저장 한계를 극복한 효율적인 디지털 워터마크 생성 방법 연구

A Study on Effective Digital Watermark Generation Method to Overcome Capacity Limit

조대제, 김희선
안동대학교 전자정보산업학부

Dae-Jea Cho(djcho@andong.ac.kr), Hee-Sun Kim(hskim@andong.ac.kr)

요약

기존의 디지털 워터마킹 방법에서는 주로 PN-수열을 사용하여 산출된 이진데이터를 디지털 워터마크로 사용하였다. 이 방법은 영상의 크기가 작은 경우, 제한된 크기의 원 영상에 삽입 할 수 있는 워터마크의 크기는 한계가 있다.

본 논문에서는 혼돈 함수에 의하여 산출되는 혼돈수열을 이용하여 디지털 워터마크를 생성하고, 이를 사용하는 방법을 제시하였으며, 이것이 기존의 PN-수열을 대신하여 사용할 수 있음을 보였다. 또한 워터마크로 사용될 임의의 문장을 혼돈 수열로 변환하는 방법을 제시하였다.

실험을 통하여, 임의의 문장을 디지털 워터마크로 변환하여 원본 영상에 삽입하고 이를 추출하여 다시 원래의 문장으로 복원하는 과정을 구현하였다.

본 논문에서 제시한 알고리즘은 긴 문장을 짧은 혼돈 수열로 함축하는 방법을 사용하여 기존의 방법에 비해 보다 많은 정보를 원본 영상에 숨길 수 있기 때문에, 제한된 저장 한계를 극복할 수 있었다.

■ 중심어 : | 디지털 워터마크 | 인증 | 혼돈 수열 | JPEG 압축 | PN-수열 |

Abstract

During the design of a successful digital watermarking systems, Pseudo-Noise(PN) sequences are widely used to modulate information bits into watermark signals. In this method, the number of bits that can be hidden within a small image by means of frequency domain watermarking is limited.

In this paper, we show the possibility of introducing chaotic sequences into digital watermarking systems as potential substitutes to commonly used PN-sequences. And we propose a method that transforms the text to chaotic sequence.

In our current implementation, we show how the sample text is expressed by an implied unit data(watermark) and the implied unit data is regenerated into the original text.

Because we use this implied data as watermark for information hiding, we can insert much more watermark compared with previous method.

■ Keyword : | Digital Watermark | Authentication | Chaos Sequence | PN-Sequence |

* 본 연구는 2005년도 교육인적자원부 NURI사업 공동연구비 지원에 의해 수행되었습니다.

접수번호 : #051012-001
접수일자 : 2005년 10월 12일
심사완료일 : 2005년 11월 25일
교신저자 : 조대제, e-mail : djcho@andong.ac.kr

I. Introduction

Digital watermarking is a technique to insert a digital signature into an image so that the signature can be extracted for the purposes of ownership verification and authentication. This type of technology is becoming increasingly important due to the popularity of the usage of digital images on the World Wide Web and in electronic commerce[1].

Those watermarks are embedded into the images, and have the following features[2-4].

- Difficult to notice: It means 'imperceptible'. A watermark signal in an original data is noise to itself. So watermark signal must not distort the original data. If it is visually detected, the media data that a watermark is inserted into is not worthy of itself.
- Robustness: As watermark information is mixed with an original data, the watermarked data does not increase data size. And watermarked data can be changed by applying signal processing - low pass filtering, rotation, zoom in, zoom out, cut etc - on it. But, at least, applying any processing on watermarked data must not change a watermark information.
- Tamper-resistance: Sometimes we need to add new watermark signal to the watermarked data. Also we need to remove the signal from the data. Watermark data is required to be robust to a legitimate signal distortion and so watermarking system needs tamper-resistance.
- Scalability: Besides, the watermarking system requires scalability. We can not say that present methods are also good in the future. In later when an improved system is designed, past methods and improved methods can be used simultaneously.

During the design of a successful digital watermarking systems, Pseudo-Noise(PN) sequences are widely used to modulate information bits into white noise-like wide band watermark signals to be added into the cover objects including video, audio, images or text. They have already been extensively used in spread-spectrum communication systems and stream ciphers because of their noise like characteristics, resistance to interference, and good Auto-Correlation Functions(ACF).

The most widely used PN-sequences are Maximum length linear feedback shift register sequences(m-sequences), which are generated by Linear Feedback Shift Register(LFSR) of fixed length m. They are periodic, noise-like and binary. The feedback polynomial of the LFSR is defined as:

$$f(x)= c_0+c_1x+c_2x +...+c_{n-1}x^{n-1}+x^n \qquad (1)$$

Where, coefficients c_l are binary feedback constants. And the arithmetic addition is modulo two. The output sequences are periodic and their periods are determined by the properties of feedback polynomials $f(x)$, which also called as characteristic polynomial. An m-sequence has the maximum period, 2^m-1, and corresponds to the case when the feedback polynomial is primitive. In fact, There is a one-to-one correspondence between polynomials of degree less than m and the set of 2^m-1 output sequences of the LFSR corresponding to the 2^m-1 non-zero possible initial conditions.

The ACF's of m-sequences are very desirable and they have noise-like characteristics. That is the reason for its popularity.

In a recent paper, Goffin et al.[5] use m-sequences to generate orthogonal code words to spread the information bit stream and every researchers also use m-sequences to generate watermark signals. In fact, in the historical paper in literature, they use an m-sequence as the watermark signal, which is considered as an important concept in watermarking.

However, there are some disadvantages exist for m-sequences. For example, large spikes can be found in their cross-correlation functions, especially when partially correlated. Another drawback of m-sequences is that they are relatively small and periodic characteristics[6].

However, chaotic sequences have several good properties including the availability of a great number of them, the ease of their generation, as well as their sensitive dependence on their initial conditions.

Almost watermarking methods are assumed to consist in the modification of a set of full-frame DCT(DFT) coefficients. As the amount of modification each coefficient undergoes is proportional to the magnitude of the coefficient itself, so that an additive-multiplicative embedding rule results. The number of bits that can be hidden within an image by means of frequency domain watermarking is limited[7].

To solve this problem, we compress the watermarks using chaotic function. The predictive characteristic of chaotic function makes it possible.

In this paper, we propose a method that transforms the sample text to chaotic sequences. And we present how the sample text is expressed by an implied data and the implied data is regenerated into the original text. We use this implied sample text as digital watermarks. The rest of the paper is structured as follows: in section 2, we describes characteristic of deterministic chaos function. And in section 3, we propose new watermark generation algorithm. In section 4, experimental results are shown, and last section gives conclusions and direction for future works.

II. Deterministic chaotic function

Chaotic sequences have several good properties including the availability of a great number of them, the ease of their generation, as well as their sensitive dependence on their initial conditions.

Chaotic sequences are derived from the discrete time dynamical system. Perhaps the simplest example of a nonlinear dynamical system is the celebrated logistic map. A discrete time dynamical system can be defined as following equation. It is logistic map[8]:

$$x_{n+1} = ax_n(1- x_n) \qquad (2)$$

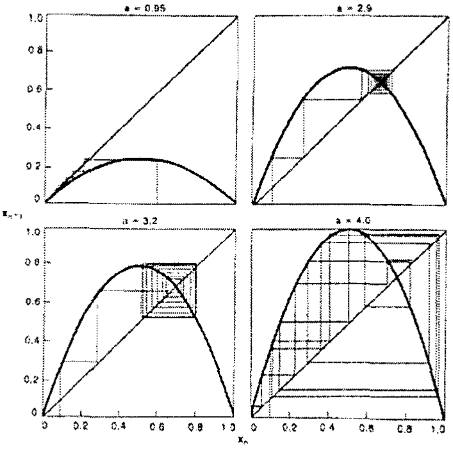


Figure 1. Characteristics of logistic map

[Figure 1] shows characteristics of logistic map(equation 2). When a is less than 1, as in the graph at the upper left, all initial conditions converge to 0. When a is increased to a value between 1 to 3, as in the upper right, almost all initial conditions are attacked to a fixed point. When a is larger than 3, however, the fixed point becomes unstable; at a=3.2 there are two fixed points between which the value for x eventually oscillates. As a continues to increase, there can be more and more fixed points, and for many values of a, as when a=4, the values for x wander over entire intervals in an apparently random fashion[8][9].

That is to say, it has been proved in literature of chaotic dynamical systems that when $1<a\leq3$, x_{n+1} is converged and when $3<a\leq3.57$, x_{n+1} is diverged. But when $3.57<a\leq4$, logistic map will operate in chaotic state. That is to say, the sequence $\{x_n\ ;\ n=0,1,2,3,...\}$ it produced with initial condition x_0 will be non-periodic and non-converging.

The characteristics of chaotic systems are very sensitive to their initial conditions. For example, given two very close initial conditions, after several iterations of the map, the two resulting sequences will appear totally uncorrelated. That is to say, if we make a slight change in the initial condition will produce a completely different sequence. Thus, a large number of uncorrelated, random-like, yet deterministic and reproducible chaotic signals can be generated with small perturbation of the parameters.

This makes them candidates to be used in a wide range of fields including digital communication, cryptography, etc. The advantages of chaotic sequences can be concluded as follows[3]:

- Compact description: only the parameter of the chaotic map and its initial condition are needed to regenerate the sequences. There is no additional burden to store the whole long sequences
- Sensitive to initial conditions: we can easily produce an abundant of almost uncorrelated sequences. And in most cases, the initial condition of a system can not be deduced from a finite length of the sequence. That is important from the view of security.
- Noise like and non-periodic characteristics

III. Watermark generation algorithm

We use the chaotic sequences generated by discrete-time dynamical systems operating in chaotic state.

3.1 Text implication algorithm

In this section, proposes a method that transforms the sample text to chaotic sequence. And we present how the sample text is expressed by an implied data. The sample text implication procedure is described below:

Step1: The sample text is converted to the discrete signal code using figure 2.

Step2: The discrete signal code is converted to chaotic area using following function:

$$mhh=h_{max}+h_{min}+1.0 \quad (3)$$

$$g_i=(h_i+h_{min})/mhh \quad (4)$$

Where, h_{max} and h_{min} are maximum and minimum value in the discrete signal code set. And h_i is the i-th discrete signal code.

Step3: Generate new chaotic sequences using equation 2 with seed value CX_0.

Step4: Find the closest value CX_1 to $g1$ in the chaotic sequences.

Step5: Compute new seed value by subtracting index value from CX_1.

Step6: The procedures 3, 4, 5 are repeated to all chaotic sequences until final value CX_n is computed.

Step7: Finally, convert CX_n to binary code.

This binary code is final watermarks that we insert into image in this paper.

3.2 Text restoration algorithm

In this section, we explain a method that regenerates the implied chaotic sequence to the original sample text. As above chaotic function has not its inverse function, one part of implication procedure is repeated. The sample text restoration procedure is described below:

Step1: First, extracted watermark data(binary code) is converted to CX_n.

Step2: Generate chaotic sequence s_{11} using equation 2 with seed value CX_0.

Step3: Compute SX_1 by subtracting index value from s_{11}.

Step4: Generate chaotic sequence s_{21} using equation 1 with new seed value SX_1.

Step5: Compute SX_2 by subtracting index value from s_{21}.

Step6: The procedure 3, 4, 5 are repeated until find SX_n that is equal to CX_n. If SX_n is equal to the implied value CX_n, find prediction values $s_{11}, s_{21}, \ldots, s_{n1}$.

Step7: Restore to the discrete signal code using following inverse function:

$$h_n = g_n(h_{max}+h_{min}+1.0) - h_{min} \tag{5}$$

IV. Experimental results

In order to implement our proposal, we use P.C and C++ in Windows environment. [Figure 2] is the character code converting table. In this figure, 26 characters, 9 special characters and 1 blank are mapping to 36 signal codes. One character is converted into four digit binary code.

We represent the original sample text and converted binary watermarks in [Figure 3]. Single text is implied to 40 bits binary data. Even if the text is long sentence, we can get implied values using this method.

Characters	Signal Code	Characters	Signal Code
a	10	!	280
b	20	@	290
c	30	#	300
:	:	$	310
:	:	%	320
x	240	–	330
y	250	&	340
z	260	*	350
' '(blank)	270	?	360

Figure 2. Code converting table

These watermarks are embedded in the image and extracted from it with Langelaar's watermarking method[10]. [Figure 4] shows the extracted watermarks after JPEG compression. [Figure 5] shows bit error rate by quality factor of JPEG compression for applying various images.

sample text	Implied Value	Watermark
Copyright Korea All rights reserved.	0.38232 0.64714	00111000001000110010 01100100011100011000

Figure 3. sample text and binary watermark

Quality factor	Extraction result	Hit rate
90,80,70 60,50,40	00111000001000110010 01100100011100011000	100%
30	00111000101000110010 01100100011100011000	97.5%
25	00111000101000110010 01100000011100001000	92.5%
15	00111000101000110000 01111000001101011000	80.0%
10	01001000101000110000 01111000001101011000	72.5%

Figure 4. The extracted watermark after JPEG

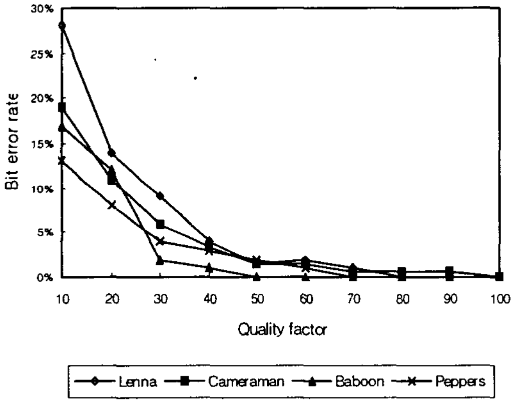
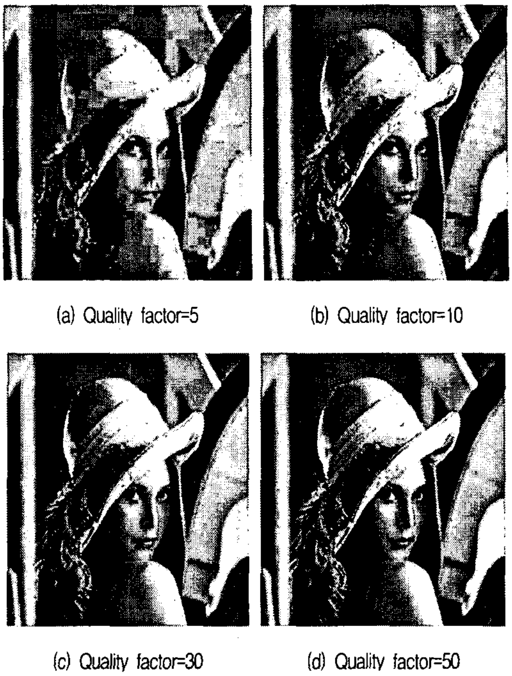


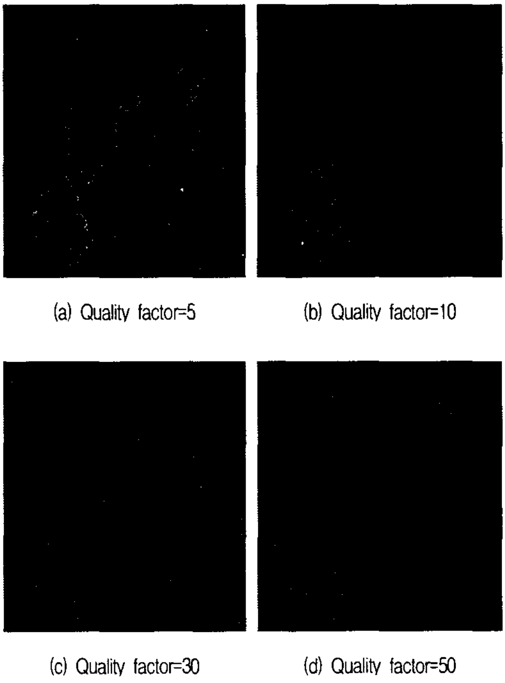
Figure 5. Bit error rates by quality factor of JPEG compression

[Figure 6] shows the JPEG compressed images after watermarking. Although they are watermarked, we can not recognize when the quality factor is more than 30. We can recognize the hiding watermarked data using the differential images between original image and watermarked images. [Figure 7] shows the differential images.


(a) Quality factor=5 (b) Quality factor=10

(c) Quality factor=30 (d) Quality factor=50

Figure 6. The JPEG compressed images after watermarking


(a) Quality factor=5 (b) Quality factor=10

(c) Quality factor=30 (d) Quality factor=50

Figure 7. The differential images between the original image and the images in Figure 6

[Figure 8] shows the performance comparison of the proposed method and other methods using Lenna image. When the JPEG quality factor is over than 50, bit error rate increases rapidly in Cox[1] and Swanson's methods. But, when the JPEG quality factor is less than 50, bit error rate is very low in the proposed method. Even if compression 'rate is high, it is less than 15%.

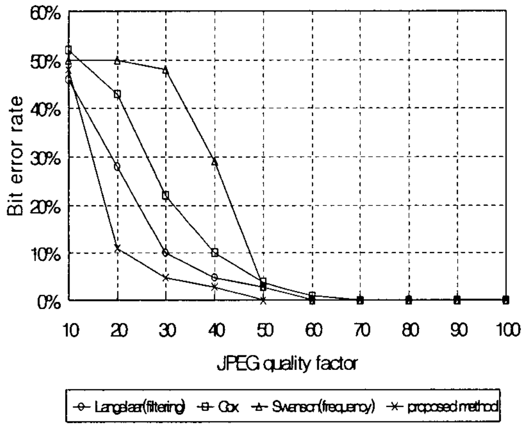


Figure 8. The performance comparison of the other methods using Lenna image

V. Conclusion

In this paper, we propose the possibility of introducing chaotic sequences into digital watermarking systems as potential substitutes to commonly used pseudo noise sequences. Chaotic sequences have several good properties including the availability of a great number of them, the ease of their generation, as well as their sensitive dependence on their initial conditions. And the quantization does not destroy the good property.

Almost watermarking methods are assumed to consist in the modification of a set of full-frame DCT(DFT) coefficients. As the amount of modification each coefficient undergoes is proportional to the magnitude of the coefficient itself, so that an additive-multiplicative embedding rule results. The number of bits that can be hidden within an image by means of frequency domain watermarking is limited.

In this paper, solving this problem, we compress the watermarks using chaotic function. The predictive characteristic of chaotic function makes it possible. We propose a method that transforms sample text to chaotic sequence. We present how the sample text is expressed by an implied data and the implied data is regenerated into the original text. In this paper, we use this implied sample text for digital watermarking. These watermarks are embedded in the image and extracted from it with Langelaar's watermarking method. We got satisfactory experimental results. The experimental results show that proposed watermarking method is robust to the transform such as JPEG compression and much more watermark data are inserted into the limited image space. The sample text is implied to 40 bits binary data. Even if the text is long sentence, we can get implied values using this method. We experimented with gray level images only but expect good results with color image also. Future works will focus on the development of more efficient watermark data including audio watermarking.

References

[1] P. W. Wong, "A Public key Watermark for Image verification and Authentication," *Proc. of IEEE Int. Con. on Image Processing*, Vol.1, pp.455-459, Chicago

Illinois, Oct, 1998.

[2] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Images, Audio and Video," Proc. IEEE Int. Conf. on Image Processing, Vol.III, pp.243-246, 1996.

[3] A Piva, M. Barni, F Bartolini, and V. Cappellini, "DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image," Proc. of the 1997 IEEE Int. Conf. on Image Processing, Vol.III, pp.520-523, 1997.

[4] J. W. Shin and D. S. Jeong, "A New Watermarking Method Using Entropy-Based Region Segmentation," SPIE, Multimedia Systems and Applications, Vol.3258, pp.531-538, 1998.

[5] F. Goffin and J. F. Delaigle, etc., "A Low Cost Perceptive Digital Picture Watermarking Method," *SPIE* Vol.3022, pp.264-277.

[6] H. Xiang, L. Wang, H. Lin, and J. Shi, "Digital Watermarking Systems with Chaotic Sequences," *Proceedings of the Security and Watermarking of Multimedia Contents*, pp.449-457, January, 1999.

[7] M. Barni and F. Bartolini, A. De Rosa, and A. Piva, "Capacity of the Watermark-Channel: How Many Bits Can Be Hidden Within a Digital Image?," *Proceedings of the Security and Watermarking of Multimedia Contents*, pp.437-448, January, 1999.

[8] Hao Bai-Lin, *Chaos II*, World Scientific Press, pp.93-97, 1989.

[9] Ghobad Heidari-Bateni and Clare D. McGillem, "A Chaotic Direct-Sequence Spread-Spectrum Communication System," *IEEE Trans. On Communications*, Vol.42, No.2/3/4, Feb. 1994.

[10] G. C. Langelaar, J. C. A. van der Lubbe, and R. L. Lagendijk, "Robust Labeling Method for Copy Protection of Images," *Proc. of SPIE ELECTRONIC IMAGING '97, storage and Retrieval for Image and Video Databases V*, pp.298-309, February, 1997.

저자소개

조 대 제(Dae-Jea Cho) 종신회원

- 1986년 2월 : 경북대학교 전자공학과(공학석사)
- 2001년 8월 : 경북대학교 컴퓨터공학과(공학박사)
- 2002년 9월~현재 : 안동대학교 전자정보산업학부 부교수

<관심분야> : 콘텐츠 보안, 교육, IT, 문화 콘텐츠

김 희 선(Hee-Sun Kim) 정회원

- 2001년 2월 : 경북대학교 컴퓨터과학과(이학박사)
- 2005년 3월~현재 : 안동대학교 전자정보산업학부 조교수

<관심분야> : 멀티미디어 저작, 멀티미디어 공학, 콘텐츠 저작