Watermarking scheme of colour image based on chaotic sequences*

LIU Nian-sheng(刘年生)[1], and GUO Dong-hui(郭东辉)[2]**

1. School of Computer Engineering, Jimei University, Xiamen 361021, China;

2. School of Information Science and Technology, Xiamen University, Xiamen 361021, China

(Received 16 February 2009)

The proposed perceptual mask is based on the singularity of cover image and matches very well with the properties of the human visual system. The cover colour image is decomposed into several subbands by the wavelet transform. The watermark composed of chaotic sequence and the covert image is embedded into the subband with the largest energy. The chaos system plays an important role in the security invisibility and robustness of the proposed scheme. The parameter and initial state of chaos system can directly influence the generation of watermark information as a key. Moreover, the watermark information has the property of spread spectrum signal by chaotic sequence to improve the invisibility and security of watermarked image. Experimental results and comparisons with other watermarking techniques prove that the proposed algorithm is effective and feasible, and improves the security, invisibility and robustness of watermarking information.

Document code: A **Article ID:** 1673-1905(2009)03-0227-5

DOI 10.1007/s11801-009-9044-4

Since Van Schyndel[1] introduced the method of digital watermark on the gray images in 1994[2], many digital watermark schemes have been published[2-5]. This paper develops a novel color image watermarking scheme based on chaotic sequences. The watermark signal generated by chaos system can be embedded into the host image as a small noise-like signal. We will use the Chebyshev maps to generate such a pseudorandom sequence.

A generic model of the proposed watermarking system is shown in Fig.1. The watermark information is made from the chaotic system and the host image, and added to the host image. The approximation coefficients of host image multiwavelet domain are selected as the embedding host of watermark information to improve the robustness of watermarking system. Then, the idea of cryptosystem is inducted watermarking system via Chebyshev maps. The expression of Chebyshev maps is as follows,

$$X_{n+1}=\cos(P\cos^{-1}(X_n)) \quad -1\leq X\leq 1\ , \tag{1}$$

where P is the degree of Chebyshev map. Its corresponding invariant density is as follows.

$$r(X)=1\Big/(p\sqrt{1-X^2})\ . \tag{2}$$

Chebyshev maps have important properties of excellent cryptosystem[6]. If $P\geq 2$, the Lyapunov exponent of Chebyshev maps is positive, which predicates that Chebyshev maps are chaotic. The real number sequences generated by Chebyshev map are orthogonal each other. Furthermore, their correlation functions are all d function. The parameter P and initial state value X_0 are regarded as the key of proposed watermarking system. The key must be kept secret in the proposed scheme.

The watermarked image is obtained by performing the inverse multiwavelet transform of the watermarked coefficients, and transferred via public channel.

Watermark extraction is similar to the watermark generation step of the watermark embedding process. The watermarked image obtained from public channel is regarded as the tested image.

The tested watermark is compared with the real watermark information using the method of test threshold, if the correlation coefficient of them is bigger than a given critical value, the tested image will be regarded as real watermarked one. Otherwise, it isn't considered that the tested image is real watermarked one.

The 512×512 pixel Lena image is used as the host images;

* This work has been supported by the National Natural Science Foundation of China (No. 60076015), the Natural Science Foundation of Fujian Province in China (No. A0640009), the Science Project of Xiamen City in China (No. 3502Z20081073), and the Foundation for Young Professors of Jimei University in China (No. 2006B003).

** E-mail:nsliu@jmu.edu.cn

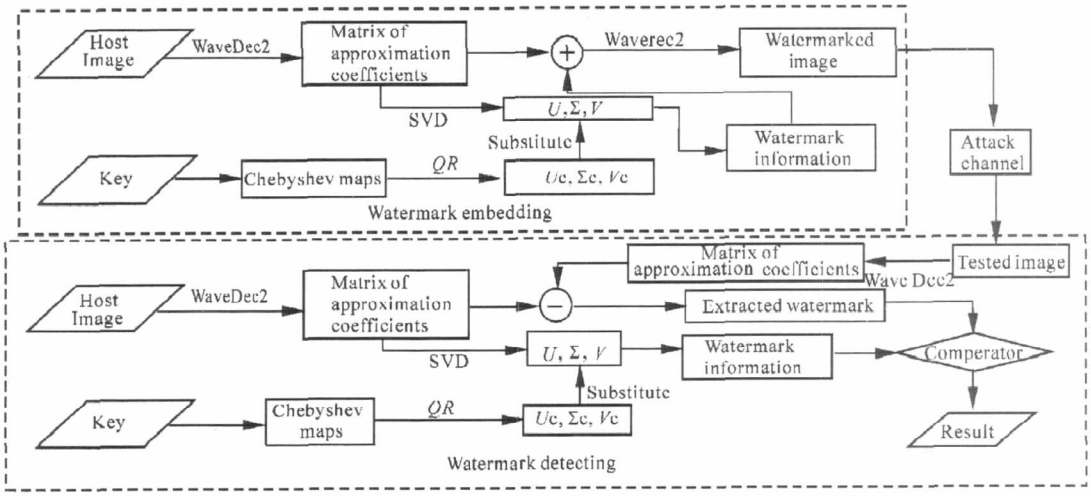


Fig.1 Proposed watermarking system based on chaotic sequences

the 512×512 pixel gray image is generated by the combination of chaos system the and the host image is used as the watermarks. The Chebyshev map is adopted to generate chaotic sequences as chaos system.

According to the proposed image watermarking scheme, corresponding programs are written in order to estimate the performance of scheme through simulation. The correlation coefficient and peak signal to noise ratio (PSNR) between the host image and the watermarked image are regarded as quantitative measures to characterize the invisibility of watermark information. The definition of correlation coefficient between the host image and the watermarked image is as follows.

$$r=\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(H_{(i,j)}-\overline{H})(W_{(i,j)}-\overline{W})}{\sqrt{(\sum_{i=1}^{m}\sum_{j=1}^{n}(H_{(i,j)}-\overline{H})^2+\sum_{i=1}^{m}\sum_{j=1}^{n}(W_{(i,j)}-\overline{W})^2)}}, \quad (3)$$

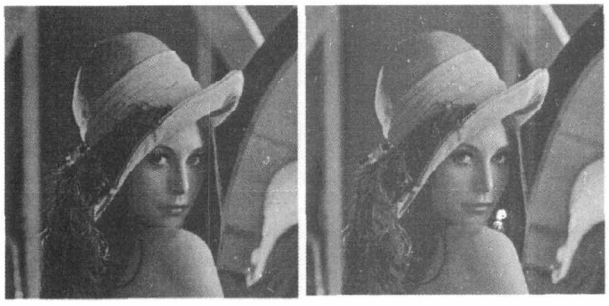
where $\overline{H}$ and $\overline{W}$ represent the mean value of $m\times n$-pixel host image H and watermarked image W, respectively. When correlation coefficient γ is bigger than a certain critical value γ_c, the host image and watermarked image are the same for human visual system. In the simulation experiment, it is found that the critical value γ_c is (0.996 ± 0.001) $(p=0.05)$ using the method of TAFC (two alternatives force choice).

The definition of *PSNR* between the host image and the watermarked image is as follows,

$$PSNR=10\ \log_{10}\frac{D^2mn}{\sum_{i=1}^{m}\sum_{j=1}^{n}(H_{(i,j)}-W_{(i,j)})^2}, \quad (4)$$

where D is the peak of image signal.

The simulation results are shown in Fig.2, 3 and 4. In Fig.2, when watermarking strength K is smaller than 0.1, the correlation coefficient γ between the host image and the watermarked image is 0.99994 and exceeds the given critical value 0.996. Corresponding *PSNR* is 53.7935 dB. So we find no noticeable difference between the host and the watermarked image shown in Fig.2(a) and 2(b). The watermark information shown in Fig.3 is imperceptible in the watermarked image. It depends on the host image and the secret key of chaos system. Every key consists of three pairs of different combination with parameter p and initial state value x_0. The length of key is over 128 bits that the proposed watermarking system can be against the Birthday attack. The obtained watermark information will be different when the key of chaos system is different. The coefficients of conventional correlation test and DCT correlation test between the real watermark and the tested watermark are used to estimate whether the test image is embedded real watermark information[8]. A real key is given, while the other 19 keys are randomly selected. Simulation results are shown in Fig.4. It is proved that the key is very sensitive in the proposed scheme. It is hard to extract and detect the watermark information



(a) Host image (b) Watermarked image

Fig.2 Comparison between the host and the watermarked image

without the exact key.

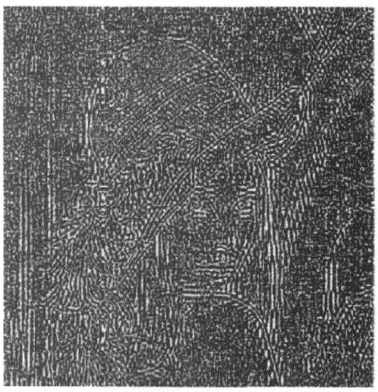


Fig.3 Watermark information embedded in the watermarked image

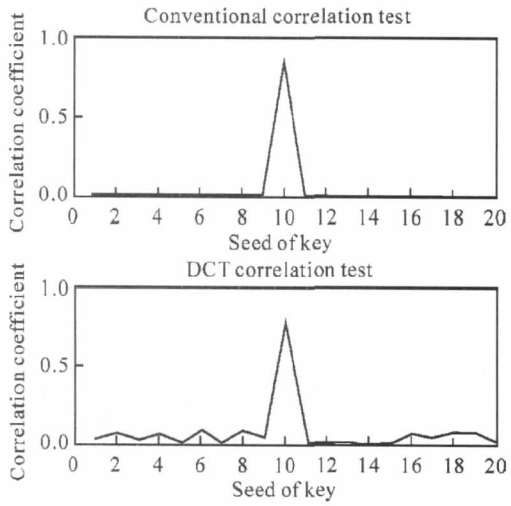


Fig.4 Comparison of watermarking correlation detection using different keys

The performance of the proposed scheme against JPEG compression, rotation, cropping, and other attacks is evaluated as follows.

Fig.5 shows the detected results from a JPEG compressed version of the watermarked images with the compression quality factor ranging from 0 to 100%. Obviously, the correlation coefficient decreases as the compression ratio increases. When the compression ratio is high enough, the watermark will be destroyed and become indiscernible. In comparison with the conventional scheme using pseudorandom function (in gin general, linear congruence algorithm) to substitute Chebyshev map, our scheme has better property against the JPEG compression attack.

Fig.6 shows the relationship between the similarity measurement and the cropped block size from the watermarked image. The bigger the cropping size is, the smaller the correlation coefficient is. The cropped position of watermarked image is randomly selected during the experiment. However, although the part of the watermarked image is discarded, the correlation coefficients are still bigger than the threshold value (In generation it is 0.1).

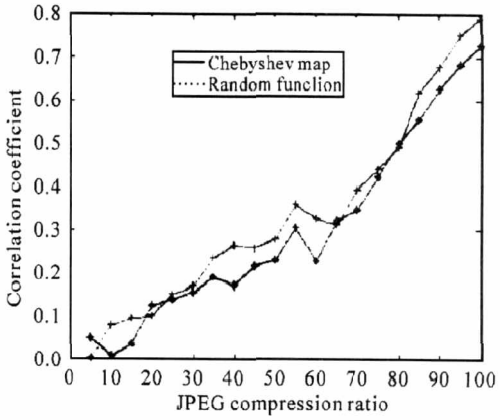


Fig.5 Comparison of correlation detection against the JPEG compression between the proposed and conventional schemes

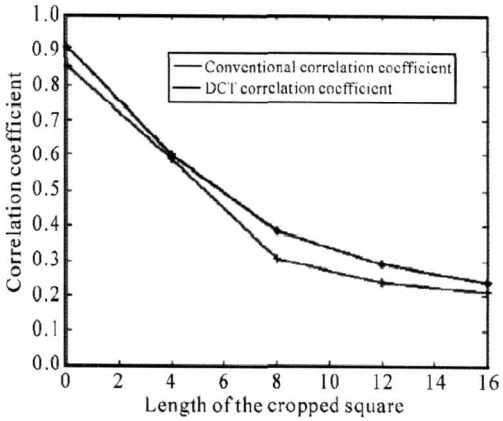


Fig.6 Results of correlation detection against the attack of image cropping

The experimental results shown in Fig.7 show that the embedded watermark can be exacted perfectly and detected when the watermarked image is rotated to 0.1^{o} max in our scheme. The proposed scheme can be powerfully against the attack of the slight rotation of image.

Fig.8 shows the results of adding Gaussian noise with zero mean and variance from 0 to 0.001 to the watermarked Lena image. The embedded watermark can be exacted effectively and detected from the watermarked image of added Gaussian noise. It is obvious that the proposed approach is strong enough against the attack of adding multipliable noise. Even if the watermarked image quality is degraded greatly, the watermark information can be detected perfectly.

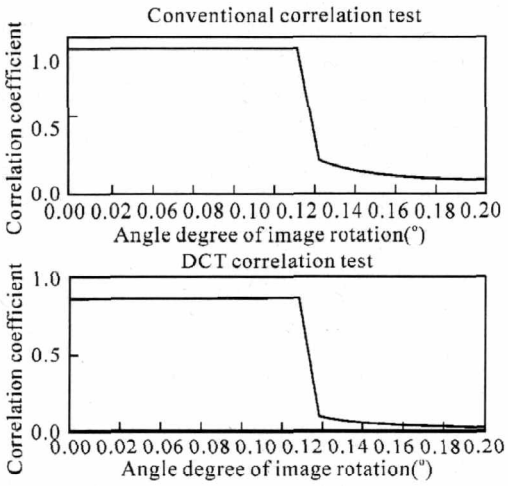


Fig.7 Results of correlation detection against the attack of image rotation

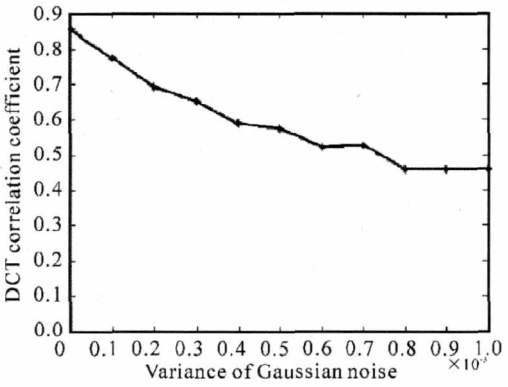


Fig.8 Results of correlation detection against the attack of adding Gaussian noise

The secret keys in the proposed consist of two pairs of P and X_0, where P is any positive integer over 1, while X_0 is any floating point number. If P and X_0 are defined as short integer and double floating point number, respectively, in the java program, the sum of binary length in the memory for any pair of P and X_0 is 80 bits. According to the IEEE 754 for double floating point numbers and the ranges of P and X_0 in the Chebyshev maps (conventionally, they are [2, 100) and [-1, 1], respectively), the binary length of secret keys in new scheme is over 180 bits because three pairs of P and X_0 are used in the proposed scheme. For example, for an exhaustive search attack, the complexity of computation is 2^{180}. Even if a dedicate computer that can perform a search of 10^6 groups P and X_0 in one second is used, the time required to search exhaustively the entire key space is 4.8×10^{40} years. It is infeasible in fact.

Chebyshev map is a classic chaotic system with the sensitivity of initial state. The chaotic sequences generated by Chebyshev map have pseudorandom property shown in Fig.9. Using a wrong key (2, 0.2000000001), (2, 0.20) and (4, 0.50) to substitute a right key (2, 0.20), (2, 0.20) and (4, 0.50), the corresponding extracted watermark image is shown in Fig. 10. It is completely different from the true watermark image shown in Fig.3. Its detection response value is about 0.04, and is smaller than a given threshold value (in generation 0.1).

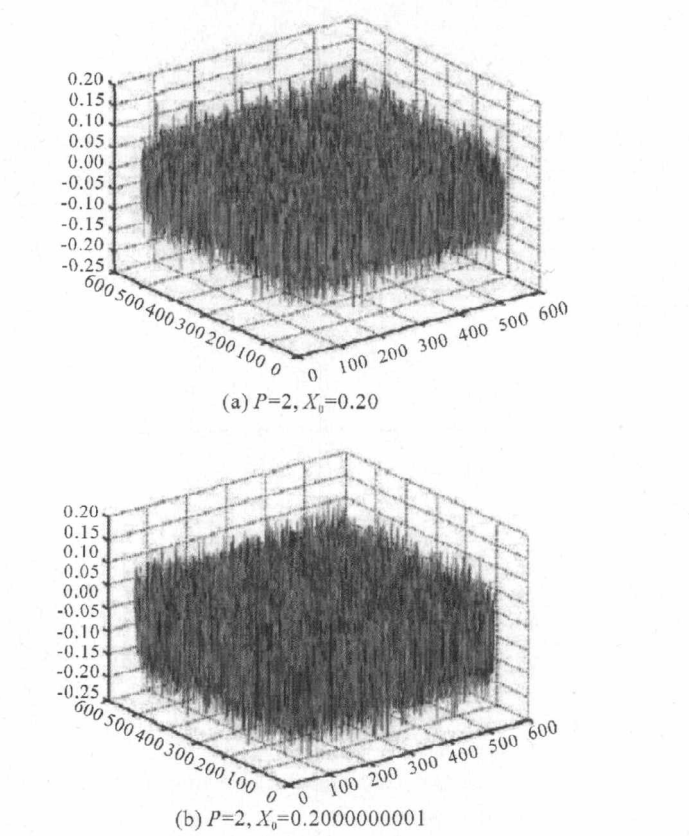


Fig.9 Chaotic sequences generated by Chebyshev Map

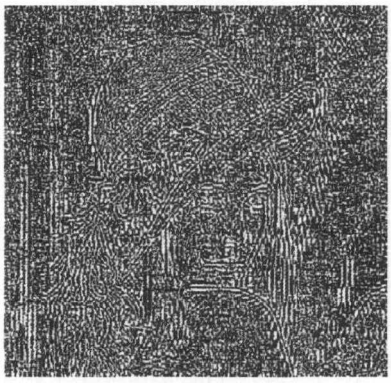


Fig.10 Watermark information extracted with wrong secret key

It is impossible to find the private key by using chosen-plaintext attack or known- plaintext attack at present[9]. Only an exhaustive search based on the statistical probabilities of plaintext characters can succeed in breaking our proposed cryptosystem. However, the breaking cost of this method is very high because the length of key is over 180 bits.

Tab.1 shows the result of the proposed scheme in comparison with the scheme in Ref.[2]. Our scheme has obvious superiority in the performances of watermarking information with invisibility, robustness and security.

Tab.1 Performances comparison between the proposed scheme and Chen's scheme

Watermarking scheme	PSNR (dB)	Correlation coefficient	Gaussian noise (Variance 0.1)	JPEG (%)	Rotation (°)	Key (bit)	Time of watermark detection (Second)
The proposed Scheme	53.8	0.99994	0.5	85	0.1	180	1.58
Chen's Scheme	45.7	0.9937	0.5	15	No Data	null	1.63

In conclusion, using chaotic sequences, a new image watermarking scheme is proposed. The chaotic sequences generated by Chebyshev map not only act as the secret key of watermarking system to enhance the watermark security, but also make the watermark signal add to the host image as a white noised-like form. Experimental results and comparisons with other watermarking techniques prove the proposed scheme is feasible and robust against conventional attacks. The authors intend to develop this work further through refinement and analysis of the protocol performance and its use for secure communications across fixed and wireless networks.

References

[1] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, In International Conference on Image Processing, **2** (1994), 86.

[2] Chen Kailiang, and Wang Jianjun, Journal of Computer-Aided Design & Computer Graphics, **19** (2007), 811.

[3] Dong Ping, G. Brankov Jovan, and P. Galatsanos Nikolas, IEEE Transactions on Image Processing, **12** (2005), 2140,

[4] ZHANG Ying, WEN Xian-bin, and WANG Chun-dong. Journal of Optoelectronics · Laser, **19** (2008), 1097. (in Chinese)

[5] Fujita Takaaki, Yoshida Maki, and Fujiwara Toru, IEICE Transactions on Fundamentals of Electronics,Communications and Computer Sciences, **E90-A** (2007), 216.

[6] Hane Ryuichi, and Kohda Tohru, International Journal of Bifurcation and Chaos, **17** (2007), 3618.

[7] Niansheng Liu, and Donghui Guo, Computer Engineering, **32** (2006), 135.

[8] W. Stallings, Cryptography and Network Security: Principles and Practice. 2nd ed, Prentice –Hall, Inc. (2003), 24.