EasyChair Preprint

№ 4865

An Analysis of Different Techniques of Security for Hiding Images

Monika Sharma, Manoj Kumar Sharma and
Prem Kiashor Gautam

January 5, 2021

An ANALYSIS of DIFFERENT TECHNIQUES of SECURITY for HIDING IMAGES

Monika Sharma [*1], Manoj Kumar Sharma[#2], Premkishor Gautam[#3]
[*1] *M.Tech Scholar, Department of Computer Science & Engg., MIT Bulandshahr UP, India*
[1]monika1512015@gmail.com
[2, 3] *Assistant Professor, Department of Computer Science & Engg., MIT Bulandshahr Up, India*
[2]manojcs2005@rediffmail.com
[3]pk_enggcs@yahoo.co.in

Abstract: Now's a day world is the system of sending and displaying data over the network, the security is the main issue concerned with his. In this paper we study of different hiding techniques for secure data. Security system uses different communication channels between sender and receiver. In security system cryptography, steganography and information hiding techniques use for hiding data and provide security in the public places. Cryptography is the technique and method of storing and transmitting data in a particular way for secure communication. Cryptography is the process in which plain text converted in to cipher text. Steganography is the art of hiding data and convert original image into stego-image.

Keyword – Steganography, Data hiding, Digital Images, Watermarking Technique, Fingerprint.

I. INTRODUCTION

System security or information security require more important after the spread of internet application. However, developers of sensitive documents, data and files must protect from unwanted spying, copying, theft and false representation. This problem solved by using steganography and information hiding technique. We study many differences between cryptography and steganography but the major difference is cryptography view individual's information by seeing the coded information but in steganography, the existence of the information in the sources will not be noticed at all. In the digital world, steganography technique is not based on computer program coding but is based on human vision system. In this system human eyes cannot see any complex binary patterns that mean human eyes are blind. In other word authorized and an unauthorized person cannot see the directly effect of the data changes. Human vision system play important key role in steganography for large capacity image hiding. This uses a color image in a BMP file formats. Normally, security system hides information in two ways 1) Cryptography and 2) Steganography. Cryptography method provides the data undecipherable to visitor by many transformations, whereas steganography method hides the existence of data. So this method and technique of hiding is called image steganography. In hiding information techniques, each pixels of image divided in to a particular secret data so human easily not access it. Now using a steganography and other hiding security system, this improve the quality of image and secure data. Steganography also used in other field like e-document, copyright and so on [1].

1). System Security: In system security there are three techniques for hiding data like cryptography, steganography and watermarking. Steganography and Watermarking techniques both are used for hiding and secure data in the public places. In figure.1 represented here steganography in digital image and does not discuss other types of steganography (such as linguistic or audio). Watermarking technique is the second type of information hiding technique. This technique applies on robustness for hiding and secures data with help of imperceptible, visible image and biometric features like fingerprint, face reorganization. Iris etc.

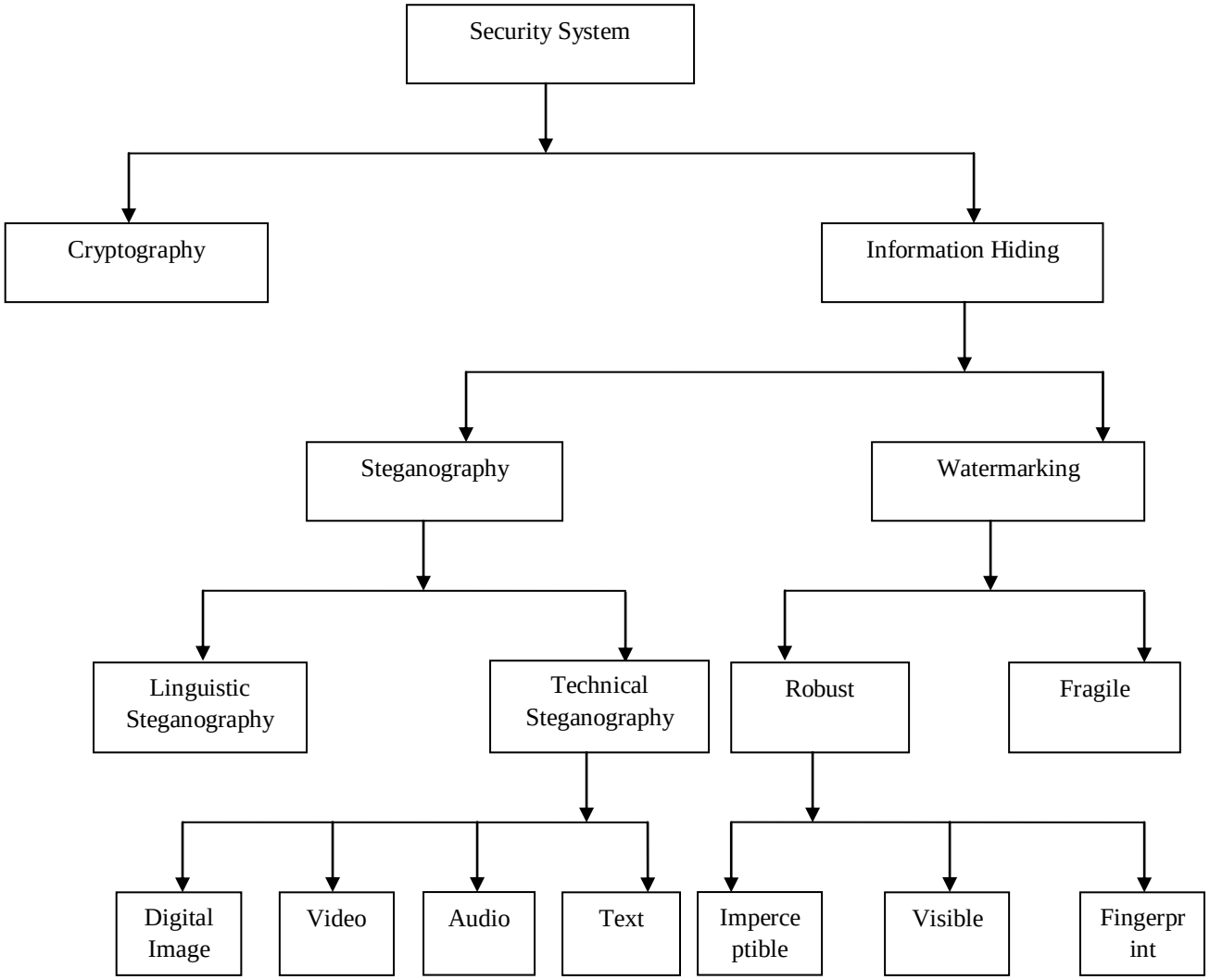

Figure. 1 Overview of Security System

I. STEGANOGRAPHY TECHNIQUE

Steganography is a technique of hiding information from original image to cover image (stego-image). Its acts as a art and science for hiding data. Steganography is a combination of two words “stego” and “graphy”. In greeks words “stego” means “covered” and “graphy” means “writing” that is “covered writing”. The main purpose of this technique is that observer and unauthorized person cannot view true message.

Unauthorized person should not be able to view cover image and stego-image. Now’s a day steganography is mostly used in digital data hiding/ image and networks for high delivery channels [4].

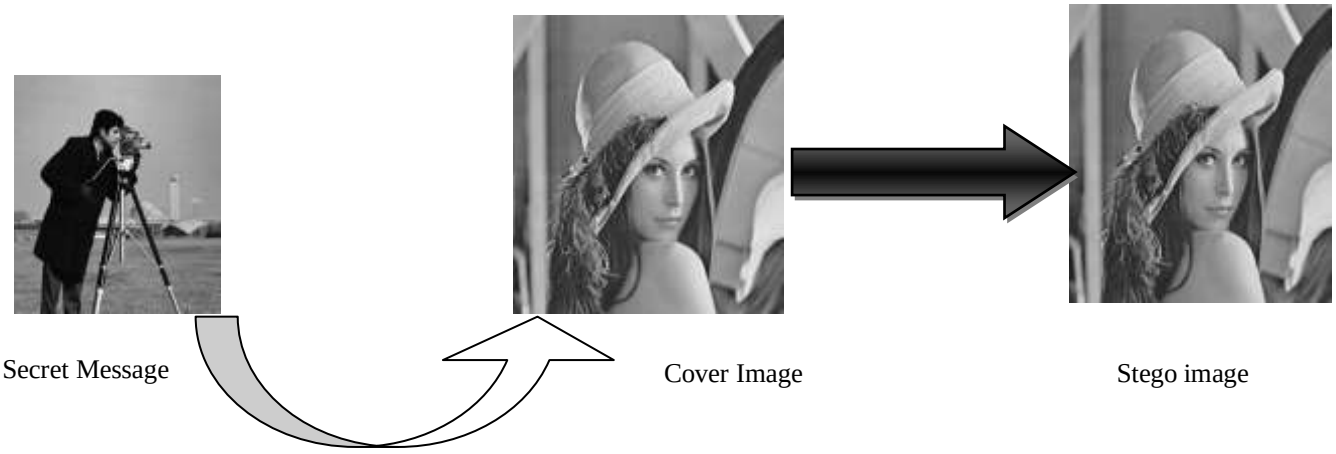

Figure. 2 Block diagram of steganography technique

Mostly steganography technique are used in many different file and text formats but in the digital world digital images and data are most used for hiding information because of their high communication frequency on Internet [5].

a) *Image Steganography:* In the image Steganography the information is hidden absolutely in images. The Image Steganography has been categorized into two [6].

b) *Spatial domain Steganography:* It primarily comprises LSB Steganography and Bit Plane Complexity Slicing (BPS) algorithm [8, 9]. Spatial domain is frequently used because of its high capability of hiding information and easy realization.

c) *Transform domain Steganography:* The secret information is embedded in the transform coefficients of the cover image. Examples of transform domain Steganography are Discrete Cosine Transform, Discrete Fourier Transform and Discrete Wavelet Transform. [7]

II. WATERMARKING TECHNIQUE

Watermarking technique is a process in which developer and an owner verifies information and embedded into digital image/data. These digital images/ data in the form like videos, pictures, text and audios.

Watermarking is of two types; visible watermarking and invisible watermarking [10] shown in Figure. 3.

Figure. 3 Visible and Invisible Watermark

A watermark is a "Secret message" that is embedded in to a "Cover message". Secret key allows us to extract the watermarking using LSB and Random [12].
Watermark techniques depend on two algorithms 1) Watermark Embedding Algorithm and 2) Watermark Extracting Algorithm.

a). Watermark Embedding Algorithm : The digital data watermark embedding algorithm used single value decomposition technique, these technique perform the characteristics of the D and U components. In the embedding algorithm, the largest coefficients in D component were customized and used to embed a watermark [11]. In this way, the quality of the watermarked image can be decomposed by quantization method. The watermarks embedding algorithm can be described as follows.

Step 1: Read the original image.

Step 2: Partition the image into blocks of n × n pixels.

Step3: Perform singular value decomposition (SVD) transformation**.**

Step 4: Extract the greater coefficient D (1, 1) from each D component and quantize by using a predefined quantization coefficients A.
Suppose that S = D(1, 1) mod A.

Step 5: Perform embed the two pseudo-random sequences PN0, PN1, that is applied to the mid-band coefficients. If A is the matrix of the mid band coefficients of SVD transformed block, then embedding is done as follows:
If the watermark bit is 0 then,
D′(1, 1) = D(1, 1) + K/4 – A,
so that [A < 3K/4]
Otherwise, if the watermark bit is 1 then, D′(1, 1) = D(1, 1) –K/4 + A,
so that [A < K/4].

Step 6: Perform the inverse of singular value decomposition transformation to reform the watermarked image.

a) *Watermarking Extracting Algorithm:* The digital data watermark extracting algorithm is similar to the watermark embedding algorithm. Extraction algorithm is the same as embedding and pre-filtering is used before applying SVD transform to superior split watermark in-formation from original image [14]. The watermark extraction algorithm is performed as described by the following steps [11]. These extracted bit values convert the original image SVD from the extracted watermark. The extracted watermark can be specified by original watermarked image **.**

Step 1: Read the watermarked image.

Step 2: watermarked it into blocks of n × n pixels.

Step 3: Perform the SVD transformation.

Step 4: Extract the greater coefficients D"(1, 1) from each D component and quantize by using a predefined quantization coefficients A.
Suppose that S = D'(1, 1) mod A.

Step 5: Regenerate the two pseudo random sequences number using the same key, which is used in the water-mark embedding algorithm.

Step 6: For an extraction watermark bit valued of zero, if A < K/2. On the other hand, the extraction watermark bit value of one, if A > K/2.

Step 7: The watermark is restructured using the extracted watermark bits, and compute the similarity between the original watermark and extracted watermarks [11].

1). Biometry: All human has its own or personal genetic and biological structure and these genetic structure totally different to each other. We know that every human being has its own uniqueness in the behavior, habits and so on.
Basically biometric techniques divided into five types fingerprint recognition, iris recognition, finger vein recognition, palm vein recognition and facial recognition. Biometric data basically come from biological structure so we can say that its totally unmatched and different from one another. Biometric structure explains in three methods 1) Physical 2) Behavioral and 3) Chemical. And all the characteristics used for authentication procedure and divided in like DNA, Face, Fingerprint and so on [13].
In this paper we discuss about fingerprint biometric feature. Fingerprint biometry based on human behavior. Fingerprint technology is one of the most widely used biometric that has been utilized in order to identify human being. Such technology now used almost everywhere regarding to prove person identity [14]. The minutiae features of the fingerprint are: whorls, loops, arches, and ridges (Figure. 4). All these features can be extracted from the image of the fingerprint. Many approaches have been adopted to perform the fingerprint recognition. The main benefit of using fingerprint biometric is low-error rate for such biometric [15, 16].
The uniqueness of a fingerprint is identified by a number of features called minutiae. This play a key role in the fingerprint.

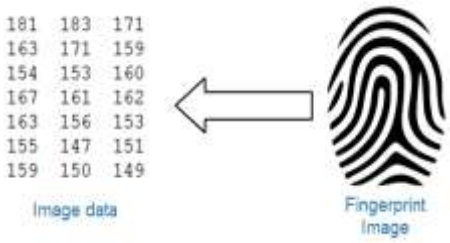

Figure. 4 Reading Fingerprint

The minutiae of the input fingerprint are founded. This step insures the use of only the most significant data out of all data inside fingerprint image. Then the finger minutiae has been encrypted using AES algorithm to enhance the security side in case using such fingerprint across networks which might be under unknown threats. The fingerprint minutiae are shown as Figure. 5.

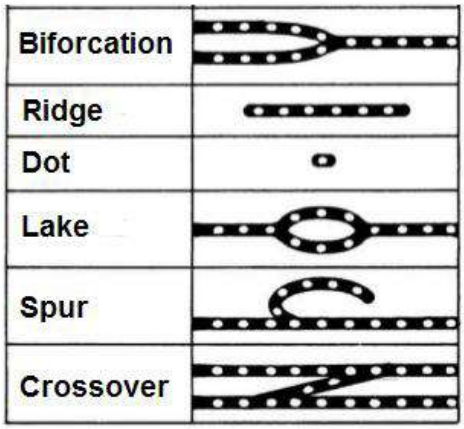

Figure. 5 Fingerprint Minutiae

III. COMPARISION TABLE

CRITERION/ METHOD	STEGANOGRAPHY	WATERMARKING	ENCRYPTION
Carrier	Digital media	Most image/ audio files	Text based
Secret data/ Key	Payload / optional	Watermark	Plain text/necessary
Input files/ detection	At least two unless in self-embedding/Blind	Usually informative	One/Blind
Authentication	Full retrieval of data	Usually achieved by cross correlation	Full retrieval of data
Objective	Secret communication	Copyright preserving	Data Protection
Result	Stego-file	Watermarked-file	Cipher-text
Concern	Delectability/ Capacity	Robustness	Robustness
Types of attacks	Steganalysis	Image processing	Cryptanalysis
Visibility	Never	Sometimes	Always
Fails	It is detected	It is removed/replace	De-ciphered
Relation to covers	Not necessary	Attribute of the cover image	N/A
Flexibility	Free to choose	Cover choice is restricted	N/A
History	Very ancient except its digital version	Modem era	Modem era

IV. CONCLUSION

In this research paper we discuss steganography and watermarking differences. The many non-oblivious watermarking techniques presents, which are most flexible for

geometric attacks and image processing to find the presence of a watermark using a correlated with an original head except in the rare watermarking like blind detection scenario.

Both digital watermarking and steganography employ steganographic methods to make a hiding data correctly in noisy signals. Basically digital watermarking tries to control the robustness as high priority, steganography role for imperceptibility to human senses. Many questions arise according to this technique. According to this paper one question arise child pomography exist inside evidently innocent image and audio files? Answer still is not unimportant but an evident is steganography and watermarking techniques useful for many encryption application and other technologies it can be misused.

REFERENCES

[1] Shashikala Channalli, Ajay Jadhav Sinhgad College of Engineering, Pune"Steganography an art of hiding data"(2009).

[2] Sudipta Kr Ghosal Greater Kolkata College of Engineering & Management Kolkata, India" A New Pair Wise Bit Based Data Hiding Approach on 24 Bit Color Image using Steganographic Technique".

[3] C.P.Sumathi, T.Santanam and G.Umamaheswari" A Study of Various Steganographic Techniques Used for Information Hiding".

[4] A.Nag!, S. Biswas*, D. Sarkar*, P.P. Sarkar*" A novel technique for image steganography based on Block-DCT and Huffman Encoding"

[5] Pratiksha Sethi, V. Kapoor(Dept. of Information & technology Institute of Engineering and Technology Devi Ahilya Vishwa Vidhyalaya, Indore)" A Secured System for Information Hiding in Image Steganography using Genetic Algorithm and Cryptography".

[6] Silman J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001.

[7] Lee Y. K. and Chen L. H., "High capacity image steganographic model", IEEE Proceedings of Visual Image Signal Processing, Vol. 147, No. 3, pp. 288-294, 2000.

[8] Ker A., "Improved detection of LSB steganography in grayscale image", Lecture Notesin Computer Science, pp. 97-115, 2005.

[9] Mahdavi, Samavi Sh., Zaker N. & M Hashemi.,"Steganalysis Method for LSB Replacement Based on Local Gradient of Image Histogram", Iranian Journal of Electrical & Electronic Engineering, Vol. 4, No. 3, pp. 59-70, 2008.

[10] https://www.slideshare.net/sudipnandi/steganography-and-watermarking-48088575

[11] Manjit Thapa, Sandeep KumarSood" On Secure Digital Image Watermarking Techniques,2011

[12] https://www.slideshare.net/sudipnandi/steganography-and-watermarking-48088575

[13] Sercan Aygün, Muammer Akçay"Securing biometric face images via steganography for QR-code".

[14] M. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, and R. López-Gutiérrez, "A robust embedded biometric authentication system based on fingerprint and chaotic encryption," Expert Systems with Applications, vol. 42, pp. 8198-8211, 2015.

[15] D. Bhattacharyya, R. Ranjan, A. Farkhod Alisherov, and M. Choi, "Biometric authentication: A review," International Journal of u-and e-Service, Science and Technology, vol. 2, pp. 13-28, 2009.

[16] M.-C. Cheung, M.-W. Mak, and S.-Y. Kung, "Intramodal and intermodal fusion for audio-visual biometric authentication," in Intelligent Multimedia, Video and Speech Processing, 2004. Proceedings of 2004 International Symposium on, 2004, pp. 25-28.