International Journal of Security and Its Applications
Vol. 9, No. 4 (2015), pp. 175-184
http://dx.doi.org/10.14257/ijsia.2015.9.4.17

A Robust Watermarking Scheme Based on Least Significant Bit and Discrete Cosine Transform*

Zhou Fu-an

Beijing Technology and Business University
netzfa@163.com

Abstract

In this paper, an image watermarking scheme is presented, in which Least Significant Bit and discrete cosine transform are used. The discrete cosine transform is performed on the original host image, and the secret watermark image is embedded into the coefficient of discrete cosine transform, which will replace the least significant bit. The embedded secret watermark bit will cause minimal distortion of the original host image, but we cannot find the difference of the original host image and the watermarked image. The experiment based on this algorithm demonstrates that the watermarking is robust to the common signal processing techniques, including noise attack, JPEG Compression attack and so on.

Keywords: *least significant bit; watermarking; Discrete Cosine Transform*

1. Introduction

In recent years, with the development of the technology of computer software and network technology day by day, digital products such as text, image, audio and video are widely used. The acquisition, copying and transmission of digital products was getting easier. As a result, illegal reproduction of digital information started to pose a real problem. This has raised questions and concerns about ownership rights [1-3]. Digital watermarking provides a solution for this problem. In short, it refers to embedding a secret imperceptible signal (watermark) in the original host-media, it was originated in the open network environment to protect copyright of multi-media, it verifies the copyright owner of digital products, identify vendors, buyers or evidence tampering identification, provides information on the content of other digital products and additional information. The information is not visible to the human eye[4-7].

LSB watermarking studied in this paper is most widely used but difficultly detected. In the past research people use the length of watermark to detect the existence of LSB watermark if the length is larger than some value. Many experts proposed new kinds of methods. Andrew D. Ker improved RS algorithm by new mask. He also improved SPA algorithm by increasing the samples calculated. Xiangwei Kong defined the bit-plane -complexity to find difference between cover images and steg-images.

In this paper, Based on chaotic sequence, an image watermark algorithm in DCT domain is presented and implemented. The watermark can be extracted from the watermarked image in a blind way, which does not require the original host image.

* * This paper is supported by the scientific research fund project launched by the young teachers of Beijing Technology and Business University in 2102Project No. QNJJ2012-12
This paper is supported by students' scientific research and entrepreneurial action plan project of Beijing Technology and Business University in 2014

ISSN: 1738-9976 IJSIA

2. Related Work

A. LSB Algorithm

The least significant bit (LSB) algorithms are based on bit-map method, which disrupted the input signal, and according to certain rules so that the distribution of the embedded information can be spread to all the pixels on the image, increasing the difficulty of destruction and change the watermark. The LSB technique is that inside of a cover image pixels are changed by bits of the secret message. Although the number was embedded into the first 8 bytes of the grid, the 1 to 4 least bits needed to be changed according to the embedded message. Because the lowest position of 1-4 is weak signal energy, it is difficult to detect visually and acoustically. On the average, about half of the original bits in an image will be modified to hide a secret message using a cover image. Figure 1 shows the 1-bit LSB.

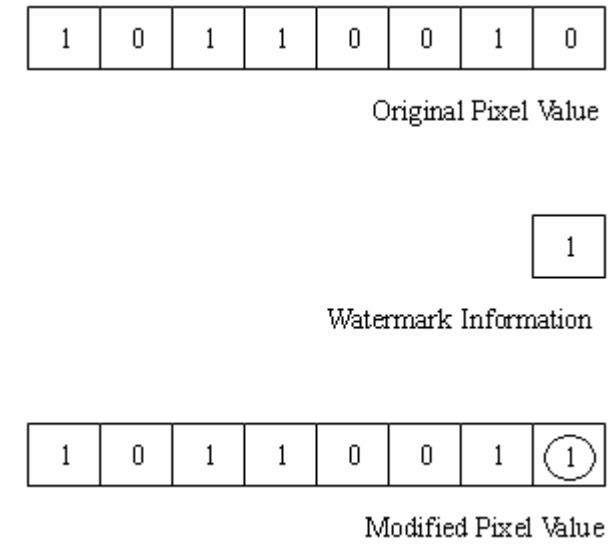

Figure 1. An Example of 1 Bit LSB

3. Algorithm Description

B. DCT BASED Watermarking

Discrete Cosine Transform (DCT) is a real number domain transform. Its transform is a cosine function of real number. It processes some other characteristics and advantages such as vector base good embodiment about image information, small computational complexity, high compression ratio, low error rate, good concealing, and so on, so it is considered the optimal transformation in the digital image processing [8].

When an image is processed by DCT, we can gain the Direct Current coefficients (DC) and the Alternating Current coefficients(AC).

Direct Current coefficients (DC): It is the first coefficient after the image transforming, which can indicate the average brightness of image.

Alternating Current coefficients (AC): It is the rest of coefficients except for DC. AC includes the high frequency coefficients, the intermediate frequency coefficients and the low frequency coefficients.

Figure 2 shows the frequency distribution of DC and AC. Figure 3 shows the direction distribution of DC and AC.

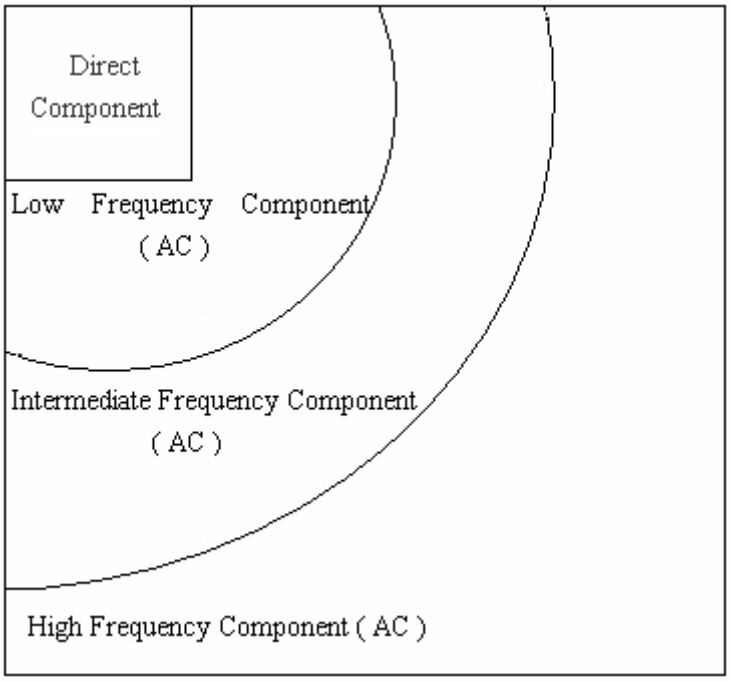

Figure 2. Frequency Distribution Diagram of DCT Coefficients

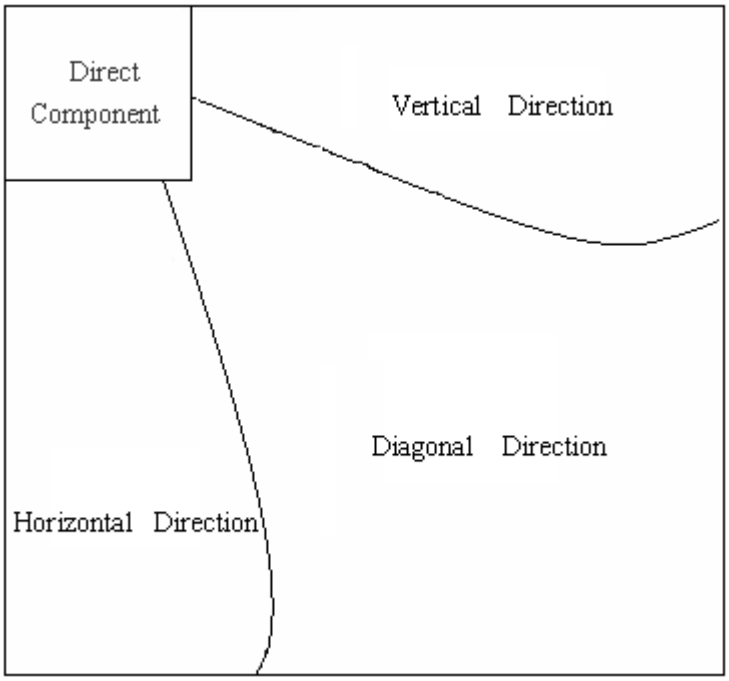

Figure 3. Direction Distribution Diagram of DCT Coefficients

The formulae of the 2-D DCT is expressed in formulae 1 and the formulae of the 2-D inverse DCT is expressed in formulae 4.

Formulae of the 2-D DCT:

$$F(u,v) = c(u)c(v)\frac{2}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\times\cos\left(\frac{2x+1}{2N}u\pi\right)\times\cos\left(\frac{2y+1}{2N}v\pi\right)$$

（1）

Which:

$$x, y, u, v = 0,1, \cdots, N-1$$

（2）

$$c(u) = c(v) = \begin{cases} \frac{1}{\sqrt{2}} & u = 0, v = 0 \\ 1 & Others \end{cases}$$

（3）

Formulae of the 2-D inverse DCT:

$$f(x, y) = \frac{2}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} c(u) c(v) F(u, v) \cos\left(\frac{2x+1}{2N} u\pi \right) \cos\left(\frac{2y+1}{2N} v\pi \right)$$

（4）

Which:

$$x, y, u, v = 0,1, \cdots, N-1$$

（5）

$$c(u) = c(v) = \begin{cases} \frac{1}{\sqrt{2}} & u = 0, v = 0 \\ 1 & Others \end{cases}$$

（6）

C. Image Embedding Algorithm

The framework of embedding is shown in Figure 4. Firstly, Logistic chaotic map is utilized to encrypt the embedding bits; Secondly, the original host image is performed on discrete cosine transform (DCT);Thirdly, the watermark bits are embedded into the coefficient of DCT by replacing Least Significant Bit; Lastly, the embedding bits are performed on inverse discrete cosine transform (IDCT), and the watermarked image is generated.

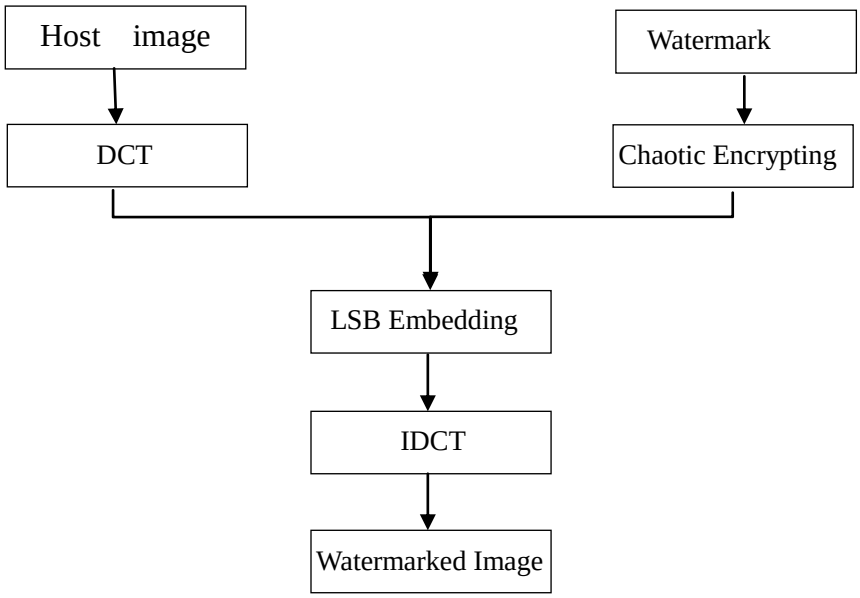

Figure 4. Framework of Embedding Watermark Into Host Image

D. Image Extracting Algorithm

The extraction process is far more simpler comparing to the embedding process.The framework of extracting watermark image is shown in Figure 5. The retrieved image is a binary image. In this process we don't need any additional information about the image. So the extraction is blind.

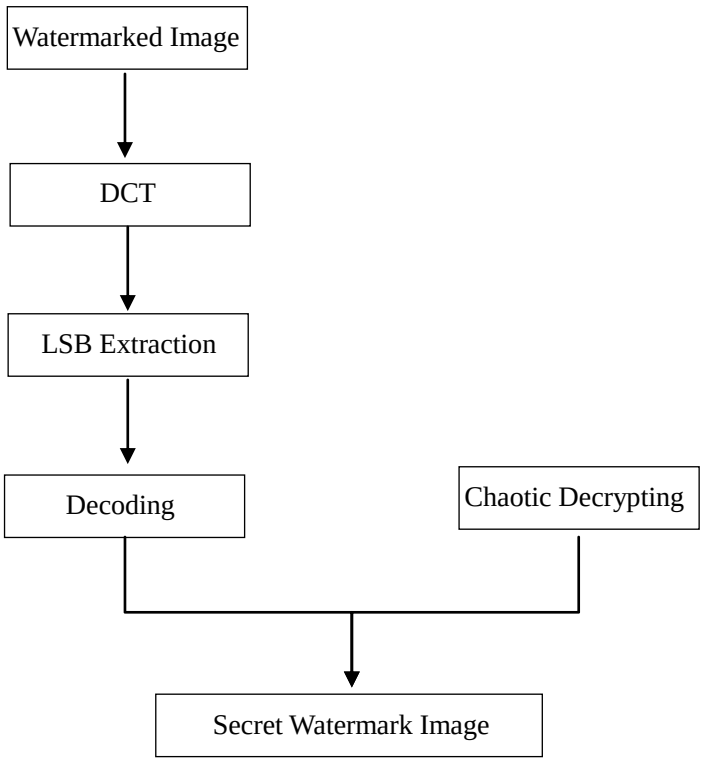

Figure 5. Framework of Extracting Watermark from Watermarked Image

4. Simulation Results and Analysis

Several simulations were performed to verify the validity of the proposed watermarking algorithm. A image of 512×512 pixels was used as host image. A binary image, with 32 ×32 bits, was used as watermark in the simulations.

we use the Bit Error Ratio(BER) and Signal-to-Noise Ratio(SNR) as the evaluation standard of the algorithm.As defined in [8], signal to noise ratio for the watermark embedded in time-domain is computed using the relation:

$$BER = \frac{1}{N}\sum_{i=0}^{N-1}\begin{cases}1 & w_i^{'} \neq w_i \\ 0 & w_i^{'} = w_i\end{cases} \quad (7)$$

$$SNR = 10\log_{10}\left\{\frac{\sum_{i=1}^{N} x_i^2}{\sum_{i=1}^{N}(x_i^{'} - x_i)^2}\right\} \quad (8)$$

Which:

In formula (7), $w_i^{'}$ represents extracted watermark bits and w_i stands for the bits of original watermark image;

In formula (8), $x_i^{'}$ represents sample of input image sequence and $x_i^{'}$ stands for sample of image with modified LSB.

A. Demonstration of invisibility

In the condition of no attack, the original host image and watermarked image are shew in Figure 6 and Figure 7 respectively; the original watermark image and extracted watermark image are shew in Figure 8 and Figure 9 respectively.

Figure 6. Original Carrier Image

Figure 7. The Watermarked Carrier Image

Figure 8. Original Watermark

Figure 9. Extracted Watermark

We test the difference between the original host image with the watermarked image. Experimental results show that the watermarked image has transparent feature, furthermore the quality of the extracted watermark image is satisfying, there is no obvious difference between the original watermark image with the extracted image.This is because digital watermark technology can take advantage of the characters of human hearing and vision to add some information in digital media, making it is very difficult for people to identify the differences between original message and changed message.

B. Demonstration of Robustness

（1）JPEG Compression Attack

In order to test the robustness of the algorithm, some attachs (such as JPEG attack, noise attack) have been done, and the test results are followed below:

Figure 10. Robustness Experiment 1

（ Quality Coefficient = 10%, BER=0.2146 ）

Figure 11. Robustness Experiment 2

（ Quality Coefficient = 40%, BER=0.0985 ）

Figure 12. Robustness Experiment 3

（ Quality Coefficient = 80%, BER=0.01876 ）

（2）Noise Interference

In order to test the robustness to Noise interference attack, we do some experiments by Lena and fruits. Experimental result shows in the fig 13, we can extract the secrect image correctly in the circumstances of strong noise.

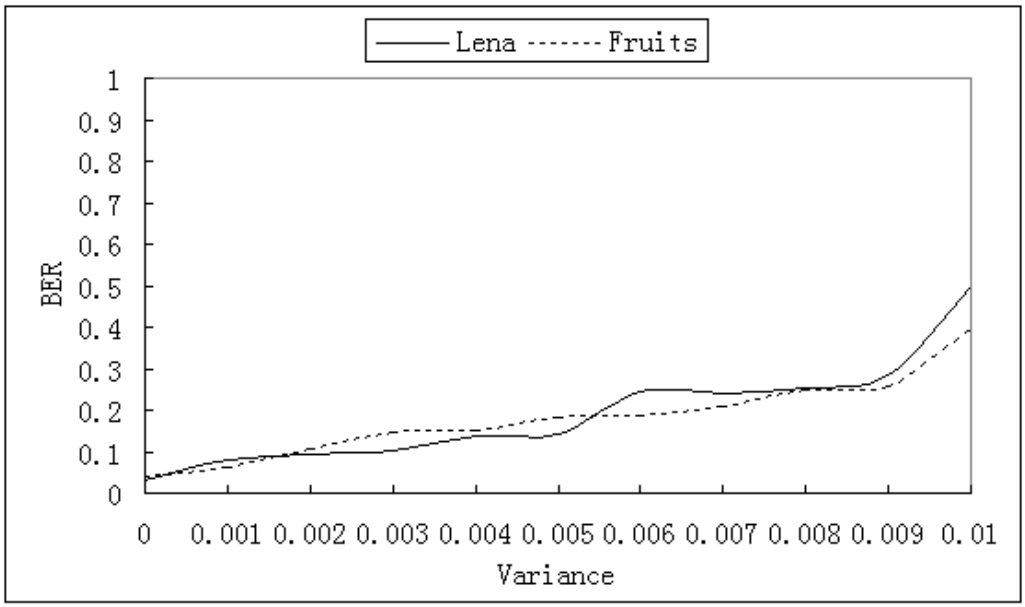

Figure 13. Result of Noise Interference Attack

The interference from white noise to the watermarked image is verified. The experimental result shows that we can extract the watermark image correctly in the circumstances of strong noise. The watermarked images are shown in fig 14 and fig 15, which are attacked by noise interference.

(a). Boat

(b). Airplane

Fig 14. Watermarked Image which are Attacked by Noise Interference (Variance = 0.004)

5. Conclusion

In recent years, digital watermarking technology becomes new information hiding technology from the research topic, it is a digital image as a cover for the media, the information will be kept confidential in accordance with an algorithm embedded in digital images.In this paper, we propose a blind image watermarking algorithm. The algorithm has the following advantages: Concealed, this feature is guaranteed by the

least significant bit embedding features, this algorithm changes the original host image little, which does not cause reduced visual quality; Robustness, the algorithm is robust to some attacks; High efficiency, the algorithms is simple, and have no special complex calculations; Practical, it can be applied to copyright protection easily. This algorithm is robust to many attacks, such as JPEG Compression attack, noise attack and so on.. It is fit for copyright protection, and it proposes a new measure for covert communication.

References

[1] N. Ishihara and K. Abe, "A Semi fragile watermarking scheme using weighted vote with sieve and emphasis for image authentication", IEICE Trans Fundam., E90-A, no.5, **(2007)**, pp. 1045-1054.
[2] A. Tjokorda Agung, B. W. Adiwijaya and F. P. Permana, "Medical Image Watermarking with Tamper Detection and Recovery Using Reversible Watermarking with LSB Modification and Run Length Encoding (RLE) Compression", COMNETSAT, **(2012)**, pp. 167-171.
[3] G. D. Duan and X. Zhao, "A Novel Semi-fragile Digital Watermarking Algorithm for Image Content Authentication", Localization and Recovery, Acta Electronica Sinica, **(2010)**, pp. 842-847.
[4] D. C. Lou and C. H. Hu, "LSB steganographic method based on reversible histogram transformation function for resisting statistical steganalysis", Information Sciences, vol. 188, no. 4, **(2012)**, pp. 346−358.
[5] B. Saha and S. Sharma, "Steganographic techniques of data hiding using digital images", Defence Science Journal, vol. 62, no. 1, **(2012)**, pp. 11−18.
[6] Y. M. Y. Hassan and A. M. Hassan, "Tamper Detection with Self Correction Hybrid Spatial-DCT Domains Image Authentication Technique", Communication Systems Software and Middleware and Workshops COMSWARE, **(2008)**, pp. 608-613.
[7] L. N. Cao, Y. J. Chen and L. Z. Ren, "A Robust Watermarking Algorithm Based on DCT Region and Its Realization by Means of Matlab", Computer knowledge and technology, no. 9, **(2007)**, pp. 813-814
[8] R. Zhang, "A Novel Image Authentification Based on Semi-fragile Watermarking", Proceedings of the Fifth International Joint Conference on Computational Sciences and Optimization, CSO, **(2012)**.
[9] K. Roland, M. Peter and U. Andreas, "A lightweight Rao-Cauchy detector for additive watermarking in the DWT-Domain", International Multimedia Conference Proceedings of the 10th ACM workshop on Multimedia and security, **(2008)**, Oxford.

Authors

Zhou Fu-An,he received the B. education technology degree from Qu Fu Normal University and the M. education technology degree fr om He Bei University in 2004 and 2007 respectively. He is currently working in Bei Jing Industry and Commerce University. He is current ly researching on E-commerce Security and The Practice Teaching M ethods

