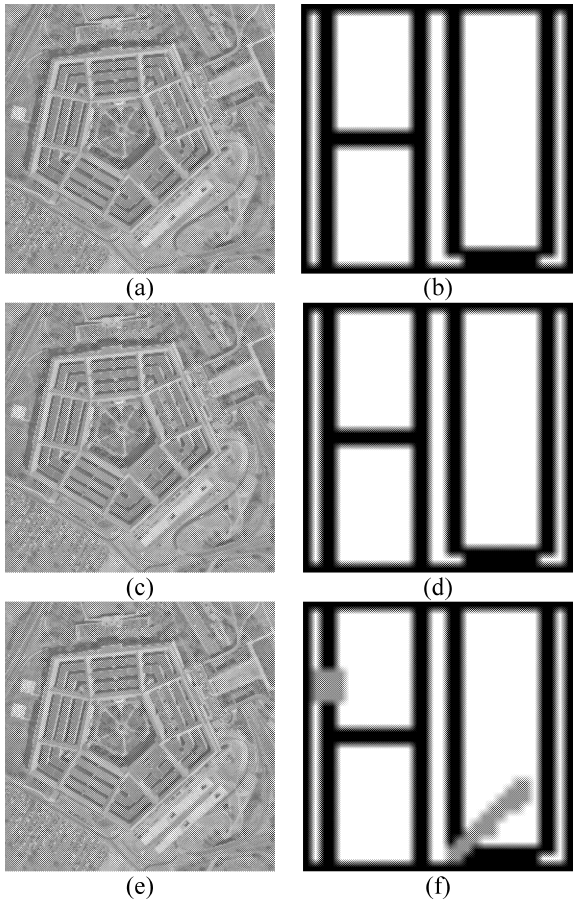

Fig. 3 Experimental results: (a) original image ($256 \times 256 \times 8$ bits), (b) signature image($32 \times 32 \times 1$ bits), (c) embedded image, (d) extracted signature image from (c), (e) altered image, and (f) extracted signature image from (e).

5. Conclusion

In this paper, we have presented an asymmetric fragile watermarking technique based on a NTT. In the future, we will apply this method to JPEG images and consider the security issues of this method. Furthermore, it is possible that the safety of the proposed technique decreases when the public key is altered. Therefore, it is necessary to consider the operational infrastructure of the public key.

References

[1] H. Tamori, N. Aoki, and T. Yamamoto, "A localizing technique of alteration using fragile digital watermarking based on number theoretic transform," IEICE Trans. Fundamentals (Japanese Edition), vol.J86-A, no.8, pp.872–879, Aug. 2003.

[2] P.W. Wong, "A public key watermarking of image verification and authentication," Proc. ICIP, vol.1, pp.455–459, Oct. 1998.

[3] T. Furon and P. Duhamel, "An asymmetric watermarking method," IEEE Trans. Signal Process., vol.51, no.4, pp.981–995, April 2003.

[4] I.S. Reed, T.K. Troung, Y.S. Kwoh, and E.L. Hall, "Image processing by transforms over a finite field," IEEE Trans. Comput., vol.C-26, no.9, pp.874–881, Sept. 1977.

[5] S. Hirata, K. Takahashi, and M. Mimura, "Vulnerability analysis and improvement of cancelable biometrics for image matching," SCIS 2007, 3C1-2, Sasebo, Jan. 2007.