Secure Web-Based Image Transmission System Using Digital Watermark

K.Karthik [1], Dr M.A.Dorai Rangaswamy[2]

[1]*Assistant Professor (Grade-II) Department of CSE Technology AarupadaiVeedu Institute of Technology*

[2,]*Senior Professor & Head Department of CSE Technology AarupadaiVeedu Institute of Technology*

Abstract: *A web-based image transmission system using digital watermark is presented with experimental results in this paper. This system assures when pirated image is found, the illegal user can be traced. The user's message after chaotic encryption as watermark embeds into image. Experimental results show our system which is used for a web-based image transmission is effective and robust. Especially, user's message can also be extracted from watermark image under diverse attacks such as some image-processing operations and JPEG compression.*

Keywords*-digital watermark; chaotic sequence; image transmission; robust*

I. INTRODUCTION

In the recent years, with the rapid development of communication and the computer technology, it has created an environment in which it became very easy to obtain, replicate and distribute digital media products such as digital text, image, video and audio without any loss in quality. In fact, an enormous number of digital products have been pirated. Protection of digital multimedia products have therefore become an increasingly important issue for products owners and service providers. Digital watermarking is finding more and more support as a possible solution for the protection of intellectual property rights[1].Digital watermarking is a technique of embedding some information into the given media, which can be later extracted or detected for variety of purposes[2-5]. The data embedded is called as watermark and the given media is called as host or cover media. A user can pay for obtaining on-line image from a productprovider∧PP∧. However, unprotected image can be easily pirated by some users, while the user may leak theImage to illegal user. Ever if a pirated image has been found, it is almost impossible to identify which user has pirated the image.The traditional watermark technology can't solve these problems. According to the different user ID, the unique ID watermark is generated and embedded host image before distributing[6]. In this scheme, if a pirated image has been found, the PP can extract the user ID to trace the leaker and supervise illegal using. This model provide an effective watermark to protect property.

II. THE IMAGE TRANSMISSION SYSTEM BASED ON WATERMARK

The image transmission system based on watermark resolves the defect of conventional watermark image. In this system, users' privacy message can be embedded image in order to obtain trace of output images.The system's target is when pirated image is found, we can extract watermark from image to identify which user pirates image. Therefore, embedded watermark must be able to verify the unique user. The different user gets different embedded watermark image, though it is the same host image. The differentiation among embedded watermark images can't recognized by human eyes.

The system's detail is described below with an illustration in Fig1.

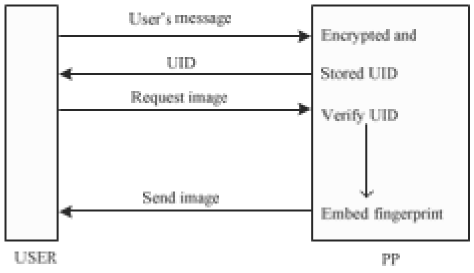


Fig1 Image Transmission System

[1] The user proceeds for registration through the registration website managed by PP. The user enters his name, email address, purchasing card and so on to obtain a unique user ID(UID) for ever y user. UID is chaotic encrypted and stored in user account database of PP.

[2] The user sends a message to request an image from PP. PP verifies the user's UID.

[3] If the user's UID is legal, PP embeds the chaotic
encryption of UID into image. The watermark image is sent to

III. WATERMARK EMBEDDING

In this section, we describe the processing of watermarking. UID is stored by PP, and PP encrypted every user's UID by the chaotic sequence as UID watermark[7,8]. When a user asks PP for an image, PP embeds a unique watermark according to the different UID into an image and sends it to the user.

A. Chaotic encryption for UID

Because of the fine pseudo-random features of chaotic sequence ︿ the randomness of the watermarking can be improved by Logistic chaos. UID is a string of binary data UID[i], according to the length of UID[i], the same length of chaotic sequence L[k] is selected, which is permuted by key A we make logic opertation between UID[i] and L[k],Y[i] is the result. Y[i] is oversampled by Cutting frequency speed C, the modulated signals D[k] is generated. D[k] is modulated by chaotic spread spectrum sequence formed the same key A. then final watermarking signal W[k] is generated

B. Embedding Procedure

The embedding technique of watermark is given as follows and the steps of embedding approach are shown as Fig2.

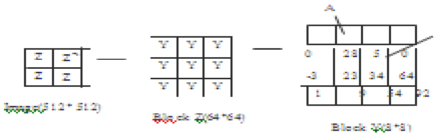


Fig2 Embedding Procedure

1) Assume that the size of the host image is 512×512. Host image is divided into small *M* ×*M* blocks *Z*, block Z is divided into small *M* ×*M* blocks Y. If M=8 is used, the size of block Y is 8×8. 2) A number of pairs of coefficients (*A*,*B*) in block *Y* are chosen as $A = a_1, \ldots, a_n, B = b_1, \ldots, b_n$ based on a pseudo-random numbers, and mapping key that contains index of original chosen coefficients are kept. For coefficient selection, it is required that S_n is the expected value of the sum distance between a_i and b_i, which approaches 0[9].

$$S_n = \frac{1}{n}\sum_{i=1}^{n}(a_i - b_i) \qquad (1)$$

$$\lim_{n \to \infty} s_n \to 0 \qquad (2)$$

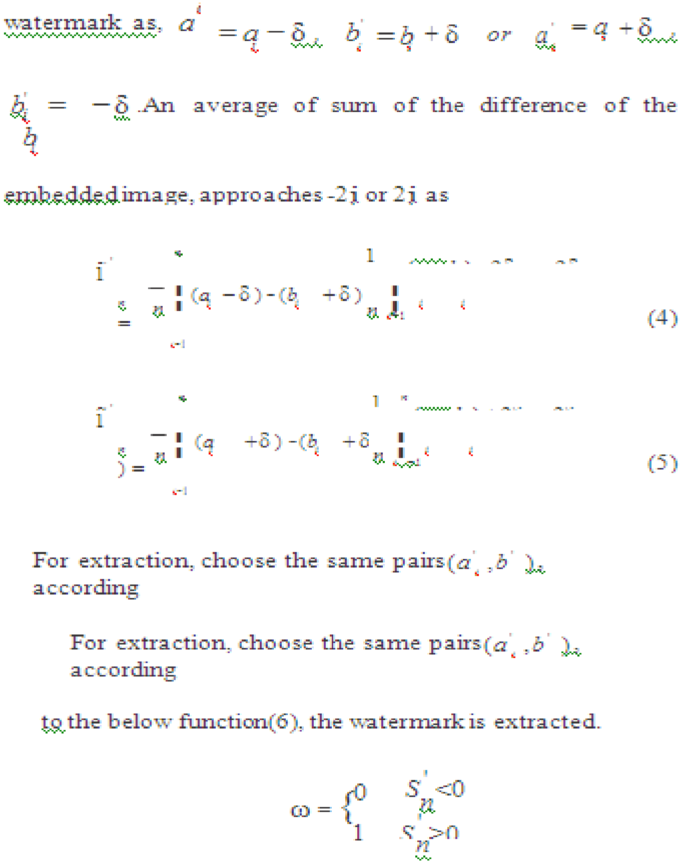
3) For embedding, two coefficient values (a_i, b_i) are modified by add parameter *ί* which is a parameter for watermark strength. i=1,…,n.

$$m = \begin{cases} 0 & a_i - \delta \ and \ b_i + \delta \\ 1 & a_i + \delta \ and \ b_i - \delta \end{cases} \qquad (3)$$

4) continue the above process according to *n*. Each block Y is embedded 1 bit watermark and watermark length decides how many block Y is embedded.

IV. WATERMARK EXTRACTION

In this section, the watermark extraction process is described.First, choose pseudo-random numbers and mapping key to assign two pixels (a_i, b_i) for n pairs from each block and modified value of the assigned pixels after embedded



watermark as, $a'_i = a_i - \delta$, $b'_i = b_i + \delta$ *or* $a'_i = a_i + \delta$,

$b'_i = b_i - \delta$ .An average of sum of the difference of the

embedded image, approaches -2į or 2į as

$$\bar{\imath}' = \frac{1}{n}\sum_{i=1}^{n}\left[(a_i-\delta)-(b_i+\delta)\right] \qquad (4)$$

$$\bar{\imath}' = \frac{1}{n}\sum_{i=1}^{n}\left[(a_i+\delta)-(b_i+\delta)\right] \qquad (5)$$

For extraction, choose the same pairs(a'_i, b'_i) according

For extraction, choose the same pairs(a'_i, b'_i) according

to the below function(6), the watermark is extracted.

$$\omega = \begin{cases} 0 & S'_n < 0 \\ 1 & S_n > 0 \end{cases}$$

Fig4 Watermarked Lena Image

To test and verify the robustness of watermark, the watermarked image is attacked by Gaussian filtering, sharpening, noise addition, cropping, median cut and JPEG compression[10].The results of watermark extraction which undergone above PP decrypted the extracted watermark by chaotic sequence and can restore the user's message.

VI.EXPERIMENTAL RESULTS

To illustrate the performance of the system, We implement the process by Matlab2007b.In the simulation, the host image is the “Lena” of size 512×512 pixels, as shown in Fig3 and Fig4 is watermarked image which is difficult to perceive the existence of watermark by human eyes. The watermark is binary message of 512 bits.

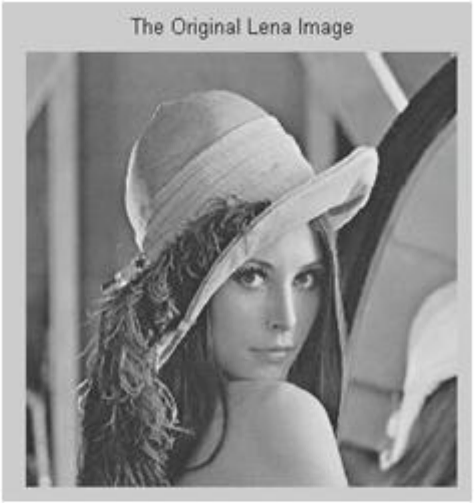


Fig3 Original Lena Image attacks are provided in Tableĉ.

Tableĉ Evaluation Results under Attacks

Attacks	Number of Attacks	Succeed
Gaussian filtering	2	ALL
sharpening	4	97%
noise	8	50%
cropping	3	NONE
median cut	4	95%
JPEG compression	7	ALL

Experiment results show that most extracted watermarks can be restored to UID after being attacked except noise and cropping attacks. there are not too much pirated value of the image, after noise and cropping attacks.

This means that the system can achieve good resistance to common web-based pirated image.

VII. LEAST SIGNIFICANT BIT INSERTION

The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels.

Simplified Example with a 24 bit pixel:
1 pixel:
(00100111 11101001 11001000) 2
Insert 101:-
(00100111 11101000 11001001)
red green blue
Simplified Example with an 8 bit pixel:
1 pixel:
(00 01 10 11)
white red green blue

Insert 0011: (00 00 1111) white blue blue

7.1Advantages of LSB Insertion: A major advantage of the LSB

algorithm is it is quick and easy. around LSB color alterations via palette manipulation. LSB insertion also works well with gray-scale images.

VIII. CONCLUSION

In this paper, a web-based image transmission system using digital watermark is presented with experimental results. Feasibility and robustness have been satisfied by encryption and watermark. Experimental results provide validity of our system which is used for a web-based image transmission under which user's message can be extracted when pirated image is found. Experimental results also demonstrate that user's message can be extracted from image under some image-processing operations such as JPEG compression and Gaussian filtering.

REFERENCES

[1] Nasir Memon and Ping Wah Wong ^" Protecting DigitalMediaContent", Communications of the ACM, vol.41, no.7, pp. 36-43, July 1998.

[2] Ingemar J.Cox, Joe Kilian,F.Thomson and Shamoon, "Secure Spread Spectrum Watermarking for Multimedia",IEEE Transactions on Image Processing,vol.6, no.12, pp. 1673-1687, Dec. 1997.

[3] F. A. P. Stefan Katzenbeisser, Information Hiding Techniques forSteganography and Digital Watermarking. Artech House, 2000.

[4] Yi Xiang,Wang Wei-Ran, "A Secure Watermarking Algorithm Based on Coupled Map Lattice ",Journal of Electronic Science and Technology of China, vol.3, no.1, 2005, pp.27-29.

[5] J. FURUKAWA, "Secure detection of watermarks," IEICE, vol. E87-A, no. 1, pp. 212–220, Jan 2004.

[6] Mitsuo Okada, Yasuo Okabe, Tetsutaro Uehara, "Security analysis on privacy-secure image trading framework using blind watermarking," The Third Workshop on Middleware Architecture in the Internet (MidArc2009), pp. 243–246, Jul 2009.

[7] Wang Hong-Xia , He Chen, "Robust Public Watermarking Based on Chaotic Map", Journal of Software, vol.15, no.8, August 2004, pp.1245-1251. [8] Voyatzis G, Pitas I. "Embedding robust watermarks by chaotic mixing" .13th International Conference on Digital Signal Processing. Santorini , Greece , 1997 :213-216.

[8] Voyatzis G, Pitas I. "Embedding robust watermarks by chaotic mixing" .13th International Conference on Digital Signal Processing. Santorini, Greece , 1997 :213-216.

[9] W. Bender, D. Gruhl, and N. Morimoto, "Technique for data hiding,"SPIE, vol. 2020, pp. 242–248.

[10] F. A. P. Petitcolas, "Watermarking schemes evaluation," IEEE Si