Research Article Impact Factor: 0.621 ISSN: 2319-507X
Gauri Joshi, IJPRET, 2014; Volume 2 (9): 935-940 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

APPLICATION OF DIGITAL WATERMARKING FOR DIGITAL CONTENT SECURITY

GAURI R. JOSHI[1], VIJAY B. GADICHA[2]

1. M. E. Scholar, department of CSE, P. R. Pote (Patil) College of Engineering, Amravati, India.
2. HOD, P. R. Pote (Patil) College of Engineering, Amravati, India.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, and video) within the signal itself. The steganography is closely related to this concept of watermarking, in that they both hide a message inside a digital signal[3]. However, the goal of these techniques separates them with one another. Watermarking tries to hide a message related to the actual content of the digital signal, while the digital signal has no relation to the message in steganography, and it is simply and only used as a cover to hide its existence. The digital content such as audio, video and multimedia etc that is freely available on internet must be secured is now a day's become critical issue. Embedding information data with an inaccessible form for human audio video system is realized by digital watermark. Digital watermark are transparent signature and are incorporated within the digital filers as noise or as random information being well managed and distributed throughout the entire digital file. It must be difficult for attacker to remove watermark purposely. In this we reviewed various watermarking methods techniques and application that have been presented and studied [1].

Keywords: Digital Watermarking, Data hiding, Copyright, Steganography.

PAPER-QR CODE

Corresponding Author: MS. GAURI R. JOSHI

Access Online On:

www.ijpret.com

How to Cite This Article:

Gauri Joshi, IJPRET, 2014; Volume 2 (9): 935-940

INTRODUCTION

In steganography the branch of computer science information hiding or hiding data in a message or file is the important principle. Cryptography, Steganography, and Watermark are three main categories of information hiding. The process of converting intelligible data into unintelligible data that can't be understand by unauthorized users is called cryptography. The only authorized user can decrypt the cipher text with the key. Now a day's many advances were made in the field of communication, now to decrypt a cipher text into intelligible data is become very simple. Hence cryptography is replaced by more sophisticated techniques. These methods are known as Steganography and Watermarking. Steganography is very lengthy and time consuming process. The real abstract of information is not detected by the attacker as this process hides the information over cover object. Watermarking is related to the steganography. Watermarking hides the information that is related to the cover object this is the main difference of steganography and watermarking. Watermarking is mainly used for copyright protection, owner authentication and id card security. Digital watermarking is the technique of embedding a digital signal (audio, video or image) or hide a small amount of digital data in intelligible data which cannot be easily been detected is called digital watermarking. Digital watermarking is also called data embedding.

Embedding, attack and detection are three steps of watermarking. The host(user) and data is accepted as input to be embedded and produce the watermarked signal in embedding by an algorithm. Then watermarked signal is transmitted to another person. If respective person makes a changes to the watermarked signal is called an attack. Various types of attacks are possible on the watermarked signal. An algorithm which accept attacked signal as input and extract the watermark signal from the attacked signal is called detection.

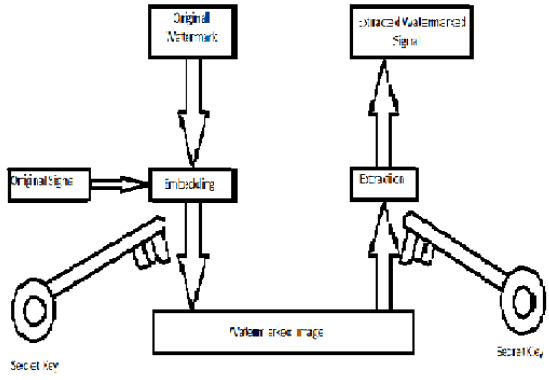

Fig 1: Block Diagram

2. METHODS AND MATERIALS:

2.1 Watermarking process:

The stages of watermarking are described as follows. Any watermarking generally consists of these three parts [1]:

1. The watermark

2. The encoder

3. The decoder

Each user has unique watermark or a user can also put different watermarks on different objects. Marking algorithms incorporate the watermarking into the object.

2.2 Types of Digital Watermarking:

There are two types of digital watermarking, these are

A. Visible watermark

B. Invisible watermark.

A. Visible Watermark:

Visible watermark consists of visible message or a company logo, used to identify the owner. The watermark signal is visible in the image, video or text, in the visible watermarking.

Example- Logo of the broadcaster such as ZEE TV, SONY, Life OK etc is on the right top corner of the television, it is visible to every user.

B. Invisible Watermarking:

The watermark signal is not visible in the invisible watermark. The watermark is embedded in such a way that the watermark is not visible to the user (Attacker). To provide image authentication and to protect image from being copied this technique is used. Invisible watermarking consists of encoding process and decoding process. Watermark insertion is represented as:

A" = EU (A, W)

Where A is the original image, W is the watermark information being embedded, U is the user's insertion key, and E represents the watermark insertion function.

2.2.1. Least significant bit watermarking:

Least significant bit watermarking is the spatial domain technique of watermarking. It can be applied to both visible and invisible watermarking. Modifying the pixels of one or two selected subset of the image is done by spatial domain technique. There we take an example of watermarking on image.

Steps-

1) Two images A, B will be selected from set of set of standard test image. The image A is the base image on which the watermark will be added and is selected from standard set of images. Second image B is considered as watermark image which will be added to the base image.

2) The most significant bit (MSB) of watermark image will be read and written on the least significant bit (LSB) of the base image A.

3) Now C will be watermarked image, resulting of combination of A will be watermarked with B. C is resulting image which is produce through combination of A and B.

Therefore C will contain an image A after its LSB replaced with the MSB of the image B. The base image and watermark image is consider in binary form-

Watermark Image= 11110101

Base Image= 11010111

2.3 Application Area

Any watermarking technique consists of a marking algorithm that inserts information, the watermark, into an image this is the basic concept. The watermark is inserted into the image by two ways the spatial domain or spatial frequency domain. As part of the watermarking technique, a testing algorithm must be defined in such way that tests an image to see whether a particular watermark is contained in the image. Depending on the desired properties of the data hiding scheme, we can classify data hiding applications into the following three categories:

(i) Watermarking for protecting intellectual property protection.

(ii) Watermarking for tamper detection.

(iii) Data hiding for multimedia delivery.

2.4 General Requirements:

Each watermarking application satisfies its own specific requirements. Therefore there is no globally accepted set of requirements as such that must be met by all watermarking techniques. There are some requirements mentioned below for watermarking techniques:-

1. Imperceptibility

2. Robustness

3. Resistance

4. Security

5. Computational Complexity

6. Modification and Multiple Watermarks

7. Scalability

2.5 Watermarking Techniques:

The watermarking techniques can be broadly classified in to two categories:

1. Spatial Domain: The pixels of one or more randomly selected subsets of item are modified in this domain [7, 8].

2. Frequency Domain: In this technique alters the certain frequency value from original value [9].

3. RESULT AND DISCUSSION:

Fig: The Image

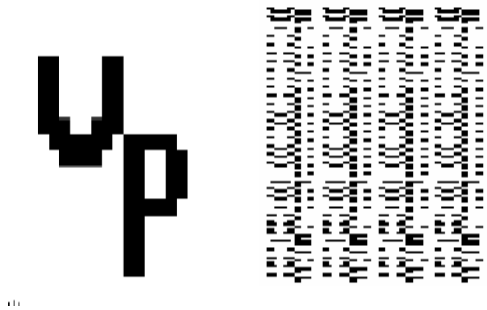

Fig: The original and recovered Watermark

The above three figure shows the original image and the watermark and the watermarked recovered when coded with LSB techniques. So, it becomes difficult for attacker to identify the data.

4. CONCLUSION:

The usage of internet has been tremendously increasing so it becomes very important to protect data from hacker. In this paper we discussed about digital watermarking technique. There are two types of digital watermarking techniques known as visible and invisible watermarking. Watermarking is the process of providing the authentication to the owner or the user. We can protect data from unauthorized duplication of data, if we will use digital watermarking technique in proper way.

5. REFERENCE:

1. I. J. Cox et al , "Digital Watermarking and Steganography" (Second edition), Morgan Kaufmann, 2008.

2. W. Bender D. Gruhl N. Moromoto and A. LU Techniques for data hiding. IBM Systems Journals, 35(3- 4):313_336,1996.

3. C. Cachin. AN information- theoretic model for steganography. Proc. Of 2nd Workshop on information hiding, 1996.

4. J Cox, M.L. Miller, J.M.G. Linnartz and T. Kalker, "A Review of Watermarking Principles and Practices" in Digital Signal

5. Bloom, J.A, I.J Cox, T. Kalkar, J.M.G Linnartz, M.L Miller and C.B.s Traw,1000. Copy protection for DVD Video

6. Cox, I.J, M.L Miller, J.M.G Linnatz and T.Kakar,1999, A Review of watermarking Principal and Practices.

7. Katezenbeisser, S.C.,1999, Principle of Steganography.

8. Kutter, M. and F. Hatung, 19999, Introduction to Watermarking Techniques.

9. Iangelaar, G.,I. Seyawan and R.L. Lagendijik,2000, Watermarking Digital Image And Video Data.

10. Meel, J., 1999. Spreed spectrum.