Image Watermarking Technique Based on Two-Dimensional Chaotic Stream Encryption

Hanping Hu[1] and Yongqiang Chen[1,2]

[1] Institute for Pattern Recognition and Artificial Intelligence,
State Education Department Key Laboratory for Image Processing and Intelligent Control,
Huazhong University of Science and Technology, Wuhan 430074, China
[2] Department of Computer and Information Engineering,
Wuhan Polytechnic University, Wuhan 430023, China
chenyqwh@163.com

Abstract. This paper proposes a kind of wavelet domain image digital watermarking technique using two-dimensional chaotic stream encryption and human visual model. A stream encryption algorithm based on two-dimensional Logistic chaotic map is researched and realized for meaningful grayscale watermarking image. The block embedding intensity is calculated and combined with the human visual model, so that the embedding and detection steps of encrypted binary watermark can be adaptively fulfilled in the wavelet coefficients of the host image. The experimental results have shown that this watermarking technique can endure regular digital image processing and have preferable performance.

1 Introduction

Digital watermark is a kind of technology that embeds copyright information into multimedia data. Unlike encryption, the watermark remains in the content in its original form and does not prevent a user from listening to, viewing, examining, or manipulating the content. Digital watermark technology opens a new door to authors, producers, publishers, and service providers for protecting their rights and interests in multimedia documents[1].

Considering the watermark security and embedded information's secrecy, we can use the cipher technology to encrypt the information codes and positions. The chaotic encryption technology is a novel method that has good performance and has been developed in recent years. Currently, most image watermarking schemes usually embed chaotic signals produced by given chaotic system into host image[2]. Methods that encrypt meaningful watermarking signals are mainly based on one-dimensional chaotic system, but methods based on two-dimension are rarely found[3]. Besides, attack methods aiming at low dimensional chaotic systems have been found, so the security couldn't be guaranteed.

This paper employs the two-dimensional chaotic Logistic map to encrypt the meaningful gray image[4,5]. Based on HVS model[6-8], we embed the encrypted binary image into the wavelet domain of host image to get more security.

T. Enokido et al. (Eds.): EUC Workshops 2005, LNCS 3823, pp. 817 – 824, 2005.

2 Two-Dimensional Logistic Map

As the encryption using chaotic sequence produced by one-dimensional Logistic system is weak in security, we have to turn to two-dimensional Logistic system.

2.1 The Definition of Two-Dimensional Logistic Map

The two-dimensional Logistic map can be defined as:

$$\begin{cases} x_{n+1} = 4\mu_1 x_n(1-x_n) + g_1(x_n, y_n) \\ y_{n+1} = 4\mu_2 y_n(1-y_n) + g_2(x_n, y_n) \end{cases} \tag{1}$$

g_1 and g_2 are coupled terms, which can be used in two modes:

(1) $g_1 = \gamma y_n$ and $g_2 = \gamma x_n$, and both are simple coupled terms;

(2) $g_1 = g_2 = \gamma x_n y_n$, and both are symmetry quadratic coupled terms.

Adopting the mode of simple coupled term, we change equation (1) as follows:

$$\begin{cases} x_{n+1} = 4\mu_1 x_n(1-x_n) + \gamma y_n \\ y_{n+1} = 4\mu_2 y_n(1-y_n) + \gamma x_n \end{cases} \tag{2}$$

The dynamical behavior of this system is controlled by control parameters of μ_1, μ_2 and γ. These parameters must be suitably chosen to control the system.

2.2 Chaos of the Two-Dimensional Logistic Map

Nonlinear dynamical system will evolve into the ultimate set, namely the attractor, whose dimension is less than the phase space's. With the control parameters changing, the simple attractor will develop into the strange attractor and the system becomes chaotic. Investigating into the chaotic movement, we will observe the bifurcation figure or phase figure. However, due to chaotic complexity, some chaotic criterions are needed, such as reconstruction of phase space, power spectrum analysis, information dimension, Lyapunov exponent and metric entropy. The Lyapunov exponent calculated by difference equation group is a statistical eigenvalue depicting chaotic movement and a measurement unit of average constringency or radiation of neighboring orbits in phase space.

For the two-dimensional Logistic map, its Jacobi matrix $f'(z)$ is represented as:

$$f'(z) = \frac{\partial f}{\partial z} = \begin{bmatrix} 4\mu_1 - 8\mu_1 x & \gamma \\ 4\mu_2 - 8\mu_2 y & \gamma \end{bmatrix} \tag{3}$$

Having $J_i = f'(z_0) \cdot f'(z_1) \cdots\cdots f'(z_{i-1}) = [f^i(z_{i-1})]'_{z=z_0}$, we can compute the module of the 2 complex latent roots of J_i and permute them as $\left|\lambda_1^{(i)}\right| \geq \left|\lambda_2^{(i)}\right|$, where the

Lyapunov exponent is $\lambda_k = \lim_{i\to\infty} \frac{1}{i} \ln | \lambda_k^{(i)} |$, $k = 1,2$. If λ_1 is positive, the system would be chaotic.

When $\mu_1 = \mu_2 = \mu \in [0.6, 0.9]$ and $\gamma = 0.1$, we can analyze the Lyapunov exponent figure and bifurcation figure. The system moves periodically where $\mu < 0.815$ and $\lambda_1 < 0$. The system is chaotic where $0.815 < \mu < 0.89$ and mostly $\lambda_1 > 0$, but the system locates in periodic window with different periods in chaotic area where $\lambda_1 < 0$ in some narrow regions. The system is chaotic where $\mu \geq 0.89$ and $\lambda_1 > 0$. According to the above analysis, the map system, when satisfying the chaotic movement conditions, can be used in digital image encryption.

3 Digital Image Stream Encryption Algorithm

Stream cipher is a kind of symmetric algorithm, which encrypts one bit in the plaintext once a time, and can be regarded as a block cipher of which the block length is one. In the condition of fault transmission, there isn't false spread for stream cipher.

Let $\mathbf{F} = [F_{s,t}]_{M\times M}$ represent a gray watermarking image having L gray levels with size $M \times M$ ($1 \leq s, t \leq M$). $F_{s,t}$ ($0 \leq F_{s,t} \leq L-1$) is the decimal gray value of the pixel (s,t). x_P and y_P are values obtained after the map system is iterated P times. The encryption algorithm is described as follows:

(1)Transform $F_{s,t}$ into the binary sequence $m_{s,t} = m_{s,t,1} m_{s,t,2} \cdots m_{s,t,l}$, $l = \lceil \log_2 L \rceil$. The watermarking image will be represented by a binary matrix $\mathbf{m} = [m_{s,t}]$ with M rows and Ml columns.

(2)Transform the decimal fraction of x_i into binary sequence and choose the first l bits to be represented as $x_{i,1} x_{i,2} \cdots x_{i,l}$. Like x_i, the decimal fraction of y_i is represented as $y_{i,1} y_{i,2} \cdots y_{i,l}$.

(3) According to the row order, do the XOR operation $c^1_{s,t,j} = m_{s,t,j} \oplus x_{i,j}$, $P \leq i \leq P + M^2$, $1 \leq j \leq l$, so the binary sequences of image are encrypted firstly and $c^1_{s,t} = c^1_{s,t,1} c^1_{s,t,2} \cdots c^1_{s,t,l}$ is got.

(4)According to the column order, do the XOR operation $c^2_{s,t,j} = c^1_{s,t,j} \oplus y_{i,j}$ and get $c^2_{s,t} = c^2_{s,t,1} c^2_{s,t,2} \cdots c^2_{s,t,l}$.

(5)Revert the binary sequence $c^2_{s,t}$ into the decimal value represented as $W_{s,t}$ ($0 \leq W_{s,t} \leq L-1$) and get the encrypted image $\mathbf{W} = [W_{s,t}]_{M\times M}$.

Let $\widehat{\mathbf{W}} = [\widehat{W}_{s,t}]_{M\times M}$ represent the received encrypted image and the pixel gray value is $\widehat{W}_{s,t}$. The decryption procedure is described as follows:

(1) Transform the gray value $\widehat{W}_{s,t}$ into the binary sequence $\hat{c}^2_{s,t}$.

(2) The decimal fraction of x_i and y_i are denoted by $x_{i,1}x_{i,2}\cdots x_{i,l}$ and $y_{i,1}y_{i,2}\cdots y_{i,l}$ respectively.

(3) Do XOR operation $\hat{c}^1_{s,t,j} = \hat{c}^2_{s,t,j} \oplus y_{i,j}$, and decrypt the gray value according to the column order and get $\hat{c}^1_{s,t}$.

(4)Do XOR operation $\widehat{m}_{s,t,j} = \hat{c}^1_{s,t,j} \oplus x_{i,j}$, and decrypt the gray value according to the row order and get $\widehat{m}_{s,t}$. Transform binary value $\widehat{m}_{s,t}$ into decimal value $\widehat{F}_{s,t}$ and get decrypted image $\hat{\mathbf{F}} = [\widehat{F}_{s,t}]_{M\times M}$.

From the above encryption and decryption algorithms, it can be concluded that if the received image $\widehat{W}(s,t)$ has not been processed, the equations $\widehat{\mathbf{W}} = \mathbf{W}$ and $\hat{\mathbf{F}} = \mathbf{F}$ are satisfied after the decryption.

In the watermark embedding step, we will use the binary form of the encrypted image, namely $\mathbf{W} = [W_{i,j}]_{M\times Ml}$, $W_{i,j} = 0,1\,(1 \le i \le M,\ \ 1 \le j \le Ml)$.

The key $k(\mu_1, \mu_2, \gamma, x_0, y_0, P)$ is made up of the parameters and the initial value of chaotic system. Because the chaotic system is very sensitive to the parameters and initial value, the theoretic key space is infinite. Therefore, we can almost assign one unique key for one encryption process. The encryption algorithm accords with the Kerckhoff's rules and is a modern encryption method.

In order to demonstrate the algorithm's validity and security, a gray image of face with 256 gray levels and the size of 64×64, namely $M = 64$, $L = 256$, $l = 8$, is selected from ORL face database[9]. Assume control parameters $\mu_1 = \mu_2 = 0.9$, $\gamma = 0.1$ and initial values $x_0 = 0.1$, $y_0 = 0.11$, $P = 500$. The encryption and decryption results are described in Fig.1, in which (a) is the original image, (b) is the result of the original image encrypted only in the rows, (c) is the result of image encrypted in the rows and columns, (d) is the result of the decrypted image with right parameters. From Fig.1, we can observe that if the face image is only encrypted in the row, the sketch of face could still be found; but through encryption in both rows and columns, the resultant image is fully disordered. If only changed one parameter in decrypting step, the result would be false. From the above experiments, it can be concluded that this algorithm has simple complexity and good encrypting effect.

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

Fig. 1. Encrypted and decrypted image

4 Image Watermarking Algorithm

According to the embedding technology, the digital image watermark can be classified into two kinds: spatial watermark and frequency domain watermark. Because the frequency domain watermark is more robust than the spatial watermark, the adaptive watermarking algorithm in DWT domain of host image is adopted based on the HVS model.

4.1 HVS Model

According to the HVS model[8], the frequency response function is shown as:

$$H(\omega) = (a + b\omega)\exp(-c\omega) \tag{4}$$

ω is the radial frequency, a, b and c are parameters determining the HVS curve shape. When $\omega_{\max} = 3$, the HVS curve shape can be expressed as:

$$H(\omega) = (0.2 + 0.45\omega)\exp(-0.18\omega) \tag{5}$$

The image coding using DFT is equivalent to do symmetry spread to original image, but the human eye can't observe this phenomenon. Therefore, the HVS needs a correctional function $A(\omega)$ and the frequency function can be rewritten as:

$$\widehat{H}(\omega) = H(\omega)\left|A(\omega)\right| = \begin{cases} 0.05\exp(\omega^{0.554}) & \omega < 7 \\ \exp(-9\left|\lg\omega - \lg 9\right|^{2.3}) & \omega \geq 7 \end{cases} \tag{6}$$

$\omega = \omega_d \omega_s$, $\omega_d = (u^2 + v^2)^{0.5}/2N$, $u, v = 0, \cdots, N-1$. N is the size of the DFT block. ω_s is a sampling function of the observation distance (assume $\omega_s = 48$). The corresponding $\widehat{H}(\omega)$ of every DFT coefficient (u, v) can be computed. Thereby, the function $\widetilde{H}(u, v)$, corresponding with conjugated (u, v), is obtained.

4.2 Watermark Embedding and Extracting

Wavelet transform accords with some characters of the HVS and strengthens the imperceptibility of watermark. Colligated the HVS model and wavelet transform technology, the encrypted watermarking image is adaptively embedded into the middle frequency subbands of the host image based on the value of the frequency response function.

Let $\mathbf{I} = [I_{i,j}]_{N\times N}$ ($1 \leq i, j \leq N$) represent the host image with size $N \times N$ and $\hat{\mathbf{I}} = [\hat{I}_{i,j}]_{N\times N}$ denotes the watermarked image. The detailed steps of the embedding algorithm are described as follows:

(1)Use DWT to transform the host image $\mathbf{I}$ and get middle frequency subbands $f^{(str)} = [f_{i,j}^{(str)}]_{\frac{N}{2}\times\frac{N}{2}} (1 \leq i, j \leq \frac{N}{2})$, $str \in \{\mathrm{HL}, \mathrm{LH}\}$.

(2)Divide the binary encrypted watermark $\mathbf{W}=[W_{i,j}]_{M\times Ml}$ $(1\le i\le M,\ 1\le j\le Ml)$ into two no-overlap blocks $\mathbf{W}^{(str)}=[W_{i,j}^{(str)}]_{\frac{N}{2}\times\frac{N}{2}}$ $(1\le i,j\le \frac{N}{2})$.

(3)According to the size $(N/4)\times(N/4)$, divide the middle frequency subband into 4 no-overlap blocks $f_k^{(str)}(x,y)$, $k=1,2,3,4$.

(4)According to the block position, compute the watermark embedding intensity $\alpha^{(str)}=\frac{1}{4}\sum_{k=1}^{4}\alpha_k^{(str)}$, $str\in\{\mathrm{HL},\mathrm{LH}\}$, where $\alpha_k^{(str)}$ is defined as:

$$\alpha_k^{(str)}=\beta\left[\sum\widetilde{H}(u,v)\left|\hat{f}_k^{(str)}(u,v)\right|^2\right]^{1/2}\Big/\max_k\left[\sum\widetilde{H}(u,v)\left|\hat{f}_k^{(str)}(u,v)\right|^2\right]^{1/2}$$

$\left|\hat{f}_k^{(str)}(u,v)\right|$, coming from $f_k^{(str)}(x,y)$, can be calculated by transforming the image using DFT. β equals to one tenth of the mean gray value of the encrypted watermark.

(5)Use the equation $\hat{f}_{i,j}^{(str)}=f_{i,j}^{(str)}+\alpha^{(str)}W_{i,j}^{(str)}$ to revise the DWT coefficients of host image, then do IDWT and get watermarked image $\hat{\mathbf{I}}=[\hat{I}_{i,j}]_{N\times N}$.

The watermark detection is to detect whether the embedded watermark information exists in the prepared detection image $\tilde{\mathbf{I}}=[\tilde{I}_{i,j}]_{N\times N}$ $(1\le i,j\le N)$. The host image or watermark image is needful to determine whether watermark exists in the $\tilde{\mathbf{I}}$ through computing the correlation coefficient between $\mathbf{W}$ with $\widetilde{\mathbf{W}}$ extracted from $\tilde{\mathbf{I}}$. The watermark extracting steps are described as follows:

(1)Same as the 1st, 3rd, 4th embedding steps, do the DWT, divide subband into blocks and compute $\alpha^{(str)}$.

(2)Use the equation $\widetilde{W}_{i,j}^{(str)}=(\tilde{f}_{i,j}^{(str)}-f_{i,j}^{(str)})\big/\alpha^{(str)}$ to get sub-block $\widetilde{\mathbf{W}}^{(str)}$, and then unit the sub-blocks into $\widetilde{\mathbf{W}}$.

Set the threshold value T and use the similarity equation $sim(\mathbf{W},\widetilde{\mathbf{W}})=(\mathbf{W}\widetilde{\mathbf{W}})\big/\sqrt{\mathbf{W}\widetilde{\mathbf{W}}}$. If $sim(\mathbf{W},\widetilde{\mathbf{W}})\ge T$, we can determine that the watermark exist in the image $\tilde{\mathbf{I}}$. The above-mentioned decryption algorithm is used to decrypt $\widetilde{\mathbf{W}}$ and examine the robustness of the proposed watermarking technology.

5 Experiments about Robustness

In the experiments, we select the gray Lena image with size 256×256 as host image and the encrypted face image as watermark. Using the above adaptive watermark embedding algorithm, we embed the encrypted watermark into the host image shown as Fig. 2. The PSNR of watermarked host image is 33.1358.

(a)Original host image (b)Watermarked host image

Fig. 2. Adaptive watermark embedding

To quantificationally evaluate the robustness, we processed the watermarked host image with additive noise, median filter and JPEG compression. Then the watermark information needs to be extracted and the *sim* value should be computed to detect whether the watermark exists. If the watermark exists, the extracted watermark needs to be decrypted. Results of the experiments are shown in Tab.1 and Fig.3.

Table 1. The results of experiments

Processing method	Processing intensity	PSNR	*sim*
Gaussian noise	Mean 0,Variance 0.0005	29.8779	0.8920
Salt-pepper noise	Mean 0,Variance 0.001	30.5550	0.9926
median filter	7×7	26.2942	0.5478
JPEG compression	Quality 70%	31.1711	0.7903

(a) Gaussian noise (b) Salt-pepper noise (c) Median filter (d) JPEG compression

Fig. 3. Decrypted result of the extracted watermark

Setting the threshold, we can detect the watermark's existence under the condition of processing method and intensity mentioned in Tab.1. In Fig.3, the decrypted watermarks, except the one from the image processed with median filter, may be faintly distinguished. Therefore, the proposed watermarking algorithm can withstand the processing of adding noise, median filter and JPEG compression to a certain extent, demonstrating needful robustness.

6 Conclusion

The digital watermark satisfies some basic requirements for security, robustness, imperceptibility and authorization. In this paper, we adopt some technologies to satisfy these requirements:

(1) Based on the analysis of chaotic encryption methods, we research the two-dimensional Logistic map system and the chaotic conditions. After a key is selected, the chaotic map system is used to encrypt the meaningful gray image. This encryption method meets the requirement and has good secure performance.

(2) The proposed watermarking scheme that embeds the encrypted watermark into the DWT domain of host image is a digital watermarking technique in frequency domain. From the theory of the frequency domain watermark and the results of our experiment, this watermarking scheme demonstrates good robustness and can resist the attacks of the noise, filter and compression.

(3) Combined with HVS model, the embedding intensities for each sub-block are computed according to the characters of texture and energy of the host image. The watermark is self-adaptively embedded into the host image, which balances the requirements between robustness and imperceptibility.

(4) The correlation analysis can determine whether the appointed characteristic information exists in the pending image.

The grayscale face image and Lena image are used as examples in our experiments. In fact, other grayscale images or color images which intensity dealt as gray could be used and the same results can be gotten.

References

[1] Cox I J, Miller M L, Bloom J A. Digital watermarking. San Francisco: Morgan Kaufmann Publishers, 2002

[2] Yang J, Lee M H, Chen X H et al. Mixing chaotic watermarks for embedding in wavelet transform domain. In: Proceedings of IEEE International Symposium on Circuits and Systems V2, Phoenix, USA, 2002:668-671

[3] Yen J C. Watermarks embedded in the permuted image. In: Proceedings of IEEE International Symposium on Circuits and Systems V2, Sydney, Australia, 2001:53-56

[4] Tefas A, Pitas I. Image authentication using chaotic mixing system. In: Proceedings of IEEE International Symposium on Circuits and Systems V1, Geneva, Switzerland, 2000:216-219

[5] Ferretti A, Rahman N K. A study of coupled Logistic map and applications in chemical physics. Chemical Physics, 1988, 119:275-188

[6] Nill N B. A visual model weighted cosine transform for image compression and quality assessment. IEEE Transaction on Communication, 1985, 33(6):551-557

[7] Tan S H, Ngan K N. Classified perceptual coding with adaptive quantization. IEEE Transaction on Circuits and Systems for Video Technology, 1996, 37(6):375-383

[8] NILL N B. A visual model weighted cosine transform for image compression and quality assessment. IEEE Transaction on Communication, 1985, 33(6):551-557

[9] AT&T Laboratories Cambridge. The ORL Database of Faces. http://www.uk.research.att.com/facedatabase.html. 2004-11-12