Volume 3, Issue 4, April 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

DIGITAL WATERMARKING

Dr. Ajit
SES, BPS Mahila Vishwavidhyalaya
India

Preeti Kalra
SES, BPS Mahila Vishwavidhyalaya
India

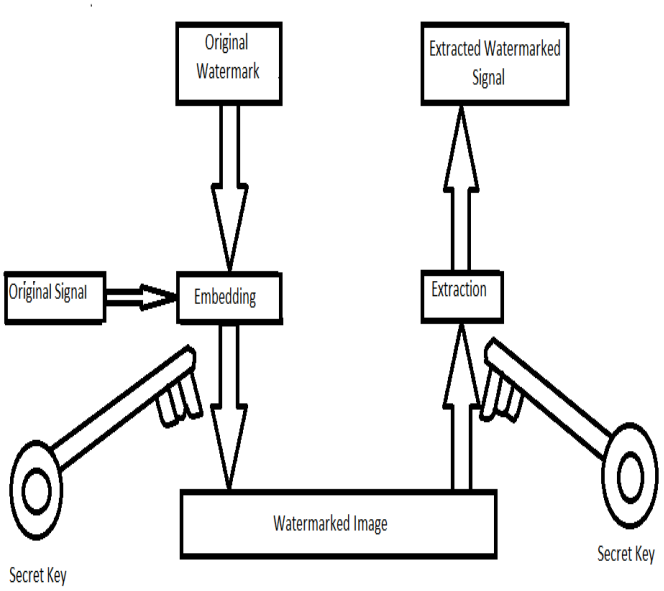
Sonia Dhull
SES, BPS Mahila Vishwavidhyalaya
India

Abstract— Everyday large amount of data is embedded on digital media and spread over the internet. This data can easily be replaced without error. Digital watermarking is the most important technology in today's world, to prevent illegal copying of data. Digital watermarking can be applied to audio, video, text or images.

Keywords— Copyright protection, Digital Watermarking, Steganography, Information hiding, Robustness.

I. INTRODUCTION

In computer science information hiding or hiding data in a message or file is the important principle of steganography. Information hiding is mainly categorized into three processes Cryptography, Steganography, and Watermark. Cryptography is the process of converting intelligible data into unintelligible data that can't be understand by unauthorized users. The authorized user with the key can decrypt the ciphertext. As many advances were made in the field of communication, now it became simple to decrypt a ciphertext into intelligible data. Hence more sophisticated methods were developed to provide better security than cryptography. These methods are known as Steganography and Watermarking. Steganography is the time consuming process. It hides information over a cover object in such a way that the sence of information is not detected by the attacker. Watermarking is related to the steganography. There is one main point in watermarking is that the hiding information is related to the cover object. 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 can not be easily removed is called digital watermarking. Digital watermarking is also called data embedding.



Watermarking block diagram

A watermarking system is divided into three steps embedding, attack and detection. In embedding an algorithm accept host and data as input to be embedded and produce the watermarked signal. Then watermarked signal is transmitted to another person. If this person makes a changes to the watermarked signal is called an attack. There are various types of attack is possible on the watermarked signal. Detection is an algorithm which accept attacked signal as input and extract the watermark signal from the attacked signal.

II. 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. In visible watermarking, the watermark signal is visible in the image, video or text.

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.

Simple watermarked image

B. Invisible Watermark- In invisible watermark the watermark signal is not visible. The watermark is embedded in such a way that the watermark is not visible to the user (Attacker). It is used to provide image authentication and protect image from being copied. 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.

Invisible Watermarking (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. Spatial domain technique modifies the pixels of one or two selected subset of the image. 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 will be selected as base image on which the watermark will be added. Second image B will be 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.

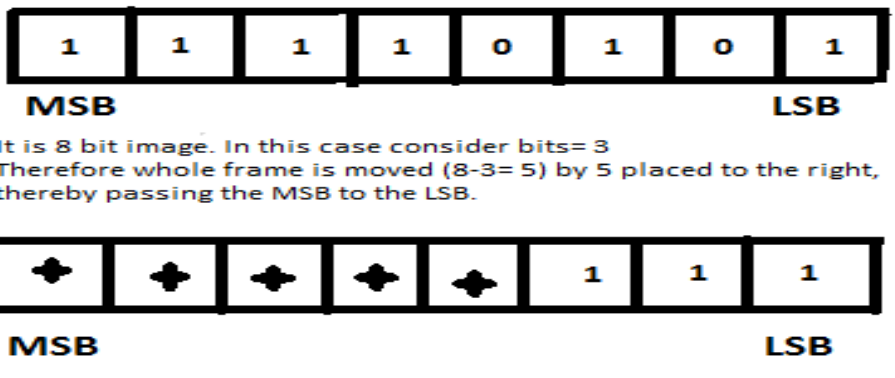
Therefore C will contain an image A after its LSB replaced with the MSB of the image B.

The base image and watermark image is consider in binary form-

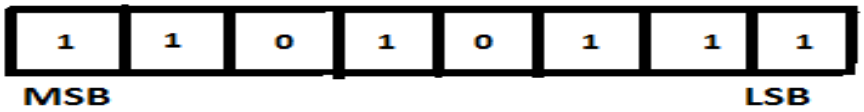
Watermark Image= 11110101

Base Image= 11010111

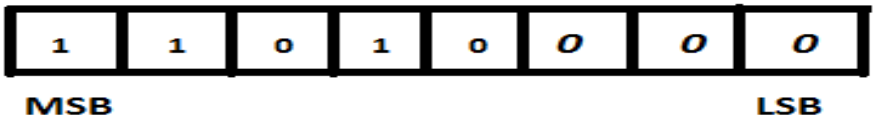
- *WATERMARK IMAGE=*



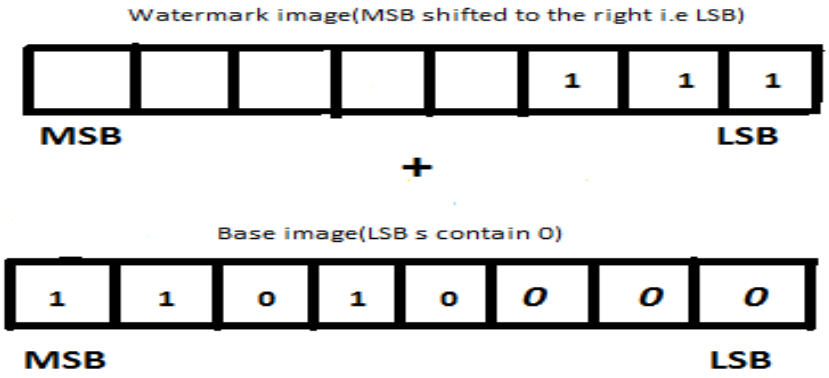
- *BASE IMAGE=*



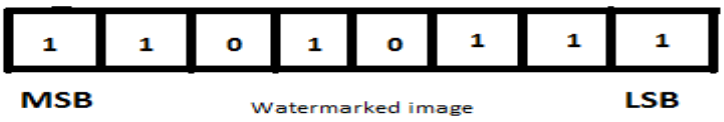
From the base imge, the LSB s(last three bits of base image) are set to 0



Now the base image which has its LSB s are set to 0 and watermark image which has its MSB shifted to its LSB, are added.

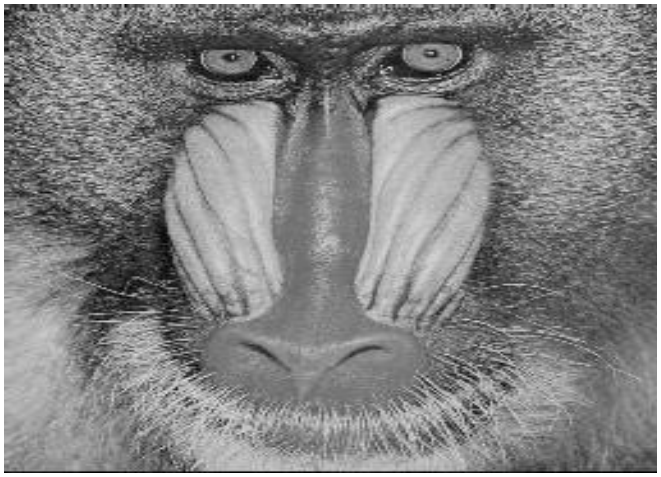


- *FINAL IMAGE=*



So the watermarked image contains its LSB s are the 3 MSB of watermarking image and contain 5 MSB s of the base image.

Base image "A"



Watermarked image "B"

Visible watermarking scheme, both base and watermarked images are combined in the watermarked image.

III. REQUIREMENTS OF DIGITAL WATERMARKING

The requirements of digital watermarking are

A. Transparency- The quality of the embedded watermark should be clear and transparent. The embedded watermark should not reduce the quality of the original image.

B. Robustness- This is one of the requirements of the watermark. There are various types of attack for destroying the watermark such as cropping, compression, scalling etc. The watermark should be design in such a way that, it is invariant to all attacks.

C. Capacity- Capacity describes the maximum amount of data that can be embedded into image, audio, video or text for proper retrieval of watermark during extraction.

IV. CONCLUSION

In this paper we discussed about digital watermarking technique. There are two types of digital watermarking techniques known as visible and invisible watermarking. Watermarking provides owner authentication. If we will use digital watermarking technique in proper way, we can protect data from unauthorized duplication of data.

ACKNOWLEDGMENT

We would like to give sincere gratitude to Dr. Ajit for his guidance to pursue this topic and help us to complete this topic.

REFERENCES

[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 Processing for Multimedia Systems, K..K- Parhi and T. Nishitani, New York, Marcel Dekker, New York, pp. 461-482, 1999.

