A Secure Watermarking Algorithm Based on Coupled Map Lattice

YI Xiang, WANG Wei-ran
(School of Electronic Engineering, UESTC Chengdu 610054 China)

Abstract Based on the nonlinear theory, a secure watermarking algorithm using wavelet transform and coupled map lattice is presented. The chaos is sensitive to initial conditions and has a good non-relevant correlation property, but the finite precision effect limits its application in practical digital watermarking system. To overcome the undesirable short period of chaos mapping and improve the security level of watermarking, the hyper-chaotic sequence is adopted in this algorithm. The watermark is mixed with the hyper-chaotic sequence and embedded in the wavelet domain of the host image. Experimental results and analysis are given to demonstrate that the proposed watermarking algorithm is transparent, robust and secure.

Key words digital watermarking; coupled map lattice; secure watermarking; wavelet transform

With the rapid development of computer and Internet, online delivery of digital media is very popular today and will become more and more important in e-commerce. However, due to the open environment of Internet downloading, there is an urgent need for copyright protection and media security. During recent years, digital watermarking has drawn a lot of attention as a solution of this problem. In this paper, a watermarking algorithm based on coupled map lattice (CML) and wavelet transform is proposed. Firstly, the principle of CML is introduced and the approach to produce the hyper-chaotic sequence is presented. Secondly, the hyper-chaotic sequence is applied in our watermarking scheme. The simulation result, discussion and conclusion are given in the last section.

1 Hyper-Chaotic Sequence Based on CML

In order to protect the watermarking information security, many researchers present watermarking algorithms based on chaos maps\(^1\),\(^2\). But there are still some problems in those methods: 1) in practical digital watermarking system, most of digital chaos maps have finite word length effects, which may cause the existence of chaotic sequence with short period. 2) those methods are based on some special chaos map functions, such as Logistic, Tent, Chebyshev map and so on. So they cannot resist the attack of cryptanalysis.

To overcome the finite precision effect and improve the security of the hiding message, we designed a new chaotic sequence based on CML. One-dimensional CML is given as follows\(^3\)

\[
x_i(n+1) = (1 - \varepsilon) f(x_i(n)) + \varepsilon f(x_{i+1}(n))
\]

where \(i\) denotes the discrete space coordinate, \(i=0,1,\cdots, L-1\) with \(L\) being the size of the lattice. \(n\) is the discrete time. \(\varepsilon\) is the intensity of the coupling. Eq.(1) must satisfy periodical boundary conditions, i.e., \(x_i = x_{i+L}\). \(f(x)\) is the local dynamics with the state variable \(x\). Logistic map is used as the local dynamics here.

\[
f(x) = 1 - 2x^2 \quad x \in U = (-1,1)
\]

Fig.1 shows the phase diagrams of the logistic map and the 1D CML. There are some advantages of CML chaos in comparison with low-dimensional chaos. The CML comprising spatially distributed interacting elements evolving via discrete time dynamics, exhibits more complex spatiotemporal behaviour than the common chaos mapping, and shows more complex phase portrait. The Eq.(1) can also be extended into two-dimensional CML model.

\[
x_{ij}(n+1) = (1 - \varepsilon) f(x_{ij}(n)) + \frac{\varepsilon}{4} [f(x_{i-1,j}(n)) + f(x_{i+1,j}(n)) + f(x_{i,j+1}(n)) + f(x_{i,j-1}(n))]
\]
It’s hard to estimate the period of chaotic sequence in finite precision without simulation. In order to avoid the short period, we combine the chaotic sequence with \(m\)-sequence in form of exclusive or operation. The block diagram of the hyper-chaotic sequence generator for practical application is shown in Fig. 2.

It can be proved that the output period of the hyper-chaotic sequence is an integer multiple of \(m\)-sequence’s period. Because of the complex spatiotemporal chaos property of CML, the hyper-chaotic sequence is of more secure quality and can be used in our watermarking algorithm.

2 Watermarking Algorithm

As we know, the human visual system (HVS) has different sensitivities to different frequencies. The low-frequency noise is usually more noticeable. Another known fact is that lossy compression often eliminates high-frequency components of image. Therefore, our approach inserts the watermark into the middle-frequency band to achieve better tradeoff between transparency and robustness. The watermark-embedding algorithm is described as follows:

1) Permute the binary watermark via toral automorphisms\(^4\):
\[
\begin{bmatrix}
    x' \\
    y'
\end{bmatrix} = \begin{bmatrix}
    1 & 1 \\
    k & k+1
\end{bmatrix} \begin{bmatrix}
    x \\
    y
\end{bmatrix} \pmod{M} \tag{4}
\]

where \(M\) is the watermark’s width (or length), \((x, y)\) and \((x', y')\) represent the pixel location before and after transform respectively, \(k \in [1, M]\) is a controlling parameter. Using Eq. (4), \(M \times M\) watermark matrix \(B\) is permuted into \(M \times M\) matrix \(B'\). From the view of encryption, \(k\) is the key to permute the data.

2) Perform two level wavelet transform to the host image \(I\). An illustration of DWT is shown in Fig. 3.

3) Embed the watermarking into the middle-frequency band in DWT domain via spread spectrum:
\[
W'_l[mN + n] = W_l[mN + n] + \alpha b[m]C[mN + n]
\]
\[1 \leq n \leq N \quad l \in \{ LH2, HL2 \} \tag{5}\]

where \(W'_l\) and \(W_l\) are the modified and the original wavelet coefficients of the host image, \(\alpha\) denotes a parameter accounting for watermark strength, \(b\) is a bit of the permutation watermarking \(B'\) got by the step 1), \(C\) represents the hyper-chaotic sequence based on CML, \(N\) is the chiprate.

4) Run inverse wavelet transform with the modified coefficients to get the watermarked image.

During watermark detection, we calculate the correlation of the observation coefficients \(W''\) and the associated chaotic sequence \(C\). The correlation decoder makes decisions according to the rule,
\[
\hat{b}[m] = \text{Sign}(R[m] - R_0[m]) \tag{6}
\]

where
\[
\begin{cases}
    R[m] = \sum_{n=1}^{N} W''[mN + n]C[mN + n] \\
    R_0[m] = \sum_{n=1}^{N} W[mN + n]C[mN + n]
\end{cases} \tag{7}
\]
3 Experimental Results

The simulations are performed in MATLAB. An example of embedding results is shown in Fig.4, where “Peppers” is the host image, and the binary image with “No.123” characters is the watermarking information.

![Fig. 4 The result of the digital watermarking](image)

To illustrate the robustness of our scheme against usual attacks, we applied common image processing tools on the watermarked image. Fig.5 shows the visual results, and the corresponding numerical results are reported in Table 1. The results show that our watermarking method achieves the eligible robustness.

![Fig.5 Robustness test](image)

4 Conclusions

In this paper, a novel algorithm for image watermarking based on CML has been presented. The performances of the algorithm are very good. 1) The proposed method doesn’t reduce the quality of the host image while the embedded watermark is imperceptible to the human visual system. 2) The watermarking is robust enough against attacks of commonly used image processing. 3) Taking advantage of the more complex spatiotemporal chaos property of CML, the algorithm provide high level security for the embedded message.

References


(Continued on page 56)