ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 4, June 2012

STUDY ON IMAGE BROADCAST USING WATERMARK AND SECURITY TECHNIQUES

SK.Sofia,
M. Tech student, Department of CSE,
Audisankara College of Engineering & Technology,Gudur

C.Rajendra,
Professor, Department of CSE,
Audisankara College of Engineering & Technology,Gudur

***Abstract*— Image broadcast is existing in this paper by experimental outcomes. In this method, an unauthorized person is easily determine through piracy of an image. Watermark is appended into image at the time of sending an image. Embedding the information into a digital signal is called as watermark and it is used to verify authenticity or identity of its owner. The embedded message contains some encryption of data. Cryptography and Digital Signatures are mainly used to provide security.**

Whatever the message will be added to image as watermark is also be extracted from watermark image to overcome different types of attacks such as image-processing operations. Digital signature and encryption must be applied at message creation time to avoid tampering. Probability and strength have been satisfied by encryption and watermark.

Keywords- watermark; encryption; image broadcast; digital signature.

I. INTRODUCTION

In the recent years, with the help of computer technology, it is very easy to establish, make an extra copy, and share out different products such as digital text, audio, video, image without any loss in quality. Even though, very large number of products are pirated. Protection that is., providing security for these type of products is a very important issue for the persons which are providing the service for these products and for the owners of these products. Digital watermarking is finding more and more support as a possible solution for the protection of intellectual property rights[1].

Encryption is any procedure to convert plaintext into ciphertext. RSA algorithm, Digital Signatures are used for encryption. Secure Quantization Index Modulation (SQIM) use both public and private keys like public key cryptosystems just like RSA. The private key is used by the watermark embedder to generate watermarks while the public key is used by the watermark detector to perform watermark detection in an encrypted domain[5].

It is mostly used to give security and unique user ids are also provided for different users. These user ids are appended with the message as watermark into an image. Different keys are used for encryption for different times. Pirated user is find out with the help of these different user ids.

Watermarking is a technique of embedding some information into the given media, and it is used to verify its authenticity or identity of its owner, and this watermark can be later extracted or detected for variety of purposes[2-5]. Data hiding is one of the technique of a steganography, in this we will embeds the data into digital media such as image for the purpose of identification.

How the data or some text will be hidden in an image? For this purpose, we will use LSB(Least significant Bit) algorithm. In the use of computing, LSB is the position of bits and in the binary integer it will give units value used to determine whether that number is even or odd. The LSB is also referred as right most bit, because we are placing less significant bits added to the right.

This steganography is one of the cryptography technique, and it is used to cover the information which is present in others. Cryptography is the combination of both encryption and decryption.

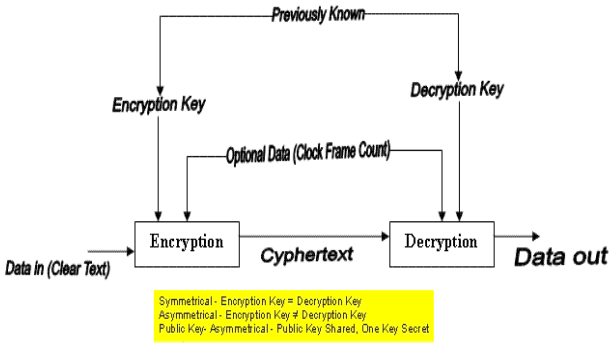


Fig: Procedure of Cryptography

The procedure of Cryptography is shown in the above figure. We are having two different techniques of steganographic algorithms:
1)Methods effort in spatial domain,
2)Methods effort in transform domain.

The best known steganographic method that works in the spatial domain is the LSB [11] (Least Significant Bit), which replaces the least significant bits of pixels selected to hide the information. This method has several implementation versions that improve the algorithm in certain aspects [7][8].

Insertion of data into images is very useful in a variety of applications. The information which is embedded into a digital signal is called as watermark, and the given media is called as host. Both Digital signatures as well as encryption should be applied at message creation time to avoid tampering.

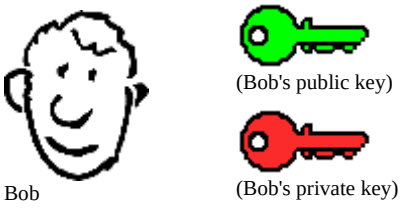
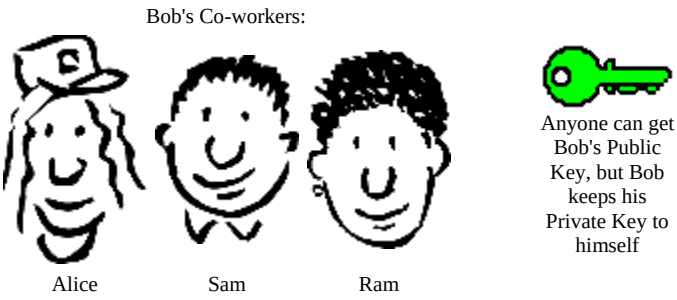


Fig: Overview of Digital Signature

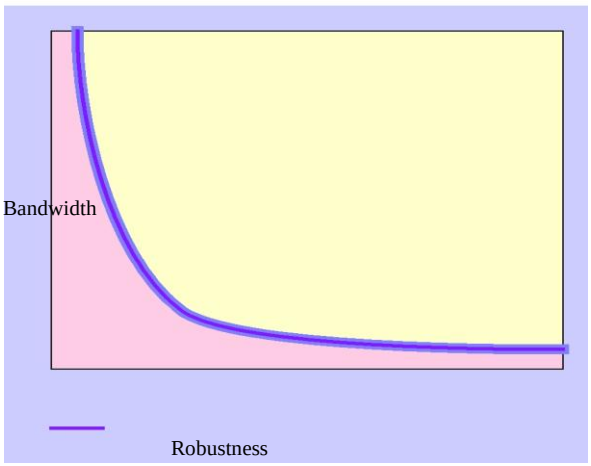
An overview of the Digital signature is shown in the above figure. Digital Signature provides a set of security capabilities that could be difficult to implement in any other way. In the above example, Bob is having 2 different keys. One of the Bob's key is known as public key and other one is called as private key. If more persons are working along with Bosb, they will get Bob's public key but they can't get Bob's private key. Bob is having his private key with himself only.



Problem space:

Each and every application of data hiding need a unique rank of variance to deviation and a variety of appended or embedded data speed. These form the imaginary data-hiding problem space which is shown in the below figure. There is a natural exchange between bandwidth and "robustness," or the level upto which, the data is protected to bother or transformations that will be happen to the signal during normal usage, for e.g., compression, resampling, etc.

Fig: Data hiding problem space



A user will pay to get on-line movies or on-line image from a service provider or Product provider PP. Even though, an unprotected image is easily pirated by various users, and they may leak the image to unauthorized persons or users. Ever if a pirated image has been found, it is very difficult to identify which user has pirated the image.

A long established watermark technique can't solve all these problems. According to the different user ID,

the unique ID watermark is generated and embedded host image before distributing[6]. Various users are having different user ids. Based on this user id, the leaker which will produce an image to unauthorized persons will be find out and the pirated image also found with the help of Product Provider.

II. IMAGE BROADCAST USING WATERMARK

Broadcast of an image with watermark solves the problems of predictable watermark image. The information which is embedded into a digital signal is called as watermark, and the given media is called as host. In this technique, the users' secracy information or message is embedded or appended into an image to get copy of various output images.

The system's main target is that when pirated image is find, we will take out watermark from the image to recognize which particular user pirates the image. Therefore, appended watermark into an image should be capable to prove the individual or unique user. Various user get various embedded watermark images, even though it will be the same image. The difference among these various embedded watermark images are not predictable by human eyes.

The entire system's architecture is described with an illustration in the following figure1.

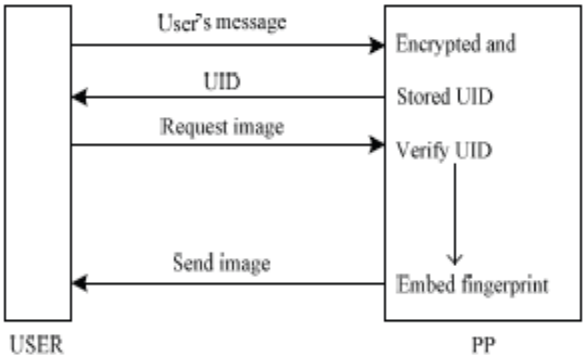


Fig1 Image Transmission System

1) The user move forwards for registration by the registration website maintained by Product Provider(PP). The user enter his or her name, email address, purchase card and so on to get a unique user ID(UID) for each and every user. This user id UID is encrypted and store in the user account database of Product Provider(PP).
2) The user will send a particular message to ask for an image from Product Provider. Then he verifies the particular user's user id UID.

3) If that user id UID is authorized, then the Product Provider (PP) embed the encryption of user id UID into an image. Then that particular watermarked image will be sent to the user.

III. PROCEDURE OF WATERMARK

In this section, we will describe the procedure of watermarking. Each and every user is having some user id, it will be differ for each user and it will be unique. This user id is stored in some database by Product Provider(PP). Every id is encrypted by using any of the encryption algorithm for ex., RSA and this encrypted user id is stored in database as watermark. When any of the user asks service provider or product provider for an image, Product Provider (PP) inserts a unique watermark with respect to various user ids into an image and it will be send to the user.

A. USER ID ENCRYPTION

User id is a collection of various strings of the binary data. Based on the length of this id, the same length of sequence bits will be selected and addition to this, we will permutted this sequence by some key. After that, we will perform some logic operations like AND, OR etc., between the user id and sequence bits, we will get some result. The result is sampled by the frequency speed C, then the modulated signal is generated. The modulated signal is modulated by the speed spectrum and formed by the same key, then the final required watermarking signal is generated.

B. EMBEDDING WATERMARK INTO IMAGE

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

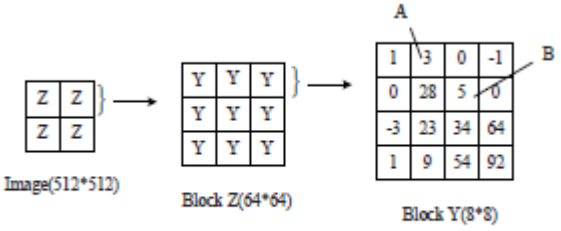


Fig2 Embedding Procedure

1)If the size of an host image is 512×512, then the actual or original image is divided into equal sized blocks $M \times M$ named as Z, and the block Z is again divided into equal sized blocks $M \times M$ named as Y. If we consider M=8, then the size of the block Y is 8×8.

2)If the number of pairs of coefficients (A,B) in the block Y are selected as $A = a_1, \ldots, a_n$, $B = b_1, \ldots, b_n$ based on a pseudo-random numbers, and the mapping key, and it contains an index of original selected coefficients are reserved. 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].

$$S_n=(1/n)\sum_{i=1}^{n}(a_i-b_i) \quad \rightarrow(1)$$

$$\lim_{x\rightarrow\infty} S_n \rightarrow 0 \quad \rightarrow(2)$$

3) For appending, these two coefficient values (a_i, b_i) are customized by the add parameter δ, which is a parameter and it is used for watermark potency. i=1,…,n.

$$\omega = a_i-\delta \text{ and } b_i+\delta \text{ if } 0; \quad \rightarrow(3)$$
$$\omega = a_i+\delta \text{ and } b_i-\delta \text{ if } 1.$$

4) Maintain the above procedure with respect to n. Each block Y is appended with 1 bit watermark and this watermark length will be decided the how many number of blocks Y are appended.

IV. WATERMARK MINING PROCEDURE

In this part, the watermark mining procedure will be described. In this, the watermark detector performs a hidden transform on the input data and then quantizes the transform coefficients while still in the encrypted domain[5].

First of all, we have to select some random numbers and the mapping key to allot two different pixel values (a_i, b_i) for n different pairs for each and every block and the customized value of the assign pixels after appended watermark as,

$$a_i' = a_i - \delta, b_i' = b_i + \delta \quad or \quad a_i' = a_i + \delta, \; b_i' = b_i - \delta .$$

Average of sum of the difference of the embedded image, approaches -2ı or 2ı as

$$S_n = \frac{1}{n}\sum_{i=1}^{n}(a_i - \delta) - (b_i + \delta) = \frac{1}{n}\sum_{i=1}^{n}(a_i - b_i) - 2\delta = -2\delta \quad (4)$$

$$S_n = \frac{1}{n}\sum_{i=1}^{N}(a_i + \delta) - (b_i + \delta) = \frac{1}{n}\sum_{i=1}^{n}(a_i - b_i) + 2\delta = 2\delta \quad (5)$$

For extraction, choose the same pairs (a_i , b_i) , according to the below function(6), the watermark is extracted.

$$\omega = \begin{cases} 0 & S_n' < 0 \\ 1 & S_n \geq 0 \end{cases} \quad (6)$$

Product Provider decrypts an extracted watermark by some sequence and it will bring back the particular user's message.

V. EXPERIMENTAL RESULTS

To explain and demonstrate the system's performance, we implement the process by Matlab2007b. In addition to this, we are also using RSA algorithm to provide encryption and security. In this simulation work, an image is the "Roses" which is of size 512×512 pixels, as shown in Figure which is watermarked image which will be complicated to recognize the reality of watermark by the human eyes. The watermark is the binary message which is having the size of 512 bits.

Fig: Roses with apending watermark into an image

To test and verify the robustness of watermark, the watermarked image is attacked by Gaussian filtering, sharpening, noise addition, crop, median cut and JPEG compression[10].

The consequences of watermark extraction which will go through the above attacks are provided in the following Table:

Attacks	Number of Attacks	Succeed
Gaussian filtering	2	ALL
Sharpening	4	97%
Sound	8	50%
Crop	3	NONE
median cut	4	95%

Table: Evaluation of results under various attacks

These experimental results illustrate most of the extracted watermarks will be restore to the user id UID after attacked, apart from sound, crop and some of the attacks. There is not to a large extent pirated value of an image, after sound and crop attacks. That is means nothing but that the system be able to attain very good resistance to frequent web-based pirated image.

VI. CONCLUSION

In this paper, an image broadcasting with watermark and some security techniques, is discussed with experimental results. These experimental results of our system shows the validity of our system which is used for a protected image transmission when piracy of the image will be found under which particular users message is extracted. Experimental results also reveal that the user's message can be extracted from image under some image-processing operations such as JPEG compression, RSA algorithm, LSB algorithms and Gaussian filtering.

REFERENCES

[1] Nasir Memon and Ping Wah Wong " Protecting Digital Media Content", 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 for Steganography 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] Moskowitz, I., Johnson, N. and Jacobs, M.: A detection study of an NRL steganographic method. NRL Memorandum Report NRL/MR/5540{02-8635, Naval Research Laboratory, Code 5540, Washington, 2002.

[8] Noto, M.: MP3Stego: Hiding text in MP3 files. Sans Institute, 2003.

[9]Wang Hong-Xia , He Chen, "Robust Public Watermarking Based on Chaotic Map", Journal of Software, vol.15, no.8, August 2004, pp.1245-1251.

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

[11] W. Bender, D. Gruhl, and N. Morimoto, "Technique for data hiding," *SPIE*, vol. 2020, pp. 2420–2440.

[12]F.A.P. Petitcolas, "Watermarking schemes evaluation", IEEE Signal Processing, vol.17, no.5, pp.58-64, Sep 2000.

[13] Kurak, C. and McHugh, J.: A Cautionary Note on Image Downgrading. Proc. IEEE 8th Annual Computer Security Applications Conference. San Antonio, USA, Nov./Dec. 1992, pp. 153-155.

[14] http://www.sciencedirect.com/science/article/pii/S0020025506001381

[15] http://www.youdzone.com/signature.html