Digital Image Watermarking Based on Normalization and Visual Feature

Chen chen[1, a *], Guo huimin[2,b]

[1, 2]The Department of Information Engineering, JinCheng College, NUAA, NanJing 211156, China

[a]550708102@qq.com, [b]chen_chen218@163.com

Keywords: image watermarking, image normalization, strength factor, DCT transform.List.

Abstract. In this paper, a Discrete Cosine Transform (DCT) domain robust digital watermarking algorithm based on image normalization of invariant moment and the sense of visual feature of person is proposed. In order to boost up the safety and the solidity of the watermark, the watermark is scrambled and chaotically encrypted before embedded into the original image. Firstly, using image normalization and the invariant centroid theory obtained a significant region from the normalized image. Then the significant region is cut into blocks of 8*8, and DCT is performed on the image blocks. While making sure of the watermark's embedding position and strength factor, this paper takes good use of the sense of visual feature of person and the characteristic of image. Experimental results show that the proposed scheme is invisible and robust against attacks.

Introduction

In recent years, with the rapid development of digital multimedia and the Internet, perfect copying, modification, and redistribution of the information is absolutely possible. Hence, the problem of ownership protection of digital information has become increasingly important. Although significant progress has been made in watermarking of digital images, many challenging problems still remain in practical applications. Among these problems is the resilience of watermarking to geometric attacks. Examples of geometric attacks include rotation, scaling, and translation(RST)[1,2]. Such attacks are easy to implement, but can make many of the existing watermarking algorithms ineffective. Therefore, how to improve the robustness of digital watermarking became the urgent needs to solve the problem.

Image normalization can solve the problem effectively. Through a series of image processing, the image was transformed into the corresponding standard forms[3], in which images are affine invariant to geometry transforms(RST). Currently some algorithms based on image normalization do well in robustness, but cannot ensure both robustness and invisibility, which are the most important requirements of digital image watermarking[4,5].

In this paper, we propose a digital watermarking algorithm based on image normalization and the sense of visual feature of person to alleviate the problem of geometric distortions and invisibility.
In order to boost up the safety and solidity of the watermark, the watermark is scrambled and chaotically encrypted before embedded into the original image using the Logistic chaos mapping. Firstly, the geometrically invariant space is constructed by using image normalization method, and the significant region is obtained from the normalized image by utilizing the invariant centroid theory. Then the significant region is cut into blocks of 8*8, and DCT is performed on each image blocks. While making sure of the watermark's embedding position and strength factor, this paper takes good use of the sense of visual feature of person and the characteristic of image. Experimental results indicate that the proposed scheme is invisible and effective in resisting geometric attacks.

Image Preprocessing

Original Image Preprocessing

(a) Image Normalization

Image normalization is one kind of pattern recognition technique, and is widely applied to obtained the normalized image, which is invariant to any affine distortions of the image. This will ensure the

integrity of the watermark in the normalized image even when the image undergoes affine geometric attacks.

The general concept of image normalization using moments is well-known in pattern recognition problems, where the idea is to extract image features that are invariant to affine transforms. In this application, we apply a normalization procedure to the image so that it meets a set of predefined moment criteria, which will ensure the integrity of the watermark in the normalized image even when the image undergoes affine geometric attacks.

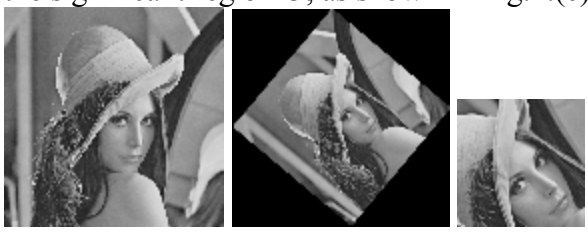
Let $f(x,y)$ denote a digital image of size $M \times N$. Its geometric moments are m_{pq} and central moments are μ_{pq} ($p,q = 0,1,2,...$).

(b) Obtained the Significant Region

Image normalization-based schemes are highly sensitive to cropping. Therefore, an invariant point that remains unchanged after geometrical or waveform attacks is needed. The invariant centroid(IC) of an image can be detected under many RST attacks, even if the image is moderately cropped[6]. The centroid $\mathrm{C}(\mathrm{C_x}, \mathrm{C_y})$ of the normalized image $\mathrm{I}(x,y)$ is calculated as follows:

$$C_x = \sum_x \sum_y f(x,y)x \qquad C_y = \sum_x \sum_y f(x,y)y \tag{1}$$

where $f(x,y) = I(x,y) / \sum x \sum y I(x,y)$ and $(x,y) \in R^2$ is the region of the image $\mathrm{I}(x,y)$. Then using the invariant centroid $\mathrm{C}(\mathrm{C}_x, C_y)$ as the center of the normalized image I to create a rectangular size of $s_1 \times s_2$, which is called the significant region O, as shown in Fig.1.(c).



(a) Original image (b) Normalized image (c) Significant region

Fig.1: Obtained the significant region

Watermark Image Preprocessing

The logistic map has been used for our study. Logistic map is a one dimensional chaotic function. It is defined as $\mathrm{f}(\mathrm{x}) = p \cdot x \cdot (1-x)$. The logistic map is sometimes called an iterated map function, since it maps one value of 'x' in the range $0 \le x \le 1$ into another value of 'x' in the same range if p is in the range $0 \le p \le 4$ [9].The iterative form of this function is written as $x_{n+1} = p \cdot x_n \cdot (1 - x_n)$ with 'x_0' as the initial value. This is also known as the seed value for the logistic map. In this paper, the logistic map has been used to encrypting watermark image with the seed value $x_0 = 0.278$ and $p = 3.58$. The original watermark image is the binary image of 32×32 pixels as shown in Fig.2.(a) and the encrypted watermark image W' is shown in Fig.2.(b). Specific steps are as follows:

① Inputting the private keys $K(p, x_0)$, producing the chaotic sequences X and putting X in ascending sequence, we $[X', l] = sort(X)$ can get , where X' is the ascending chaotic sequence, l is the index series;

② The index series l is converted to the two-dimensional matrix L;

③ According to the matrix L, rearrange the binary watermark W, we can get the scrambled watermark W'.

(a) Original watermark image (b) Encrypted watermark image

Fig.2: Encrypt watermark image using logistic map with the seed value x=0.278, p=3.58.

Embedding with HVS

Obviously, the region of toque has complex texture, which is not sensitive for eyes and can contain more information. The region of face is very smooth, so that very sensitive to any adding information. The HVS mask reflects these characteristics correctly. In this paper, we take good use of the sense of visual feature of person and the characteristic of image to embed the watermark in DCT domain with an additive manner. Firstly, divided the significant region into blocks of 8*8, computed DCT in each block and calculated the visual sensitivity value S_k^{DCT} of each block. Then determined the watermark's embedding strength factor by the size of the value S_k^{DCT}.

Let $F(x,y)\ 1 \le x \le M$, $1 \le y \le N$ be the $M \times N$ 8-bit grayscale image which is to be watermarked and $W(x,y)\ 1 \le x \le P$, $1 \le y \le Q$ be a $P \times Q$ binary image which is to be used as the watermark. The watermark embedding procedure is summarized as follows. To embed a watermark into an image:

1) Apply the normalization procedure to obtain the normalized image I. Derive the invariant centroid C from the normalized image I, and obtain the significant region O, as shown in Fig.1.(c).

2) Cut the significant region O into blocks $O_k(x,y)$ of 8×8, $0 \le k \le (M \times N)/64$, $x = 0,1,2,...7$, $y = 0,1,2,...7$. Then DCT is performed on the image blocks $O_k(x,y)$, and obtain $O_k(\mu,v)$, $\mu = 0,1,2,...7$, $v = 0,1,2,...7$.

3) Using $O_k(\mu,v)$ obtained in 2) the visual sensitivity value S_k^{DCT} of each block is calculated as follows:

$$S_k^{DCT} = \sum_{\mu=0}^{\mu=7} \sum_{v=0}^{v=7} C(\mu,v) \times \left| O_k(\mu,v) \right|^2 \tag{2}$$

where $C(\mu,v)$ is the contrast sensitivity matrix, defined as

$$C(\mu,v) = 5.05 \times e^{-0.178 \times (\mu+v)} (e^{0.1 \times (\mu+v)} - 1) \tag{3}$$

where μ,v is spatial frequency, $\mu = 0,1,2,...7$, $v = 0,1,2,...7$. The contrast sensitivity matrix is the reflection of the relationship between visual sensitivity and spatial frequencies. The value of S_k^{DCT} reflects human's visual sensitivity of each image block. When the value of S_k^{DCT} is big, human are insensitive to the noise of the image that means we can set a strong watermark strength factor.

4) Firstly, the visual sensitivity value S_O^{DCT} of the significant region O is calculated. Then compare the value of S_k^{DCT} and S_O^{DCT} to determine the strength factor α of each image block.

① If $S_k^{DCT} > 2S_O^{DCT}/3$ human are insensitive to the noise of the image block k at all. We classify these image blocks as A category, which can have a stronger watermark strength factor. In this paper, we set strength factor of these blacks of A category $\alpha = 0.09$.

② If $2S_O^{DCT}/3 \ge S_k^{DCT} \ge S_O^{DCT}/3$ human are insensitive to the noise of the image block k. We classify these image blocks as B category, which can have a strong watermark strength factor. In this paper, we set strength factor of these blacks of B category $\alpha = 0.06$.

③ If $S_k^{DCT} < S_O^{DCT}/3$ human are sensitive to the noise of the image block k. We classify these image blocks as C category, which can have a weak watermark strength factor. In this paper, we set strength factor of these blacks of B category $\alpha = 0.03$.

5) Quantify the DCT coefficients $O_k(\mu,v)$ with the JPEG standard luminosity curve quantization table, where the quantization factor is 0.5, and the result is $O_k'(\mu,v)$, then sequence $O_k'(\mu,v)$ through inverse zigzag scan. If the block belongs to A category, we embed the watermark into the first three alternating current coefficients (1,1), (1,2), (2,1). If the block belongs to B category, we embed the watermark into the first two alternating current coefficients (1,1), (2,1). If the block belongs to C category, we embed the watermark into the alternating current coefficients (1,1).

6) Encrypt the watermark image by using logistic map with the seeds value $x_0 = 0.278$ and $p = 3.58$, and get the scrambled watermark W'. Mapping W' as follows:

$W'_{im}(p,q) = \begin{cases} 1, W'(p,q) = 1 \\ -1, W'(p,q) = 0 \end{cases}$ where $p = 1,2,3,...,P$, $q = 1,2,3,...,Q$. Then embed W'_{im} in the corresponding coefficients obtained in step 5). The embedded formula is

$$P'(i,j) = O'(i,j) \times (1 + W'_{in}(p,q) \times \alpha) \quad (4)$$

where α is the strength factor determined in the step 4), and the relationship between (p,q) and (i,j) is determined in the step 5).

7) Compute IDCT in each block obtaining the watermarked block O_k', then combine O_k' with the insignificant region of the normalized image and get the normalized watermarked image I'. Because normalization will make a certain extent distortion to carrier image, we should take some steps to improve the invisibility of the watermark.

Watermark Extraction

The following steps are taken to decode the embedded watermark in an image.

1) Obtain the normalized image I^*. Apply the normalization procedure to obtain the normalized image I^*.

2) Obtain the significant region O^* from the normalized image I^*.

3) Cut the significant region O^* into blocks of 8*8, and perform DCT on each image blocks, then get the DCT coefficients.

4) With the DCT coefficients obtained in step 3), the watermark message is decoded as

$W_{out}'(p,q) = \begin{cases} 1, & \text{若 } W_{out}(p,q) > 0 \\ 0, & \text{若 } W_{out}(p,q) \le 0 \end{cases}$, where $W_{out}(i,j) = P'(i,j) / O'(i,j) - 1$.

5) Obtain the watermark image. Decrypted the image W_{out}' by using logistic map with the key value $x_0 = 0.278$.

Experimental Results

Our experimental investigations used the 512×512 8-bit gray scale test images popularly referred to as Lena. The watermark is an 8×8 binary image. The size of the significant region O is 256×256. The proposed algorithm was used to insert the binary image into the test image to obtain the watermarked Lena. For comparison, we show the results of invisibility and robustness compared with other methods [3,9,10,11].

The original image, the watermarked image without attack and the extracted watermark image are shown in Fig.3.

(a) Original image (b) Watermarked image (c) Extracted watermark image

Fig.3: Extract the watermark image without attack

The corresponding PSNR is 43.3603 dB, and the result is compared with other methods as shown in Table 1.

Table 1: Comparison of our method and other methods on PSNR

PSNR（dB）	Our method	[3]	[9]
Lena	43.3603	37.88	43.23

In order to represent our watermarking scheme is robustness against geometric distortion, we take the next research.

1) Extracted the watermark from the images which were rotated by different degrees.

Table 2: Comparison of our method and other method on rotation attack

θ/°	10	20	30	45	60	90	120	180
NC[10]	0.9683	0.8320	0.7119	0.7312	0.7859	0.8916	0.8035	0.8853
NC[our]	0.8969	0.8973	0.8362	0.8393	0.8981	0.9158	0.9156	0.9126

2) Extracted the watermark from the images which were attacked by linear translation.

Table 3: Our method on linear translation attack

(x，y)	（26，0）	（0，26）	（26，26）
NC	0.8913	0.8897	0.8574

3) Extracted the watermark from the images which were attacked by rotation together with scale transformation.

Table 4: Comparison of our method and other method on combined attack

(λ,θ)	（0.5,45）
NC[11]	0.7916
NC[our]	0.8092

Acknowledgements

In this paper, we first obtain the significant region O from the normalized image I, then divided the significant region into blocks of 8*8. Then computed DCT in each block and calculated the visual sensitivity value S_k^{DCT} of each block. Finally, determined the watermark’s embedding position and strength factor by the value S_k^{DCT}. Successively, the computer simulation illustrates that our method is invisible and robust against geometric attacks.

References

[1] Tsai J，Huang W，Kuo Y，et al,Joint robustness and security enhancement for featurebased image watermarking using invariant feature regions, J .Signal Processing. 92 (2012) 1431-1445.

[2] Valizadeh A, Wang Z J, Correlation-and-bit-aware spread spectrum embedding for data hiding, J. IEEE Trans on Information Forensics and Security. 6 (2011) 267-282.

[3] Wang Shengfang, Kang Chen, A Wavelet Watermarking Based on HVS and Watermarking Capacity Analysis. 2009 International Conference on Multimedia Information Networking and Security,2009.

[4] Wen Jie, Sun Xiaojun, Hu Minghao, Lu Kun, Robust Digital Image Watermarking algorithm Based on the characteristics, J. Computer engineering and applications. 44 (2008) 89-92.

[5] Wen Zhan, Huang Xiaoyan, Wen Chengyu, Robust Digital Image Watermarking algorithm Based on the Normalized Wavelet Transform, J. Digital video. 2 (2008) 32-34.

[6] Gao X B, Deng C, Li X L, Geometric distortion insensitive image watermarking in affine covariant regions, J. Applications and Reviews. 40 (2010) 278-286.

[7] Escalante Robert G, Malki Heidar A, Comparison of artificial neural network architectures and training algorithms for solving the knight’s tours, International Joint Conference on Neural Networks, Canada, 2006, pp. 1447-1450.

[8] Wei Rong, Liao Zhensong, Xu Wei, Digital Image Watermarking algorithm Based on visual features and DCT transform, J. Computer engineering. 33 (2007) 149-151.

[9] Niu Panpan, Yang Hongying, Wu Jun, Wang Xiangyang, Digital Image Watermarking algorithm Based on the Significant Region of the Normalized Image, J. Journal of Image and Graphics. 12 (2007) 1774-1776.

[10] Zhao Zheng，Xu Tao，Xi Pengcheng, A Robust against Geometry Transform Digital Image Watermarking algorithm, J. Journal of Nanjing University of Aeronautics & Astronautics. 37 (2005) 70-74.

[11] Luo Qiaoyi, Liu Lijun, Huang Qingsong, Robust method of digital image watermarking based on FourierMellin moments, J. Computer Engineering and Applications. 50 (2014) 99-104.