INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A COMPARATIVE STUDY ON LSB BASED WATERMARKING AND VSS BASED WATERMARKING

Ankita Sengar[1], Preeti verma[2], Prof. Shreeja Nair[3], Sanjay Sharma[4]

[1]ankitasengar_28@yahoo.co.in
[2]preetiverma@oist.ac.in
[3]shreejanair@oist.ac.in
[4]sanjaysharmaemail@gmail.com
Dept. of CSE, OIST Bhopal (M.P), India

Abstract

In recent years, internet revolution resulted in an explosive growth in multimedia applications. Internet has also made it easier to send the data/image accurate and faster to the destination. But this advantage is also accompanied with the disadvantage of modifying and misusing the valuable information. So In order to transfer the data/image to the intended user at destination without any alterations or modifications, some approach is needed. Digital watermarking is one of the proposed solutions for copyright protection of multimedia data. A watermark is a form of image or text that is hidden in digital data which provides evidence of its authenticity. This paper presents an overview of the various concepts and research work in the field of least significant bit based image watermark authentication. It also consist of comparative analysis of simple LSB based technique and technique using VSS.

Keywords: Visual Cryptography, LSB, RGB images.

1. INTRODUCTION

Rapid development of internet and wireless media has proved to be a boon to the society. Easy access and availability of data at any end of the world from any end has made internet for human like honeypot for bee. Internet has become our solution to every problem whether it is school homework, market research, bill payment or buying anything online. But this honey pot also brings with it many privacy threats. Easy copying and usage can sometime be done in illegal manner. Data can be used against the owner will. Image authentication has been a vital issue since the very starting of digital media. Easy availability and access to internet gives opportunity to share our data with society but it also needs, to stop illegal copying and usage of digital image to secure us from privacy intrusion as well as monetary loss.

Digital watermarking is one such technique that protects digital data from unauthorized usage and provides authenticity verification in case of usage by embedding information (watermark) into the original data in such a way

that it cannot be removed and remains always within the data either visible or invisible. For the watermarking method to be effective, it should be imperceptible and robust to various image processing attacks. [1], [2].Any watermarking system is usually divided into three distinct phases: embedding, attack, and detection [2]. In the embedding phase, a binary watermark is embedded into the host image and the result is a watermarked image. The watermarked image is usually transmitted or stored. If a person makes a modification to the marked image, it is called an attack. Detection (also called extraction) is an algorithm which is applied to the attacked image to extract the watermark from it. For the embedding process the inputs are the watermark, cover object and the secret or the public key. The watermark used can be text, numbers or an image. The resulting final data received is the watermarked data W'. The inputs during the decoding process are the watermark or the original data, the watermarked data and the secret or the public key. The output is the recovered watermark W.

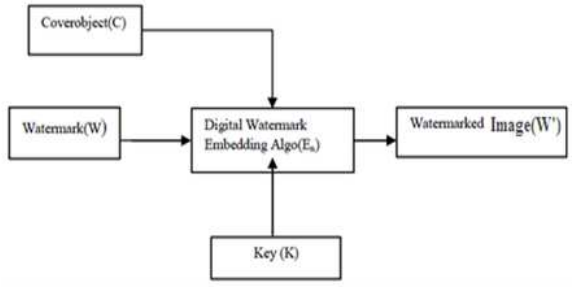


Figure 1.1: General watermarking embedding process

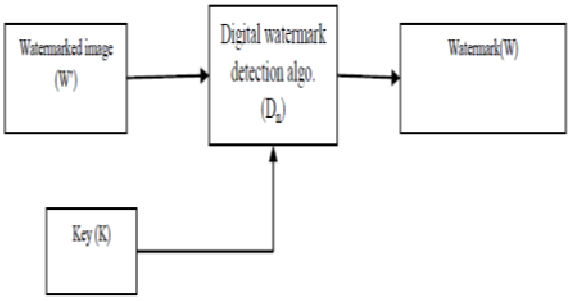


Figure 1.2: General watermarking extraction process

2. Classification of watermarking

Digital watermarking schemes can be classified into various categories based on the basis of domain. Our area of discussion will be covered by two basis of classification:

- According to working domain it can be classified into two categories namely frequency domain and spatial domain.
- According to human perception it can be classified in two categories namely visible and invisible watermarking.

This can further be classified as Robust, Fragile, Semi-fragile and Reversible watermarking.

2.1. Working domain based watermarking

Based on the domain, we are working in for embedding the watermark, watermarking can be classified as spatial domain and frequency domain watermarking. In the spatial domain watermarking, the watermark is embedded by directly modifying the pixel values of the original image. Two techniques under this category are:

a) Least significant bit substitution
b) Correlation based

In frequency domain watermarking the cover object is first transformed in frequency domain and then the watermark is added into the frequency domain. Spatial domain watermarking has the advantage that they can be easily applied to any image; regardless of subsequent processing (whether they survive this processing however is a different matter entirely).
Commonly used frequency-domain transforms are:

- Discrete wavelet transforms (DWT)
- Discrete cosine transforms (DCT)
- Discrete Fourier transforms (DFT)

Based on human perception, watermark algorithms are divided into two categories i.e visible watermarking and invisible watermarking.Visibility is associated with perception of the human eye so that if the watermark is embedded in the data in the way that can be seen without extraction, we call the watermark visible. Examples of visible watermarks are logos that are used in papers and video. On the other hand, an invisible watermarking cannot be seen by human eye. So it is embedded in the data without affecting the content and can be extracted by the owner or the person who has right for that. For example images distributed over the internet and watermarked invisible for copy protection.Additionally, classification is as follows.

- Robust watermark: One of the properties of the digital watermarking is robustness. We call a watermark algorithm robust if it can survive after common signal processing operations such as filtering and lossy compression.
- Fragile watermark: A fragile watermark should be able to be detected after any change in signal and also possible to identify the signal before modification. This kind of watermark is used more for the verification or authenticity of original content.
- Semi-fragile watermark: Semi-fragile watermark is sensitive to some degree of the change to a watermarked image.

3. LSB based watermarking

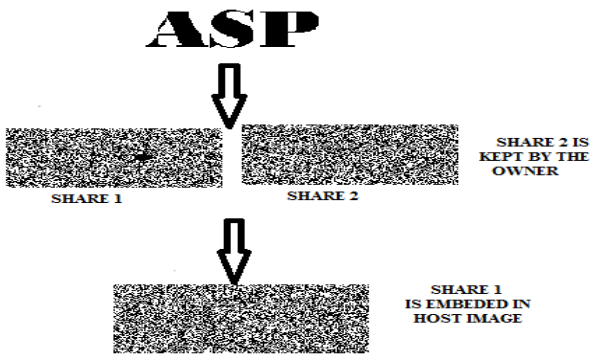
In LSB based watermarking technique, we embed the most significant bits of each pixel of the watermark in the least significant bits' places of the original image. The embedding of the watermark is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits.
In the extraction, we extract the most significant bits of the watermark that we embedded in the original image. The extracted bits do not exactly match with the inserted bits. A correlation measure of both bit vectors can be calculated. If the correlation of extracted bits and inserted bits is above a certain threshold, then the extraction algorithm can decide that the watermark is detected.
In the extraction, we extract the most significant bits of the watermark that we embedded in the original image. The extracted bits do not exactly match with the inserted bits. A correlation measure of both bit vectors can be calculated. If the correlation of extracted bits and inserted bits is above a certain threshold, then the extraction algorithm can decide that the watermark is detected.

4. Visual secret sharing algorithm

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by humans (without computers) [22].Visual cryptography (VC) is basically a secret sharing scheme extended for images. It has the ability to restore a secret without the use of computations.
A white pixel is shared into two identical blocks of sub-pixels. A black pixel is shared into two complementary blocks of sub-pixels. White creating the sheet-images, if the given pixel p in the original image is white, and then the encoder randomly chooses one of the first two columns of table 1. If the given pixel p is black, then the encoder randomly chooses one of the last columns of table 1. Each block has half white and half black sub-pixels,

independent of whether the corresponding pixel in the secret image is black or white. All the pixels in the original image are encrypted similarly using independent random selection of columns.

The result of basic (2, 2) VC scheme are shown in fig.1. When the two sheet-images are stacked together, as in fig.1. (d), the black pixels in the original image remain black and the white pixels become gray. Although, some contrast loss occurs, the decoded image can be clearly identified [7], [9].



4.1 Visual 2-2 secret sharing

5. VSS based LSB watermarking for colour image

Watermarking based on visual cryptography has become an important approach since the watermark embedded even if recovered does not provide any details regarding the original watermark , since it is nothing more than noise and similar to the LSB plane of cover image.

In today's scenario colour image proves to be an upper hand in society. And LSB watermarking applied in binary image proves normally to be more secure than the watermarking applied to colour image. PSNR measured is better in binary the colour image. But from various result analyses it proves that if we use VSS scheme then better PSNR can be achieved by following several approaches of colour image processing. One such approach is to preprocess the colour image on the basis of its RGB components. Normally the color image is represented by the standard 24 bits/pixel or 3 Bytes/pixel. Thus each pixel is represented by 8 bits of each Red, Blue and Green gray scale intensity values. If we use LSB substitution, we can embed the watermark in one of any of these three channels. In many proposed work share1 is embedded throughout the host image LSB bit like a chess board where black is embedded pixel.

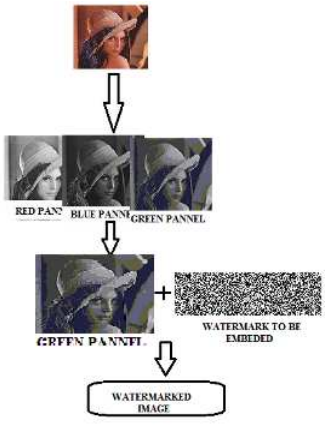


Fig5.1 Watermark Embedding

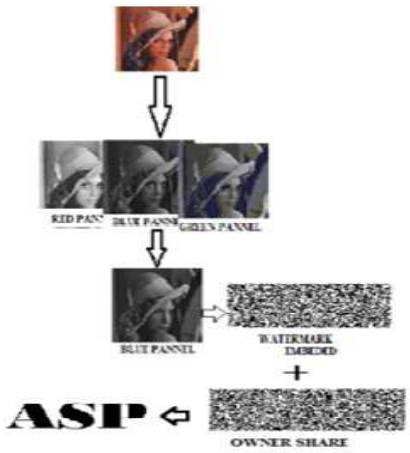


Fig 5.2 Watermark Extraction

Peak signal to noise ratio and normalized cross correlation are generally used as performance measure in image processing. Peak signal to noise ration are used to measure the quality of the watermarked image[10]

The PSNR in decibels is given by:

$$PSNR=10\log_{10}(255/\sqrt{MSE})$$

MEAN SQUARE ERROR

$$MSE = \sum[f(x,y)-F(x,y)]^2 / N^2$$

F(x, y) denotes the original image and F(x, y) denotes the watermarked image. *N X N* is the image size.

Normalized Cross Correlation (NC)

Normalized cross correlation is used to measure the similarity between the original watermark and extracted watermark

IMAGES	IMAGE (LENA IMAGE)	RED PANNEL	GREEN PANNEL	BLUE PANNEL
LSB based watermarking	**50.2096**	71.2471	71.3317	71.5059
LSB cum VSS based watermarking	**53.5063**	74.5909	74.7855	74.8111

Table 1.1 PSNR (dB) analysis

IMAGES	SALT &PEPPER NOISE	ROTATE 5 DEGREE	BLURRING IMAGE	ADDING FILTER [3,3]	ADD SPECKLE NOISE	GAUSSIAN NOISE
LSB based	37.1131	18.2311	27.1202	37.3290	23.3350	21.8178
LSB with Visual cryptography	44.9393	23.2020	33.0872	43.4867	29.7575	28.8578

Table 1.2 PSNR (dB) analyses in present of attacks

5. Conclusion

On the basis of study carried out from the work of different researcher's watermarking shows a vital progress and versatility of techniques. Emphasizing on over area of interest LSB or spatial domain watermarking proves to be easy and adaptable in comparison to transform domain on the sacrifice of instability in case of some type domain attacks. And over study also points that VSS based watermarking proves more efficient and secure then embedding without VSS.

References

V. Venkata Rama Prasad and Rama Kurupati, "Secure Image Watermarking in Frequency Domain using Arnold Scrambling and Filtering," ISSN 0973-6107 Vol.3.Number 2, pp. 23244, 2010.

Chun-Hsien Chou and Kuo-Cheng Liu, "A Perceptually Tuned Watermarking Scheme for Color Images," VOL. 19, NO. 11, Novemember 2010.

S.punitha, S.thomson and N.sivarama "binary watermarking technique based on visual cryptography"; ICCCCt10 @2010 IEEE in 2010

Roopsingh and Rekhagupta." Digital Watermarking with Visual Cryptography in Spatial Domain"; ICAC 2011

B Surekha, Dr. GN Swamy, Dr. K SrinivasaRao, "A Multiple Watermarking Technique for Images based on Visual Cryptography", Vol. 1 ,No. 11, 2010

Ching-Sheng Hsu and Shu-Fen Tu, "Digital Watermarking Scheme with Visual Cryptography", vol.1, 19-21 March, 2008.

Debasish Jena, Sanjay Kumar Jena," A novel Visual Cryptography Scheme," 978-0-7695-3516-6/08 $25.00 © 2008 IEEE.

Yu Wei, YanlingHao and Yushen Li" A Multipurpose Digital Watermarking Algorithm Of ColorImage"; Proceedings ofthe 2009 IEEE International Conference on Mechatronics and Automation.

M. S. Fu and o. C. Au, "Joint VisualCryptographyandWatermarking", In Proceedings of IEEE InternationalConference on Multimedia and Expo, pp. 975-978, 2004.

Chang, C.C., Chaung ,J. C., "An Image Intellectual Property Protection Scheme for Gray-level Images using Visual Secret Sharing Strategy", PatternRecognitionLetters, Vol. 23, pp. 931-941, 2002.

Chang, C. C., Hsiao, J. Y., and Yeh, J. C., "A Color Image Copyright Protection Scheme based on Visual Cryptography and Discrete Cosine Transform".

A Brief Author Biography

Ankita sengar – M.Tech Scholar, B.E RGPV Bhopal, Research Interest: Image processing. Other publications involve IEEE Xplore, Various International and national conference.