2008 International Symposium on Nonlinear Theory and its Applications
NOLTA'08, Budapest, Hungary, September 7-10, 2008

Method of Falsification Detection for JPEG Images Using Chaotic Watermarks and Its Evaluation

Masaru Hisano†, Taichi Umezawa† and Hiroyuki Kamata‡

†Graduate School of Science and Technology, Meiji University
1-1-1 Tama-ku Higashi-Mita, Kawasaki, Kanagawa 214-8571 Japan
‡School of Science and Technology, Meiji University
1-1-1 Tama-ku Higashi-Mita, Kawasaki, Kanagawa 214-8571 Japan
Email: ce77071@isc.meiji.ac.jp, kamata@isc.meiji.ac.jp

Abstract—The technique of the falsification detection for JPEG images using digital watermark based on the chaos theory is proposed. By embedding chaotic signals as the digital watermark data, the falsification of JPEG images can be detected because of the Sensitive Dependence on Initial Conditions and Orbital Instability of chaos. In this paper, 8-bit alphanumeric characters are decided as the original information data and are modulated to two chaotic signals. Furthermore, based on a same information data, two chaotic signals are generated by modulators with different parameters, respectively, and are embedded to a DCT coefficient block. By this method, even if the information data is uncertain, the falsification can be detected by comparing the demodulated signals. In this paper, the ability and the effectiveness of the proposed method are shown by some experimental results.

1. Introduction

Recently, as the increasing use of personal digital assistants and personal computers, opportunities to use the digital images are increased. Especially, the use of JPEG (Joint Photographic Coding Experts Group) images is being popular because of the spread of digital cameras. However, in case of using JPEG images for evidence of trial or for insurance claims procedure, it is necessary to provide against the falsification of the digital images [1] [2].

The digital watermark schemes for JPEG images have been discussed [3]-[6]. In general, the technique of digital watermark is used to protect copyright and should be robust over malicious attack. On the other hand, the digital watermark data should be fragile when the technique of the digital watermark is used to detect falsifications as this study. The reason why the falsification is detected by embedding fragile watermark data is that the watermark information can be destroyed when the data is attacked.

In addition, the fragile watermark data is generated by cascade structured chaotic modulators with different parameters [7]. By embedding chaotic signals as the digital watermark data, the falsification of JPEG images is detected because of the Sensitive Dependence on Initial Conditions and Orbital Instability of chaos. The orbit of chaos begins to shift at once, and a correct decoding becomes impossible when there is even 1-bit error in watermark information. Therefore the falsification is detected by checking whether the two decoded information accord or not.

In this paper, 8-bit alphanumeric characters are decided as the original information data and are modulated to the chaotic signals. The two different chaotic signals are embedded respectively by using two different embedding methods. By the method, even if the digital watermark data is uncertain, the falsification can be detected by comparing the demodulated signals.

In this paper, the ability and the effectiveness of the proposed method are shown by some experimental results.

2. Chaotic Modulator

First, chaotic modulator and chaotic demodulator are shown as follow equations [7]:

Modulators;

$$\begin{aligned} x_{k1}(n) &= S_k(n) - g_k(x_{k1}(n-1)) + \alpha_k x_{k3}(n-1) \\ &\quad +\theta_k \qquad (1) \\ x_{k2}(n) &= x_{k1}(n-1) - \beta_k x_{k2}(n-1) \\ &\quad -\gamma_k x_{k3}(n-1) \qquad (2) \\ x_{k3}(n) &= x_{k2}(n-1) \qquad (3) \\ S_{k+1}(n) &= x_{k1}(n) \qquad (4) \end{aligned}$$

Demodulators;

$$\begin{aligned} r_k(n) &= x_{k4}(n) + g_k(x_{k4}(n-1)) - \alpha_k x_{k6}(n-1) \\ &\quad -\theta_k \qquad (5) \\ x_{k5}(n) &= x_{k4}(n-1) - \beta_k x_{k5}(n-1) \\ &\quad -\gamma_k x_{k6}(n-1) \qquad (6) \\ x_{k6}(n) &= x_{k5}(n-1) \qquad (7) \\ x_{(k-1)4}(n) &= r_k(n) \qquad (8) \end{aligned}$$

Datadelivery :

$$x_{M4}(n) = x_{M1}(n) \qquad (9)$$

$$g_k(x) = \begin{cases} \kappa_k x + \sigma_k & (x \le -\varepsilon_k) \\ \frac{\kappa_k \varepsilon_k - \sigma_k}{\varepsilon_k} x & (-\varepsilon_k < x < \varepsilon_k) \\ \kappa_k x - \sigma_k & (x \ge \varepsilon_k) \end{cases} \qquad (10)$$

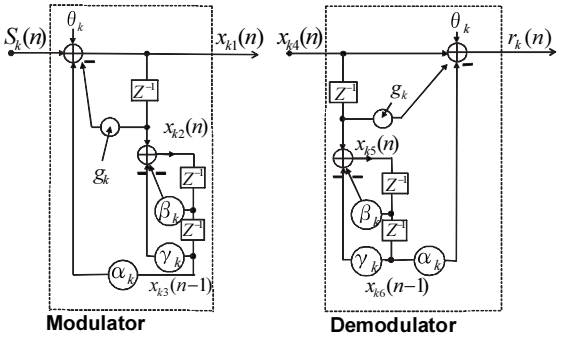

Fig. 1: Block diaglam of chaotic modulator and chaotic demodulator on step k

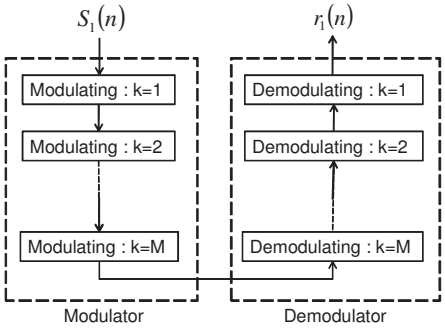

Fig. 2: Cascade structured chaotic modulator and chaotic demodulator

Figure 1 shows the structure of chaotic systems. The cascade structured chaotic modulator is shown in Fig. 2.

Where, the $S_k(n)$ shows the information signal that should be encrypted on step k, $x_{k1}(n) \sim x_{k6}(n)$ are the internal state variables of the system. The variables, α_k, β_k, γ_k, κ_k, θ_k, ϵ_k, are parameters that decide characteristic of the system. In Eq. (1) and Eq. (5), $g_k(x)$ is a nonlinear function that is shown in Eq. (10). In this system, all parameters and variables are expressed by 16-bit fixed point values and calculated [8].

In this system, chaotic signals and information data are associated by convolution. Considering the robustness against the cracking of the chaotic signals, the chaotic system used in this study is better than conventional system such as the system using PN list and exclusive OR. In addition, this system has an advantage in the varieties of initial parameters. However, this system that is shown in Eq. (1) $\sim$ Eq. (10) is not the only system for our proposed method. The systems, which have characteristics discussed above, are accepted for our proposed method.

3. JPEG

In the JPEG image process, at first, the RGB element of the source image converts to YCbCr element. Then, minimum coded unit (MCU) is decided. MCU has six element blocks: four Y element blocks, Cb element block, and Cr element block.

In the process of JPEG compression, the discrete cosine transformation (DCT) is done each MCU, after that, the DCT coefficients are quantized with the quantization table. Then the DCT coefficient is encoded.

A zigzag scanning is very important operation in the process of JPEG compression. The zigzag scanning is showed in Fig. 3. The zigzag scanning is based on that DCT coefficient appears only lower frequency area in the quantum DCT coefficient block.

In this paper, after this, DCT coefficient is shown as AC(k) (k=1,2, $\cdots$,63). However, AC(0) is excluded because it shows DC element and is not used to embed watermark information.

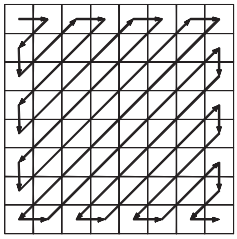

Fig. 3: Zigzag scan seaquense

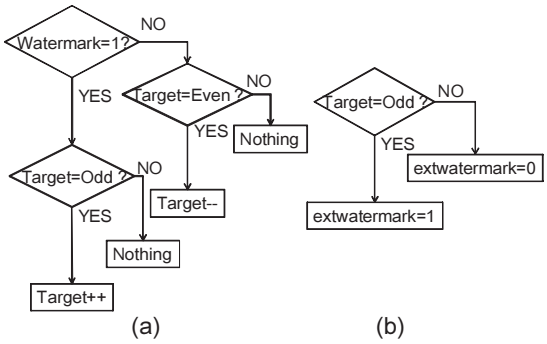

Fig. 4: Algorism of watermark embedding (a) and algorism of watermark extracting (b) (Method of replacing LSB). "watermark," "target," "Odd," "Even"and "extwatermark" mean watermark bit, DCT coefficient of watermark embedding coordinates, the odd number, the even number and watermark bit that taken out.

4. Embedding Method to JPEG Images

In this study, two conventional methods of embedding watermark information are used. One is a method that replace least significant bit (LSB) of DCT coefficient by the watermark bit 0 and 1 [8]. The other method is replacing AC(63) by the watermark bit 0 and 1 [3, 4]. When the watermark is embedded by replacing DCT coefficient, the value of the quantization table, which is corresponding to

the watermark embedding position, is changed to 1.

Replacing LSB of DCT coefficient is achieved to reverse even number and odd number of DCT coefficient. And this is achieved by adding 1 or subtracting 1 from the value of DCT coefficient. The embedding algorithm is shown in Fig. 4.

5. Proposed Method

Detail of proposed method is explained follows.

First, 8-bit alphanumeric characters are decided as original digital watermark information. Each character is modulated to the chaotic signal. Then two different chaotic signals with different parameter are generated from one character by cascade structured chaotic system (Fig. 2). The output of step k is shown as $x_{k1}(n)$. Equation (11) shows $x_{k1}(n)$ as bits.

$$x_{k1}(n) = \{a_{k15}, a_{k14}, \cdots, a_{k1}, a_{k0}\} \tag{11}$$

The chaotic watermark bits are shown as $a_{k15}(n)$, $a_{k14}(n)$, $\cdots$, $a_{k1}(n)$, $a_{k0}(n)$.

Next, two outputs of the chaotic modulator, $x_{11}(n)$ and $x_{21}(n)$, are embedded to DCT coefficient block because the number of steps is decided as two (M=2) in Fig. 2. The watermark information is embedded 1-bit a block of DCT coefficient in each technique.

By embedding these chaotic signals as the digital watermark data, the falsification of JPEG images is detected because of the Sensitive Dependence on Initial Conditions and Orbital Instability of chaos. When the images are attacked, the orbit of chaos begins to shift at once and a correct decoding becomes impossible even if the error is 1-bit. Therefore the falsification is detected by checking whether the two decoded information accord or not. Moreover, even if the watermark information is uncertain, the falsification is detected by embedding two chaotic watermark information and comparing information decoded form two chaotic watermark information.

6. Experiments

The image, Lenna (256×256), Barbara (720×576), and Baboon (500×480) are decided as source images of experiments and the characters, "tested in Meiji University." is decided as original watermark information. Peak signal to noise ratio (PSNR) is used to evaluate the quality of the image that is embedded watermark information.

First of all, the experiment that verifies the best embedding position in the embedding method of the watermark by reversing LSB is conducted. In this experiment, all LSB of DCT coefficients are reversed.

The result is show in Fig. 5. In Fig. 5, PSNR is better when LSB of the low frequency element of DCT coefficient block is reversed than when LSB of the high frequency element of DCT coefficient block is reversed. Therefore,

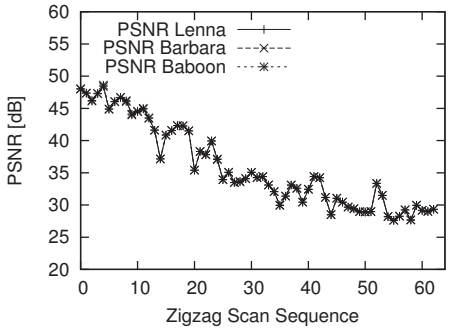

Fig. 5: Variation of PSNR with embedding position of watermark information(Method of reversing LSB of DCT coefficient)

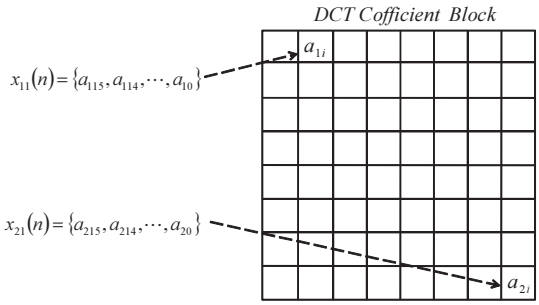

Fig. 6: Enbedding possition of chaotic bit to the DCT coefficient block

$AC(1)$ is decided as embedding position of the method reversing LSB. The embedding positions of chaotic watermark bits are shown in Fig. 6

The result of embedding the watermark by the replacement of DCT coefficient and by reversing LSB of DCT coefficient is shown in Fig. 7 and Table 1. In the result of each image, the file size of JPEG image by proposed method is increased.

The reason why the file size of JPGE image by proposed method is increased is that the efficiency of JPEG compression is felt by embedding watermark information to $AC(63)$. To decrease the file size of JPEG image by proposed method, the quantization parameter should be adjusted. Moreover, it doesn't matter about deterioration of the image if we can use special JPEG decoder that recovers changed DCT coefficient.

One of the results of falsification detection is shown in Fig. 8 and Fig. 9. Figure 8 shows the result of detection with no errors and Fig. 9 shows the result of detection with bit errors. In Fig. 9, the characters are garbled. This is caused by bit error that is added deliberately. And thus, it is impossible to decode chaotic signals correctly because of the Sensitive Dependence on Initial Conditions and Orbital Instability of chaos when the bit-error exists in watermark information. In addition, it is impossible to decode chaotic signals correctly in the experiment of recompression.

(a) (b)

Fig. 7: (a)Lenna without chaotic watermark bits(JPEG), (b)Lenna with chaotic watermark bits(JPEG)

Table 1: Result of enbedding chaotic watermark to each image

	Lenna	Barabara	Baboon
PSNR [dB]	50.67	50.86	50.87
File Size [Bytes]	9,454	56,567	42,941
File Size Ratio 1 [%][1]	140	142	124
File Size Ratio 2 [%][2]	4.80	4.54	5.96

1: The file size ratio of JPEG image without watermark information and JPEG image by proposed method.

2: The file size ratio of source image and JPEG image by proposed method.

These results of some experiment show the ability and the effectiveness of the proposed method.

7. Conclusion

In this paper, the ability and the effectiveness of the proposed method are shown by embedding two chaotic signals as watermark information. By embedding chaotic watermark information to two places, the falsification is detected by comparing decoded information from them. Furthermore, even if the two watermark bits are changed to the same, the falsification can be detected because of the difference of an initial state of the system and difference of parameters.

In the future, the direction of embedding watermark bit will be changed to detect falsification efficiently and to detect falsified positions. At the same time, the sensitivity of chaotic watermark bits against malicious attack will be discussed with Stirmark benchmark.

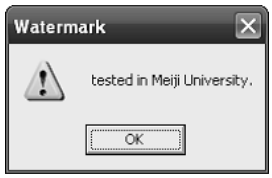

Fig. 8: Result of falsification detection with no errors

Fig. 9: Result of falsification detection with bit-errors

References

[1] Toyokawa, N. Morimoto, S. Tonegawa, K. Kamijo, and A. Koide, "A Method to Protect and Detect Alterations of Digital Photographs in Insurance Claim Process," *technical report of IEICE. IE,* vol. 99, no. 303, pp.1-8, Sep. 1999.

[2] Kamijio, S. Tonegawa, K. Toyokawa, and N. Morimoto, "A Method to Protect and Detect Alterations of Digital Photographs in Insurance Claim Process(II)," *technical report of IEICE. OFC,* vol. 99, no. 595, pp. 55-60, Jan. 2000.

[3] Kobayashi, Y. Noguchi, and H. Kiya, "A Method of Embedding Binary Data into JPEG Bitstreams," *IEICE D-II,* vol. J83-D-II, no. 6, pp.1469-1476, June. 2000.

[4] Noguchi, H. Kobayashi, and H. Kiya, "A method of Extracting Embedded Binary Data from JPEG Bitstreams Using Standard JPEG Decoder," *IEICE Trans. Fundamentals,* vol. E83-A, no. 8, pp. 1582-1588, Aug. 2000.

[5] Seki, H. Kobayashi, M. Fujiyoshi, and H. Kiya, "A Data Hiding Method without Specifying Embedded Positions for JPEG Image," *IEICE D-II,* vol. J88-D-II, no. 10, pp.2037-2045, Oct. 2005

[6] Choi, and K. Aizawa, "Watermarking Using Inter-Block Correlation: Extension to JPEG Coded Domain," *IEICE Trans. Fundamentals,* vol. E84-A, no. 3, pp. 893-897, Mar. 2001.

[7] Y. Abe, K. Tsutsumi, H. Kamata, and T. Endo, "Private communications using chaotic neurons with cascade structure,"

[8] H. Kamata, Y. Umezawa, T. Dobashi, T. Endo and Y. Ishida, "Private Communications with Chaos Based on the Fixed-Point Computation.," *Trans. IEICE,* vol. E83A, no. 6, pp. 1238-1246, 2002.

[9] Matsui, "Image deep cipher," *Morikita Publishing,* pp. 80-118, Jun. 1993.