Secure Spread Spectrum Watermarking Algorithm Based on Chaotic Map for Still Images

Rinaldi Munir[1*], Bambang Riyanto[2], Sarwono Sutikno[3], Wiseto P. Agung[4]

[1,2,3] *Bandung Institute of Technology, Jalan Ganesa 10, Bandung 40132, Indonesia*
[2] *PT. Telekomunikasi Indonesia, Jl. Gegerkalong, Bandung, Indonesia*

In this paper, a chaos-based spread spectrum watermarking algorithm is developed in the DCT domain for still image. The most important feature of chaos is its sensitivity to initial conditions. This characteristic makes chaos has been used successfully for secure watermarking and encryption. In our algorithm, we use logistic map to produce pseudo-random sequence. We use the logistic map twice: one is to encrypt the embedded position and other to generate pseudo-noise sequence. The encryption to embedding position can prevent the watermark from removing ilegally, so the security can be improved better. We also use binary meaningful watermark image so that the contents of the watermark is known. The binary image is extracted without using original image. We have also tested robustness of the proposed algorithm against various attacks using common image processing (JPEG compression, cropping, resizing, and noising). Simulations have confirmed that this algorithm is robust against the typical attacks. The extracted watermarks still can be recognized visually.

1. Introduction

Recently, with the emergence of computer network and internet, lots of digital multimedia data are easily copied, stored and transmitted over the world, leading to illegal copy or unauthorized use. Digital watermarking has been used widely as a tool for protecting copyright of digital multimedia data (e.g images). A watermark is inserted into digital images so that it is imperceptible to a person. The watermark must also be robust to typical signal processing operation such as JPEG compression, cropping, resizing, noising, rotation, and so on.

Many digital watermarking algorithms for still images have been proposed. Most of them are based on spread spectrum watermarking technique. Spread spectrum watermarking scheme consists of two processes. The first process is embedding of watermark into image. A sequence of watermark bits we want to hide in the image is spread by a large factor constant, then the amplitude of spread sequence is amplified, and modulate it with a binary pseudo-noise sequence that behaves as watermark's key. Finally, the modulated signal is added to the image, yielding a watermarked image. The second process is detecting of watermark from a test image. This process is easily accomplished by multiplying the test image with the same key that was used in embedding and then sum all of results for each watermark bit. The watermark bits can be recovered by tresholding.

In this paper, we present a chaos-based spread spectrum watermarking algorithm for still images. We use a chaotic map to produce a pseudo-random signal that behaves as embedding and detecting key. In recent years, chaotic map have been used for digital watermarking, to increase security [2]. The most important feature of chaos is its sensitivity to initial conditions. It means if two initial conditions are chosen very close to each other, the distance between their successive orbits under chaotic map diverges exponentially. Hence, a chaotic map can be used as a pseudo-random generator [3].

We also use a binary image resembling logo as watermark. At present, most of watermark that was used in watermarking scheme is a unmeaningfull pattern, so the user does not know the content of information. We design a chaos-based spread spectrum watermarking algorithm that uses binary meaningful watermark image. The binary image is extracted without using original image. The main goal of this algorithm is to design a secure watermarking technique by using a chaotic sequence to encrypt embedding position of watermark. Furthermore, encryption to embedding position can prevent the watermark from removing ilegally, so the security can be improved better [3].

The paper is organized as follows. Firstly, we will present spread spectrum watermarking. Next, we will present chaotic map. Then, we will present chaos application to spread spectrum watermarking and the experimental results; and we will finish by a conclusion.

2. Spread Spectrum Watermarking

The basic idea of spread spectrum watermarking for digital image involves the addition of a pseudo-random signal to the image that is below the threshold of perception and that cannot be identified and thus removed without knowledge of the parameters of the watermarking algorithm [1]. The pseudo-random signal behaves as watermark for the image. The signal can be a binary pseudo-noise sequence. Non binary sequence is also possible.

2.1 Embedding Scheme

Let A is the information (watermark in our scheme) we want to hide in the image, as follows:

$$A = \{a_i \mid a_i \in \{-1 , 1 \}\}. \quad (1)$$

Each bit a_i then spread by a large factor cr, called chip-rate, to obtain the spread sequence:

ISBN 978-979-16338-0-2

$$B = \{b_i \mid b_i = a_j, \quad j \cdot cr \le i < (j+1) \cdot cr\}. \qquad (2)$$

The spread bit b_i is modulated by a binary pseudo-noise sequence

$$P = \{p_i \mid p_i \in \{-1, 1\}\} \qquad (3)$$

and then its results is amplified with a watermarking strength factor α, to form the spread spectrum watermark

$$w_i = \alpha \cdot b_i \cdot p_i \qquad (4)$$

The watermark w_i is added to image $V = \{v_i\}$ yielding a watermarked image

$$\hat{v}_i = v_i + w_i \qquad (5)$$

Due to the noisy nature of p_i, w_i is also a noise-like signal and thus difficult to detect, locate, and manipulate [4]. The watermark embedding scheme is visualized in Fig. 1.

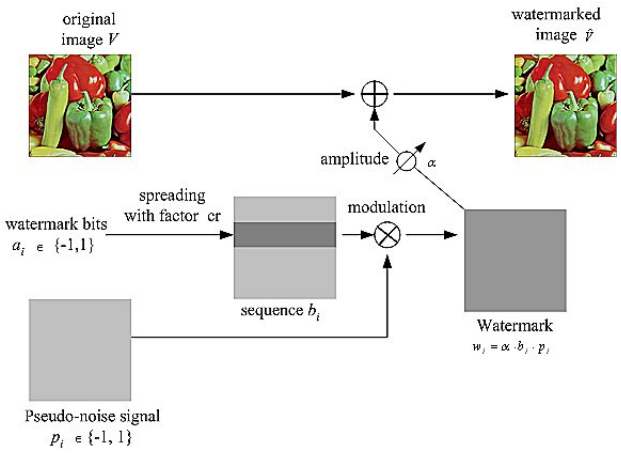


Fig. 1. Watermark embedding

2.1 Extracting Scheme

To extract watermark from a test image, receiver must have the same pseudo-noise p_i that was used in embedding process. Extraction of watermark is accomplished by multiplying the watermarked image with p_i:

$$\sum_{i=j\cdot cr}^{(j+1)\cdot cr-1} p_i \cdot \hat{v}_i = \sum_{i=j\cdot cr}^{(j+1)\cdot cr-1} v_i \cdot p_i + \sum_{i=j\cdot cr}^{(j+1)\cdot cr-1} \alpha \cdot b_i \cdot p_i^2 \qquad (6)$$

Because p_i is random, cr is large, and deviation of v_i is small, it can be expected that

$$\lim_{cr \to \infty} \sum_{i=j\cdot cr}^{(j+1)\cdot cr-1} v_i \cdot p_i \approx 0 \qquad (7)$$

So since $p_i^2 = 1$, equation (6) yield the correlation sum:

$$\sum_{i=j\cdot cr}^{(j+1)\cdot cr-1} \hat{v}_i \cdot p_i = \alpha \cdot cr \cdot a_j \qquad (8)$$

Therefore the embedded bits can be recovered by using the following equation:

$$a_j = \begin{cases} 1, & \sum_{i=j\cdot cr}^{(j+1)\cdot cr-1} \hat{v}_i \cdot p_i > 0 \\ -1, & \sum_{i=j\cdot cr}^{(j+1)\cdot cr-1} \hat{v}_i \cdot p_i < 0 \end{cases} \qquad (9)$$

The watermark extracting scheme is visualized in Fig. 2.

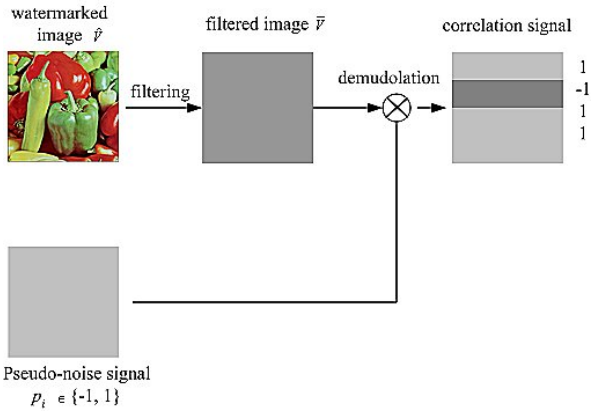


Fig. 2. Extraction of watermark

To aid the correlation step, the test image is filtered by a highpass filter as Wiener filter or edge detection filter. The filtering can remove major components of the image from the superposition of watermark and image [1].

3. Chaos and Its Application to Watermarking

One of the characteristic of chaotic systems is a sensitivity to initial conditions; i.e two relatively close initial value will diverge as the system evolves. As a result of this sensitivity, the behavior of systems appears to be random, even though the system is deterministic; i.e it is well defined and contains no random parameters. Hence, a chaotic system can be used as a pseudo-random generator. It means a large number of non-periodic, noise-like yet deterministic and reproducible sequences can be generated [5].

We consider a 1-D discrete chaotic map $\mathbf{F} : U \to U$, $U \subset \mathbf{R}$, which provides sequence of real number:

$$z(n+1) = \mathbf{F}(z(n), \lambda) \ , \ z(n) \in U, \lambda \in \mathbf{R} \qquad (10)$$

where n = 0, 1, 2, … denotes map iterations and λ is a parameter that controls the dynamic behavior of the chaotic map. In our scheme, an initial value of chaotic map behave as the key of the watermarking system.

One of the simplest chaotic maps is *logistic map*, which is a recurrence relation that describes population growth over time, desribed by

$$x_{k+1} = \mu x_k (1 - x_k) \qquad (11)$$

where $0 \le \mu \le 4$. When $3.6 \le \mu \le 4$, the map is in the chaotic state (bifurcation diagram of a logistic map is visualized in Fig. 3, displaying chaotic behavior). After the generated sequence real number is quantified, a binary sequence $s(n) \in \{0, 1\}$ is produced with approximately equal number of 1's and 0's.

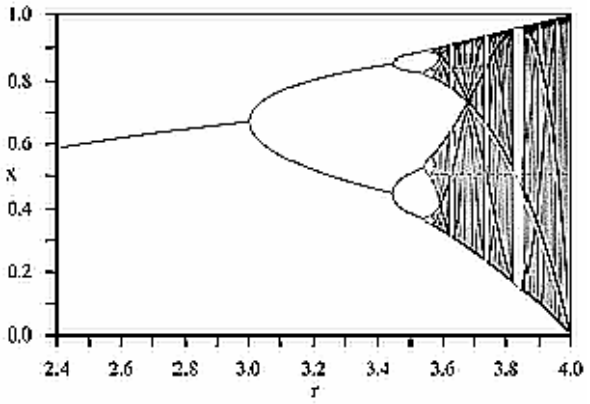


Fig. 3. Bifurcation diagram of a logistic map

In our scheme, we use logistic map to produce pseudo-random sequence. We use logistic map twice: one is to encrypt the embedded position and other to generate p_i sequence.

4. Proposed Scheme

We propose a modified spread spectrum watermarking technique to produce a secure algorithm using chaos. We use chaotic map to generate pseudo-random sequences The watermark is binary image like logo or other meaningfull image. For convenience, let us assume that the image has 256 grey levels and $N \times M$ pixels. We assume that the watermark in 2-D have been converted to an linear array A.

4.1 Watermark Embedding Algorithm

To insert watermark into an image we use the following process:

1. We first transform the original image in the frequency domain by using DCT transform. Save all coefficient of transformation into vector V.
2. Spread A by factor cr to obtain sequence B using eq. (2). Suppose length of B is L.
3. Generate pseudo-noise sequence P as follow: generate first chaotic sequence S_1 by using logistic map under an initial value, i_1. Length of the sequence is equal to L. Then, we set a threshold T_w to convert element of sequence (in real value) into binary element (+1/-1), as describe by the following formula:

$$p(i) = \begin{cases} 1 & S_1(i) > T_w \\ -1 & S_1(i) \le T_w \end{cases} \qquad (12)$$

4. Next, encrypt embedding position of watermark as follow: we must specify secret positions for embedding watermark. So, we generate the second chaotic sequence, S_2, by using logistic map under an initial value, i_2 (generally $i_1 \neq i_2$). Then, convert element of sequence (in real value) into integer by multiplying each element by $N \times M$ and then round it toward infinity. We must ensure that there are L different position of embedding.
5. The spread spectrum watermark is embedded into V, except DC value, by using equation (4) and (5) on secret positions that specified at step 4 above (Fig 4).
6. Finally, apply inverse DCT to reconstruct the watermarked image.

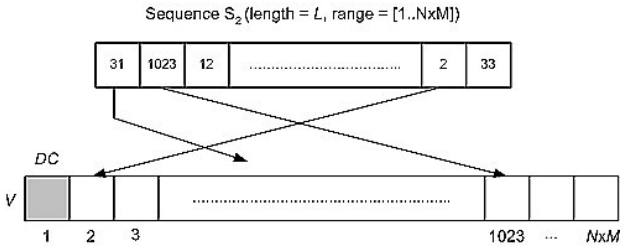


Fig. 4. Embedding watermark bits into V on secret position that specified by sequence S_2.

4.2 Watermark Extracting Algorithm

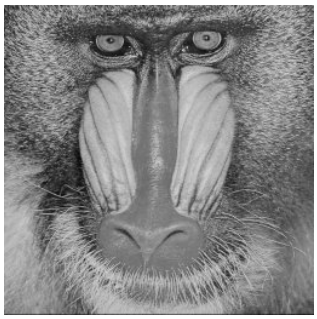
To extract watermark from a test image we use the following process:

1. We first transform the test image in the frequency domain by using DCT transform. Save all coefficient of transformation into vector $\hat{V}$.
2. Generate the same pseudo-noise P that was used in embedding process by using logistic map.
3. Generate the same secret positions that was used in embedding process by using logistic map.
4. Recover bits of the watermark A by using equation (9).

5. Experiment Results

We program the watermarking algorithm above by using MATLAB 7, and then the watermarked image is tested with some typical attacks. The attacks are JPEG compression, adding noise, resizing, and cropping. The test image is a 256 × 256 gray image 'baboon' and watermark is a 64 × 64 a binary image 'alpha' (Fig 4). Two chaotic sequences are generated in that the initial values are 0.25 (first key) and 0.36 (second key). We use α = 6.0 for watermarking strength factor and spreading factor cr = 60.

ISBN 978-979-16338-0-2



'baoon' (256 × 256)

Watermark(32 x 32)

Fig 4. Original image and *watermark*

The similarity measurement between referenced watermark A and extracted watermark $\tilde{A}$ is defined by:

$$sim = \frac{\sum_i \sum_j A(i,j)\tilde{A}(i,j)}{\sum_j \sum_j |A(i,j)|^2} \qquad (13)$$

If exact matchs occurs, then sim = 1. The threshold of the judgement is set to 0.52 [3].

Fig 5 shows the watermarked image and extracted watermark where no attack done. The watermarked image has PSNR = 32.84 and similarity between original watermark and extracted watermark is 0.9023 (not identic but it still can be recognized). When we use larger *cr* (not 60 in this experiment), we can get better result.

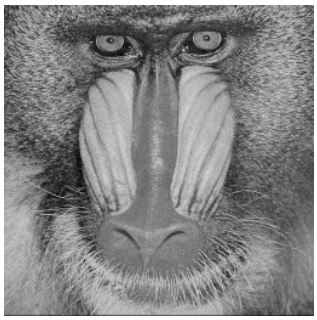


Fig 5. Watermarked image extracted watermark

Because of chaotic system is sensitive to initial condition, so a little change to initial value of chaotic map results significant error in watermark extracting process. Fig 6 shows original watermark and extracted watermark when i_2 (initial value for generating secret positions of embedding) in watermark extracting process is changed from 0.36 into 0.36001.

Fig 6. Original watermark and error extracted watermark when initial value of chaotic map is changed a little.

We have also tested robustness of the proposed scheme against various attacks using common image processing (JPEG compression, cropping, resizing, and noising). We use *Jasc Paint Shop* version 6.01 as image processing software. Fig 7 shows the extracted watermarks under the common image processing. Obviously, the extracted watermarks are still recognizable (all similarity measurement are above specified threshold).

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

Fig 7. Extracted watermarks under various attacks. (a) JPEG compression (sim = 0.82). (b) Cropping 25% (sim = 0.79). (c) Doubling size (sim = 0.71). (d) Adding random noise/salt and peppers 10% (sim = 0.73).

6. Conclusion

In this paper a secure spread spectrum watermarking algorithm based on chaotic map for still image has been proposed. This algorithm applies DCT, based on logistic map, and embed watermark into the DCT coefficient. During watermak embedding, the chaotic sequence is used twice: one is to encrypt the embedded position and other to generate pseudo-noise sequence. We also use binary meaningful watermark image. The binary image is extracted without using original image. Simulations have confirmed that this algorithm is robust against several common image processing (JPEG compression, resizing, cropping, and adding noise). The extracted watermarks still can be recognized visually.

References

1. F. Hartung, and B. Girod, "Fast Public-Key Watermarking of Compressed Video", Proceedings of the 1997 International Conference on Image Processing (ICIP '97).
2. Zhao Dawei, Chen Guanrong, Liu Wenbo, "A Chaos-Based Robust Wavelet-Domain Watermarking Algorithm", Chaos, Solitions and Fractals 22 (2004) 47 – 54.
3. Weiwei Xiao et al, "A Watermarking Algorithm Based on Chaotic Encryption", Proceeeding of IEEE TENCON 2002.
4. Jiying Zhao et al, "A video Copyright Protection System Based on ContentID", IECE Trans. Inf. & Syst., Vol. E83-D, No. 12 December 2000.
5. Hongxia Wang, "Public Watermarking Based on Chaotic Map", IECE Trans. Fundamentals, Vol. E87-A, No. 8 August 2004.

ISBN 978-979-16338-0-2