Application of Electronic Watermark in Presswork Anti-Imitations

LI Hui    XU Taiyuan
(School of Electromechanical Engineering, UESTC Chengdu 610054 China)

Abstract  This paper introduces the application of electronic watermark in presswork anti-imitation. There are two parts: creating and embedding the electronic watermark. The approach is to hide the watermark which is formed by chaos sequence used logistic algorithms into a color image, using the theory of visual sensitivity difference towards concolorous light. The other is the intellectualizing electronic watermark test device, which contains charge coupled device array and digital signal processing processor. This low cost test device together with electronic watermark printed on press products formed a sophisticated technical system of anti-imitation on presswork. The method and application system have been tested and the Anti-imitation effect is good.

Key words  electronic watermark;  chaos sequence;  visual sensitivity difference;  watermark intellectualized test

Electronic watermark is an information technique usually used in EDP area. The 1st information hidden international seminar was held in Cambridge UK and after that the technique of electronic watermark developed rapidly. It has been a focus of research when the 3rd seminar was open, in which 18 papers out of 33 involves electronic watermark. Many companies have introduced their electronic watermark products[1~4]. Traditional methods that protecting press products from imitation includes optics (fluorescence and laser), metal, watermark, etc. But all these protection methods cannot get the sound effect in the application due to their simplicity. So it is important to develop a more advanced and reliable way to protect those famous merchandise from forgery.

1  The Creating and Hiding of Electronic Watermark

1.1  The Image Disordering by Chaos

In order to get a good encrypt effect, the electronic watermark was coded and embed into the original image. In this application, the logistic algorithms are used to generate chaos image sequence.

The definition of logistic mapping is as the following
\[ X_{n+1} = \mu X_n (1 - X_n) \quad 0 < X < 1 \quad 0 < \mu \leq 4 \quad (1) \]
In order get the Chaos sequence, \( \mu = 4 \), we obtain:
\[ X_{n+1} = 4X_n (1 - X_n) \quad 0 < x < 1 \quad (2) \]
The input and the output of the Logistic mapping are all the real number of (0,1) and the chaos sequence is random, so no matter how to chose the elementary number \( x_1 \), the chaos sequence \( \{x_n, n=1,2,\cdots\} \). Will never have same value. It is similar to random process which has good secrecy. The creation and duplication of the chaos sequence are very simple. Only a chaos sequence iterative formula and an elementary number are needed to create a chaos sequence promptly.

In the mapping of the logistic, we may take the parameter \( \mu \) and elementary \( X_1 \) as the key of the sequence. The watermark may be restored when checking the existence of the watermark. The management of key is easy and safe, so it is suitable for the production and test of public watermark.

Actual digital image disordering sequence can be produced as the follows:
Here are two keys \( \{\mu_1, x_1\} \) and \( \{\mu_2, y_1\} \), so two
Logistic mapping can get two chaos sequences \( \{ x_k \} \) and \( \{ y_l \} \), and they are the electronic image pixels array row and column separately.

We can composite the 2 chaos sequences \( \{ x_k \} \) and \( \{ y_l \} \) from large to small, then we get

\[
\begin{align*}
x'_{(i)} &= x_i, & y'_{(j)} &= y_j.
\end{align*}
\]

Thus the corresponding relation of under mark of the chaos image sequence is set up.

\[
(i) = i', \quad (j) = j'.
\]

Let the \( A = (a_{ij})_{m \times n} \) be the original electronic image, under mark of pixies \( a_{ij} \) is equal to those of \( x'_{(i)} y'_{(j)} \), that is \( i = (i) \), \( j = (j) \). Then take \( B = (b_{ij})_{m \times n} \) as the original electronic image, here we assume \( b_{ij} = a_{ij}' \).

Through the chaos sequence, the pixels \( a_{ij}' \), in the original electronic image \( (i', j') \) turn into the \( (i, j) \). That means you can’t get the original image, unless you have the key.

1.2 Embed and Test of Color Image Electronic Watermark

As well known if three primary color lights Red, Green and Blue are mixed up in proper proportion, almost all colors in the world may be got. RGB mode is a common display mode adopted by video equipments such as television, computer CRT, etc\(^5\). According to the color principle, the color image brightness formula is

\[
y = 0.3R + 0.59G + 0.11B \tag{3}
\]

It is obvious that the sentence to blue light by human eyes is the least of all. So we can separate a electronic image into red, green and blue channels \( X_B, X_G, X_R \). Each channel expresses in the form of gray scale, showing the massage of primary color contended in pixels of the image. On the bases of this principle, we may embed a chaos watermark image \( W \) into a monochromatic image of blue channel in gray scale \( X_B \), and then put it \( (X_W, X_B) \) together with \( X_R, X_G \) into a color image \( X' \).

Because the different sensitivity of human visual system towards three primary colors, that is most sensitive to green, secondary to red and the least to blue, so it will be very difficult to distinguish original image \( X \) from the one with watermark \( X_W \) just by naked eyes. It is this characteristic of visual concealing that makes us possible to embed watermark into a color image.

1.3 Result and Discussion of Experiment

1) The original watermark processed by chaos.

As shown in Fig.1, the graphic \( I \) is the original watermark. We encrypt the original watermark according to the chapter 1.1 and then obtain the chaos electronic watermark which is of great difference to the original one. The chaos watermark will not be able to resume to original watermark correctly unless you have the key.

2) Embed the chaos watermark into the original image.

The following is a original multicolor image \( X \). The Chaos watermark \( W \) will be embed into the image \( X \). Embed process is as the follows:

- The original image is separated into 3 channels: \( X_R, X_G, X_B \). As chapter 1.2, we can get a watermarked image \( X_W \).
- 3) Image test.

To test a color image \( X_{\text{unknown}} \) fake or not, we should test the embed watermark. The first, before the test, we have to take a series of pretreatment, and then get a new chart \( X' \). The process of image test was described by Fig.2~Fig.4.

![Fig.1 The processing of original image](image1)

![Fig.2 Original image X](image2)
The second, the chaos watermark is extract from the new chart $X'$ that the location is $(m_0, n_0)$, $(m_n, n_n)$ ensured before the embed. It can be seen from this experiment, the intellectualized test can be carry out by key formed by the parameters, as shown in Fig. 5.

**2 Printing Process Design**

2.1 Traditional Process

The color printing processes are shown in Fig. 6.

2.2 New Process for Electronic Watermark

The new process printing electronic watermark is shown in Fig. 7.

In the new process, the watermark is embedded in final pattern which has been adjusted color by some software tools.

**3 Test Equipment Design**

The electronic watermark can’t be read with our eyes or any other optical method, so the detecting device is needed. High precision multicolor scanner and digital over 0.5 mega pixels may be used as detecting device. But it is obvious that those equipments are too costly to be widely applied for, so that we designed a low cost and portable test device. The hardware chart of it is shown in Fig. 8.

**4 Conclusions**

After times of printing tests, it is shown that electronic watermark is a practical way used for trademark printing anti-imitation. It has the advantages of invisible to the naked eye, better protection effect from faked imitation, simple key and reliable verification. The method combined with the low cost watermark checking apparatus construct an integrated system of anti-imitation in trademark presswork, which may find a wider application on the protection of names brands and valuable commodities. The techniques introduced in this paper has been applied for patent and passed the verification check.
4 Conclusions

The hybrid chaotic sequence generator is successfully designed and realized by VHDL based on the method of Top-to-Down. A great number of the simulations verify that the output sequences of the generator are very stable and the hazards can be effectively canceled by the method of the controlled output delay. Therefore, the hybrid chaotic sequences are suitable to be applied in DS-CDMA systems.

References


Brief Introduction to Author(s)

LI Hui (李辉) was born in Chengdu, China, in 1963. He received M.S. and Ph.D. degrees in Mechatronics from the Northwest Polytechnic University Xi’an China, in 1987 and 1992. He now teaches several computing courses in UESTC. He is also the researcher of School of Mechanic Electronics Eng. of UESTC. He is the author of more than 20 publications in top domestic journals and international conference proceedings. His research interests include: information system development and industry engineering (IE). E-mail: lihui@core-tech.biz.

XU Taiyuan (徐太源) was born in Chengdu, China, in 1962. He received B.S. degree in Kunming University in 1984. He received MBA degree in Sichuan University in 2003. He is now a deputy factory director in Sichuan ShiFang Cigarette factory and deal with technology management work.

RAO Nini (饶妮妮) was born in 1963. She is a Professor and Doctoral Advisor in Electronic and Electrical Engineering from UESTC. From 1997 to 1998, she was a Visiting Scholar in Dept. of EEE at the University of Bradford in the U.K. Prof. She has published about thirty academic papers in Western Journals and Chinese Journals. She is also co-author of two course books. Her current research interests include Coding, Biomedical Signal Processing, Information Hiding in Telemedicine and Bioinformatics.

ZENG Dong (曾东) was born in 1976. He is a Ph.D. student in UESTC. His research direction is Medical image processing.