IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 3, Issue 10, October 2016

Fragile Watermark-based Electronic Police Information Processing System

Wu Jianzhen[1], Li Hongqin[2], Luo Xiao[3]

School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai[1, 2, 3]

Abstract: A fragile watermarking algorithm applying to electronic police information processing system is proposed in this paper. First license plate is extracted as the embedded watermark from illegal driving automobile image and then was embedded in DCT domain; watermark was extracted without original image. MATLAB simulation results show that the proposed watermarking algorithm can be embedded in the illegal driving automobile image captured by electronic eye, and watermark can be exactly extracted under the conventional image processing such as noise addition & JPEG compression. When watermarked image is subjected to cropping and license plate content tampering attack, the extracted watermark is not clear enough, thus indicates the illegal driving automobile image was tampered.

Keywords: license plate extraction, fragile watermark, DCT transformation, content tempering

1. INTRODUCTION

With the continuous development of information technology, public security traffic police departments around the country introduce the traffic police punishment information processing system, in which the illegal vehicle images shot through the electronic eye installed in the inter-section are taken as the basis for the implementation of illegal punishment. With the rapid development of digital image processing technology, it is more and easier to modify and process digital image and the effect is more and more realistic.

If the illegal driving images as material evidence was maliciously tampered with, the results of law enforcement is difficult to be fair. As an effective means for copyright protection and authority identification, digital watermarking technology has been one of the hottest issues with rapid development in the field of multimedia information security [1-3].

Faced with this problem, the vulnerable watermark authenticity identification features [4-5] can help identify whether illegal driving images have been malicious tampered.

In this paper, firstly, the license plate is segmented by color segmentation method of color information of vehicle license plate, and the license plate image is extracted. Then, two sets of pseudo-random sequences are used to embed watermark in DCT domain. When extracting the watermark, the original illegal driving image is not needed, so it is a kind of blind watermarking system.

When the watermarked illegal image is subjected to conventional image processing such as adding noise and JPEG compression, the extracted watermark is intact. When the watermarked image is subjected to malicious cropping and content tampering, the extracted watermark is not clear enough and it indicates that the image has been tampered.

2. FRAGILE WATERMARK-BASED ELECTRONIC POLICE INFORMATION PROCESSING SYSTEM

2.1 Watermark generation

The part of the license plate from illegal driving image is used the watermark to be embedded. Therefore, it is necessary to locate and segment the license plate of the illegal driving image. According to the proven knowledge of the license plate background and so on, we use the method of color pixel points statistics to segment the reasonable license plate area and determine the gray scale range corresponding to the blue RGB of the license plate background. Then, we count the pixels point number in this color range in the row direction and set a reasonable threshold to determine a reasonable area of the license plate in the row direction. In the segmented row region, the number of blue pixels in the column direction is counted to determine the complete license plate region. After the license plate is extracted, it is transformed into a binary image with the value of {0,1} and the binary image is used as the watermark to be embedded.

2.2 Watermark Embedding Algorithm

It is supposed that the size of the illegal driving car image captured by the electronic eye of is $M \times N$. The captured images are usually color images. In order to simplify the algorithm, we first convert the color image into grayscale image and embed the watermark in the grayscale image. Inspired by reference [6], watermark embedding steps are as follows:

(1) If the size of the illegal vehicle image captured is not a multiple of 8×8 , scale it to a multiple of 8×8 .

(2) Perform 8×8 DCT transformation on the illegal driving car image.

(3) Generate two pseudo-random sequences with length of 8. These two sequences are independent of each other.

(4) According to the size of the original illegal vehicle image, we adjust the size of the binary image of the license plate. That is, the size of the binary license plate

DOI 10.17148/IARJSET.2016.31012

image should be less than $\frac{M}{8}\times\frac{N}{8}$. Otherwise, it can't be completely embedded. If the corresponding pixel position in binary watermark image $R(i, j)$ of the license plate has a value of 1, 8 locations are randomly selected in the small 8×8 blocks (a total of 64 positions) and pseudo-random sequence PN_1 will be embedded in these choosed positions. If the corresponding pixel position in binary watermark image $R(i, j)$ of the license plate has a value of 0, pseudo-random sequence PN_2 will be embedded. The watermark embedding formula is as follows:

$$X' = X + alpha * K \qquad (1)$$

where X' is the DCT coefficients with embedded watermark, X is the original DCT coefficient, $alpha$ is the embedding strength, and K is pseudo-random sequence, in our system, it will be PN_1 or PN_2. According to the watermark value of 1 or 0, it selects PN_1 and PN_2 respectively.

(5) After IDCT transformation, we get the illegal driving car images with embedded watermark.

2.3 Watermark Extraction Algorithm

After obtaining the watermarked driving car image which may suffer from the conventional image processing and various attacks during the transmission process, 8×8 DCT transform is carried out on the watermarked driving car image and then 8 chosen DCT coefficients are obtained according to 8 embedding positions.

The 8 DCT coefficients form a new sequence P that will perform correlation calculation with the related pseudorandom sequences PN_1 and PN_2. If

$$\mathrm{corr2}(P,PN_1)>\mathrm{corr2}(P,PN_2) \qquad (2)$$

The watermark bit is determined as 1, otherwise the watermark bit is determined as 0. After the watermark bit s are obtained, it can be rearranged into a matrix according to the size of the original watermark and displayed as an image, which is the extracted watermark.

3. SIMULATION RESULTS

In order to verify the validity of the proposed algorithm, simulation experiment is carried out on the illegal driving vehicle image taken from the electronic camera. The size of the original illegal color car image is 320×240 . The vehicle license plate is extracted from the image using the license plate extraction and segmentation algorithm, and is binarized as the watermark to be embedded. Then, according to the watermark embedding and extraction algorithm described above, the watermark is embedded in the inverse diagonal position of each sub-block. The embedding strength of the watermark is alpha = 14.

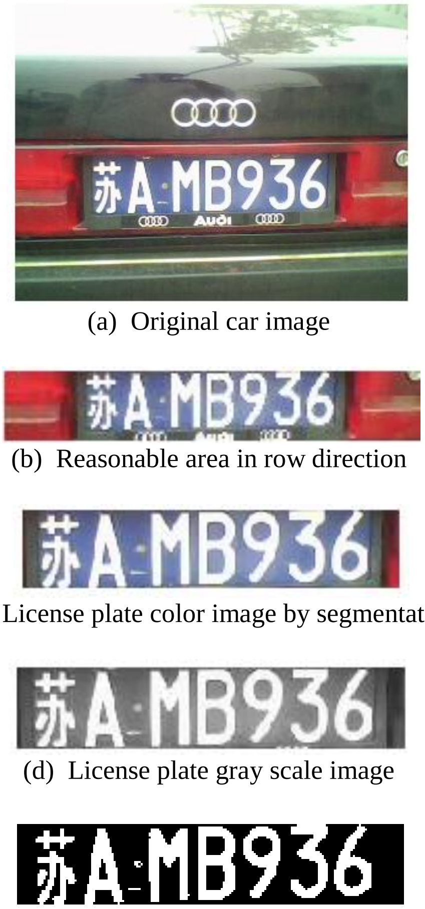
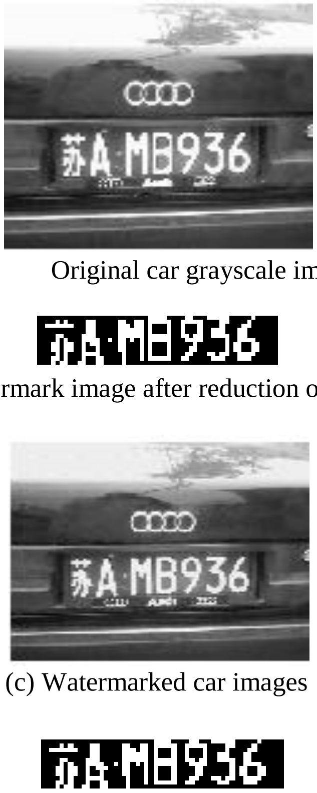

(a) Original car image
(b) Reasonable area in row direction
(c) License plate color image by segmentation
(d) License plate gray scale image
(e) License plate binary image
Fig.1 License plate segmentation process

Figure 1 shows the original car color image and the process of extracting the license plate from the image, converting the extracted color license plate into a binary image suitable as a watermark. Since the size of the extracted binary image of the license plate is greater than $\frac{320}{8}\times\frac{240}{8}$, the binary image of the license plate is reduced four times in order that it can be embedded completely. Figure 2 shows the grayscale image of the original car and the car image after embedding a 4-fold reduction of the license plate binary image as the watermark. In Fig.2, it presents the original and watermarked image, as well as the original watermark and the watermark extracted without suffering any attack. It can be seen from the Figure 2 that the watermarked image has almost no distortion. The PSNR between the original and watermarked image is 42.88dB and the extracted watermark is clearly visible. In order to verify the performance of the watermarking system when subjected to various image processing and malicious attacks, Figure 3 shows the watermarked car image and the extracted watermark with white noise added. As can be seen from the figure, although the visual quality of the watermarked vehicle image has been significantly distorted after adding noise, the extracted watermark is still clearly visible. Figure 4 shows the watermarked car image and the extracted watermark under JPEG compression with compression quality factor of 70. And also the extracted watermark is clearly visible without any distortion. Figure 5 shows the watermarked vehicle image and the extracted watermark under cropping attack. Because the upper half of the car image is cropped, the extracted watermark is not complete suggesting that the image is under attack. Figure 6 shows the watermarked car image and the extracted watermark with license plate portion is tampered. From the figure, we can see that the extracted watermark is not clear enough and it indicates that the image is subjected to malicious attack.



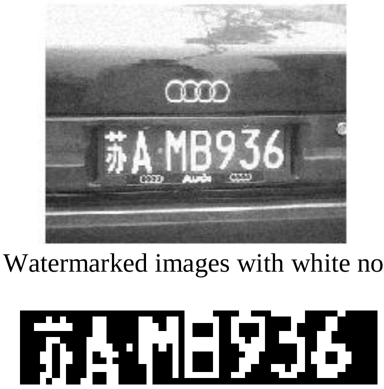
(a) Original car grayscale image

(b) Watermark image after reduction of 4 times

(c) Watermarked car images

(d) Extracted watermark without attack

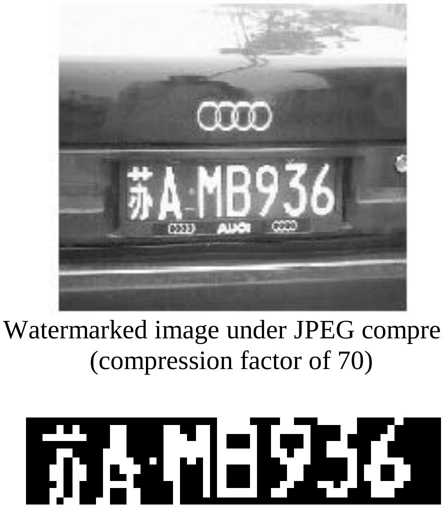
Fig.2 Watermark embedding and extracking



(a) Watermarked images with white noise added

(b) Extracted watermark under white noise attack

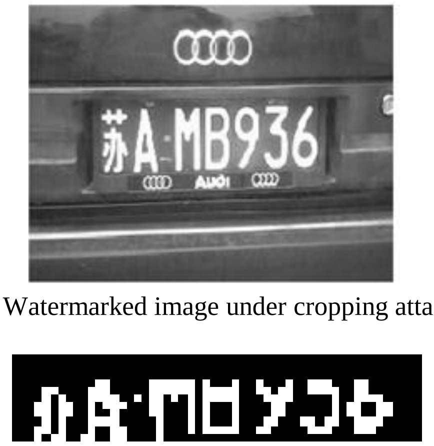
Fig.3 Watermarked image and extracted watermark under white noise attack



(a) Watermarked image under JPEG compression (compression factor of 70)

(b) Extracted Watermark after JPEG Compression

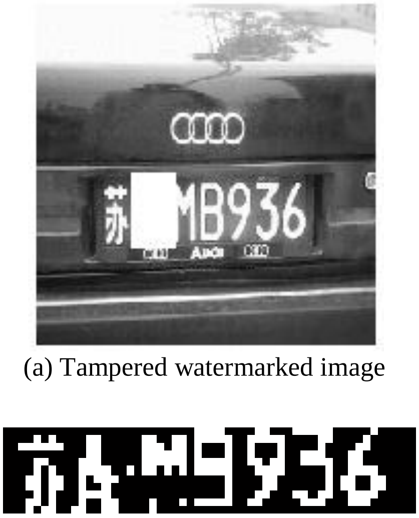
Fig.4 Watermarked image and extracted watermark under JPEG compression



(a) Watermarked image under cropping attack

(b) Extracted watermark under cropping attack

Fig.5 Watermarked image and extracted watermark under cropping attack



(a) Tampered watermarked image

(b) Extracted watermark under tampering attack

Fig.6 Watermarked image and extracted watermark under tampering attack

DOI 10.17148/IARJSET.2016.31012

4. CONCLUSIONS

In this paper, a new fragile digital watermarking algorithm used for the electronic police information processing system is proposed. The license plate image of the car image is regarded as the watermark to be embedded. After the license plate image is extracted by vehicle license plate segmentation algorithm, the vehicle license watermark is embedded into the vehicle image using the DCT transform domain algorithm. The simulation results show that the watermark can be extracted exactly when the image is not under attack, under noise and JPEG compression. When the watermarked image is croped or the content of the license plate is changed, the extracted watermark is not complete or clear, which indicates that the watermarked image is subjected to malicious attack.

REFERENCES

[1] Yao Zhao and Jeng-Shyang Pan and Zhenfen Zhu, RST Resilient Multi-bit Image Watermarking Based Bitplane Centroids, Imaging Science Journal, Vol. 56, No. 1, 2008,pp. 41-48

[2] Liao qi nan. Watermarking Geometric Correction Algorithm Based on SIFT Feature Point Matching, Journal of Computer Applications, Vol.28, No.6,pp. 2247-2249,2011.

[3] Teng Yiyan,Meng Youwen. Fast Algorithm of digital watermarking for image content authentication, Computer CD Software and Applications, No.6, pp.149-152, 2010.

[4] Zhu Congxu. Multi-functional Watermark for Image Copyright Notification, Protection and Content Authentication. Journal of Communications, Vol.30, No.11A, pp.101-104, 2009.

[5] Jiang Linsheng, Image content authentication implementation based on digital watermarking technology . Fujian Computer, No.2, pp. 15-15, 2008.

[6] Li Xudong. Image blind watermarking algorithm based on block DCT and quantization. Computer Engineering, No.21, pp.139-144, 2006.

DOI 10.17148/IARJSET.2016.31012