ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

An Overview of Digital Watermarking Against Possible Attacks

Shravya Jain [1], Venugopala P S [2], Dr.Sarojadevi H [3], Dr.Niranjan.N.Chiplunkar [4]

PG Scholar, Department of CSE, NMAMIT, Udupi, Karnataka, India[1]

Associate Professor, Department of CSE, NMAMIT, Udupi, Karnataka, India [2]

HOD, Department of CSE, NMAMIT, Udupi, Karnataka, India [3]

Principal, Department of CSE, NMAMIT, Udupi, Karnataka, India[4]

ABSTRACT: Digital Watermarking is an incredibly powerful tool for providing protection to the digital media. Video being the notable form of communication has to be secure while traversing through different medium of communication. There are diverse methods of Video Watermarking but achieving a robust method is a challenge. Analysing Video Watermarking method over different platforms and studying the results of various attacks on them will possibly help in building a robust method of watermarking that can sustain over attacks. In this paper, a spatial method of watermarking implemented over different platform and the results of them over possible attacks are studied. The evaluation parameter gives the robustness of the method.

KEYWORDS: Spatial domain watermarking, LSB, MATLAB, Android, Watermark Attacks

I. INTRODUCTION

Digital media like image, video and audio has this capacity of being reproduced at a different place or time by different people over the internet. The replicas that are produced can be easily distributed. This can lead to severe challenge of authorship, authenticity and security of the digital data. Digital Watermarking proves to be an incredible solution to these problems. It is an ideal way to embed secret bits of information into the digital media which can survive along the digital media [1]. Digital Watermarking is used to assert integrity, authorship and ownership of digital media. Watermark can be ownership identifiers, a serial number or random number sequence, copyright messages, control signals, Information about creator of work, bi-level or gray level images, Transaction dates, text or other digital data formats. Watermarks can be classified based on their characteristics like,

1) Perceptible or imperceptible: based on the visibility of watermark.
2) Blind or non- blind: based on the requirement of watermark information to extract the watermark.
3) Robust, Fragile or semi-robust: Depending on the quality of watermark extracted. Robust if it's clearly extracted. Fragile if not extracted.
4) Spatial domain or Frequency domain: Depends on the domains for watermarking.

Generally Digital watermarking involves three phases in its life cycle which include Embedding, Attack and Extraction phase. Embedding is the process of adding the watermark into the digital media and Extraction process extracts the watermark from the digital media. The major concern is the attack phase that decides the robustness of the watermark. The term attacks include an attempt to remove or detect watermark using unauthorized access [2]. Unauthorized access can be intentional or unintentional. Intentional attack could be hiding executable malicious links with in the host data and unintentional attacks like compression which occurs during the transmission of the host over the internet. Various watermarking techniques are discussed by the researchers with various functionality levels [3]. The original file of digital media is combined with bits of information to create a watermarked digital media.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

Digital watermarking is divided based on the domain of watermarking. In the Spatial domain method [4], watermark is imposed by manipulating the pixel values of digital media. Least Significant Bit (LSB), Patch work, Correlation based and texture block coding are spatial domain watermarking methods. In Frequency domain method, the digital media undergoes transformation before they are watermarked. The Frequency domain watermarking includes Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) [5], Singular Value Decomposition (SVD), Discrete Wavelet Transform (DWT) [6] and Principal Component Analysis (PCA).

Here LSB method of spatial domain watermarking is considered along with the possible attacks on the Watermarked host data. Implementing the same in different platforms is done. The Results of attacks are evaluated using the parameter of evaluation like PSNR.

II. PROPOSED METHOD

The watermarking algorithm must be consistent over transparency, security, Robustness, embedding and retrieval ease [7]. LSB method of watermarking is considered in this approach. This method deals with the direct manipulation of LSB bits of the cover image bit planes. With the fact that the LSB bits of the host image or frame contains very less information of the host data, losing these bits can cause considerable change to the host image or frame. These changes are tolerable since it doesn't cause destruction of host. LSB is implemented in MATLAB as well as in Android Platform.

LSB in MATLAB

In this approach two images involving a gray scale cover image and a gray scale watermark image are considered [2]. The cover image is larger than the watermark image in proportion to 8:1 for 8 bit images. In the embedding process, watermark image pixel bits replace the LSB bits of each pixel of cover image in proportion 8:1.

After embedding all the pixel bits over the cover image using the function 'bitset' and 'bitget' of MATLAB the gray scale watermarked image is formed. The process of watermark bits insertion and extraction in host image is done as shown in Figure 1. This watermarked image will be exposed to several attacks to check the efficiency of algorithm. Watermark is extracted from the watermarked image in the extraction process, which is the reverse of embedding.

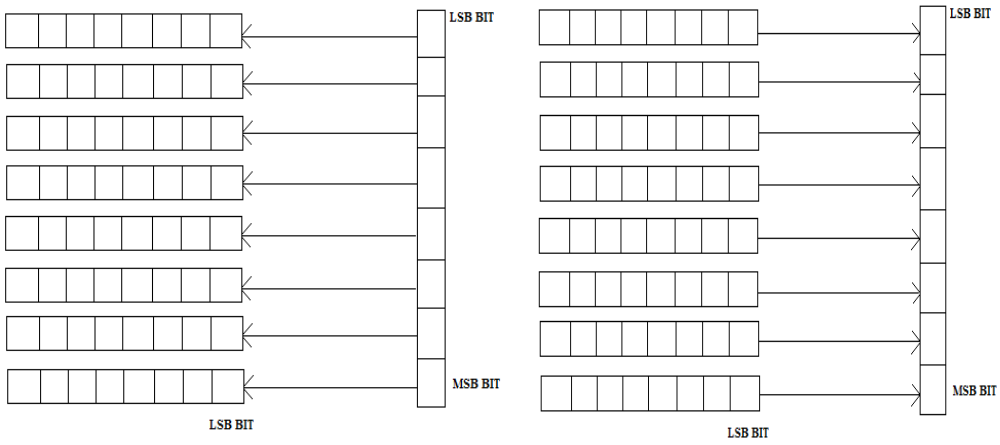


Figure 1: LSB method watermark insertion and extraction

Attacks on watermarked image:

Salt & pepper noise: is the kind of signal processing attack. It presents itself as sparsely occurring white and black pixels. The MATLAB command 'imnoise' is made use of to introduce noises like Gaussian, salt & pepper. This is done using, Imnoise (I, 'salt & pepper', noise density); [8]. Noise density set to default initially.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

Gaussian noise : is statistical noise having a probability density function (PDF) equal to that of the normal distribution, which is also known as the Gaussian distribution. The values that the noise can take on are Gaussian-distributed. The probability density function p of a Gaussian random variable z is given by:

$$p_G(z) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(z-\mu)^2}{2\sigma^2}} \quad (1)$$

Here grey level is represented by z, mean value μ and σ the standard deviation.
MATLAB command for introducing Gaussian noise in the image is A= imnoise(I,' gaussian', M,V); [8] where M the mean value set to 'zero' by default, V variance 0.01 set by default.

Rotation: The geometric attack aims changing dimension of the image to a specified angle. Rotate is the standard transformation performed on images along with cropping. MATLAB provides a feature 'imrotate' that is used to rotate the image. B = imrotate(A, angle); [8] an image A is rotated in counter clockwise direction around its centre point by angle degrees.

LSB in Android

The LSB implementation on the Video frame is considered here. This method is implemented in Android using the emulator and the mobile device [9]. Video file considered comprises of colored video frames. Each Pixel consists of the Red, Green and Blue color channels. Since the R,G and B are of 8 bits, the LSB bits of them is replaced by the watermark binary string bits that is taken as input. As shown in Figure 2. the watermark bits will be inserted into the color components of the video frame.

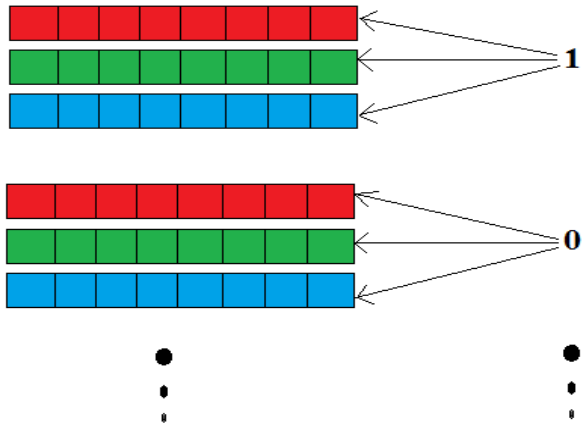


Figure 2: Watermark insertion on RGB components LSB bits

Extraction is the reverse process. The R, G, B components are extracted and the LSB bits of them are considered. Once all the bits are obtained the watermark is detected.

Attacks on the watermarked frame

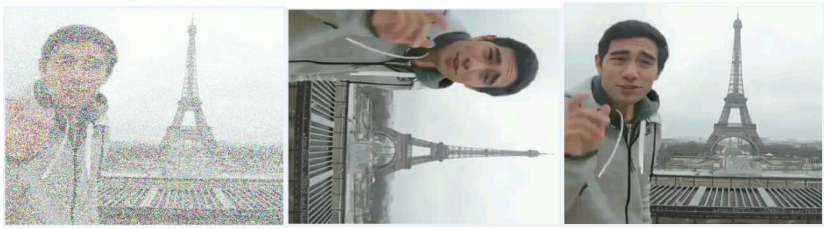
In this work three kinds of attacks are introduced into the watermarked frame which includes noise, rotation and crop attack as shown in Figure 3. In noise attack each and every pixel values of watermarked frame are altered by generating random color and inserting it to each color pixels. This generates disturbance in the frame resulting in noise. Rotation attack involves changing the dimension of the frame to specified angle. In this attack the watermarked frame is rotated by an angle of 90 degree. Cropping attack changes the aspect ratio of the watermarked frame. When the cropping removes the pixel rows and columns containing watermark bit details, the watermark information is lost. Both Rotation and cropping attack are kinds of geometric attack.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016



(a) (b) (c)

Figure3: Watermarked frame with noise attack (a) watermarked frame with rotation attack (b) watermarked frame with crop attack (c)

III. EVALUATION PARAMETERS

MSE: The goal of Mean squared error measure is to compare two images by providing a quantitative score that describes the degree of similarity or, conversely, the level of error between them.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \qquad (2)$$

Where I is a noise free image and its noisy approximation is K. The number of rows m and columns n of the input images.

PSNR: Peak Signal to noise Ratio is an approximation to human perception of reconstruction quality. The reconstruction is of higher quality if PSNR value is high, in some cases it may not.

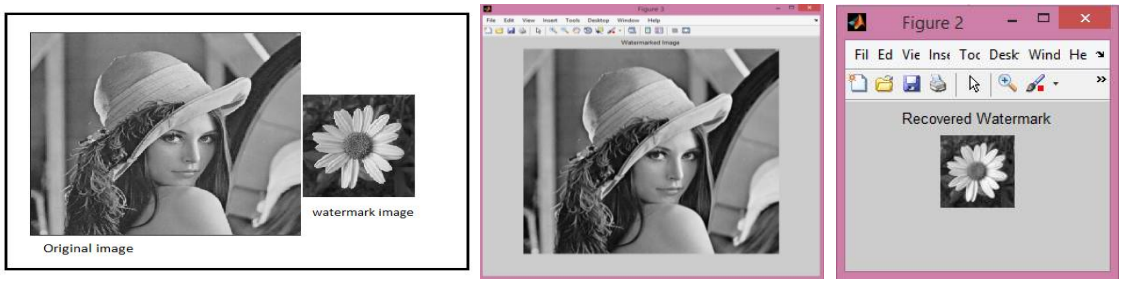
$$PSNR = 10\ log_{10}\left(\frac{R^2}{MSE}\right) \qquad (3)$$

Maximum fluctuation in input data type is 'R'. For example R is 255 if the input image has 8-bit unsigned integer data type, R is 1 for double-precision floating-point data type.

IV. RESULTS

In MATLAB, the input to the LSB based watermarking method is two gray scale images. The host image and the watermark image as shown in Figure 4 (a). The LSB bits of cover image are replaced with the bits of the watermark image. This generates the watermarked image is shown in Figure 4 (b). The recovered watermark is as in Figure 4 (c). Watermark is extracted without distortion.

The graphs in Figure 5 represent the outcome of possible attacks on the watermarked image. Salt and pepper noise increases with the increase in noise density which further increases the noise in the watermarked image as shown in Figure 5 (a). The Gaussian noise varies with the mean value. Figure 5 (b) represents the perception level on the extracted watermark against the original watermark given as input. Figure 5 (c) shows the result of rotation attack, giving the PSNR value of extracted watermark.



(a) (b) (c)

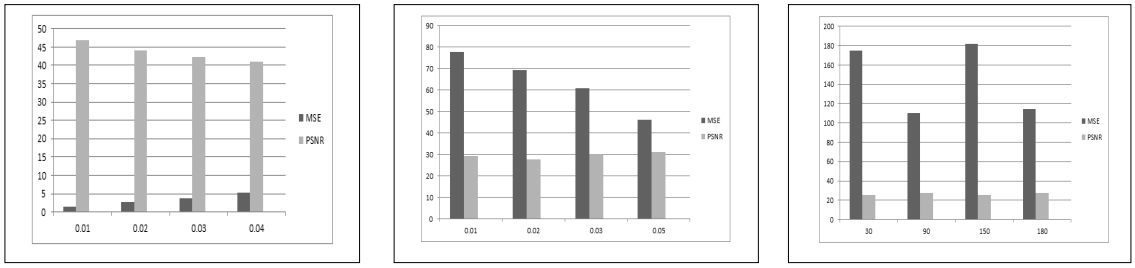
Figure 4: Original host and watermark image (a) watermarked image (b) extracted watermark (c)

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

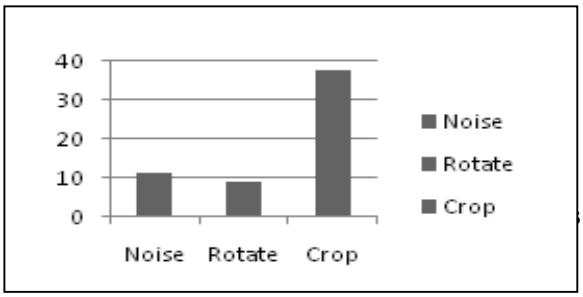
Vol. 5, Special Issue 9, May 2016



(a) (b) (c)

Figure 5: PSNR values for salt and pepper noise (a) Gaussian (b) rotation (c)

The LSB watermarking on video frames is considered in this paper. The graph in Figure 6 represents the Perception level of the attacked watermark image against the watermark image. Since the noise distorts the R, G, B components of the frame completely, the watermark bits hidden in the LSBs of them is also disturbed. The result is improper extraction of the watermark bits. Rotating the frame changes the position of extraction, leading to improper bit extraction. This also distorts the watermark information. Cropping the region in video frame which comprise of watermark information can make the LSB method of watermarking fragile.



This paper is a study on a spatial domain method of watermarking on different platforms. Least Significant Bit method of invisible watermarking is a simple to implement method of image and video frame watermarking. The digital image and frame is represented as matrix in MATLAB and in Android it is in the form of Bitmap. The watermarked image in MATLAB is sensitive to the attacks like noise and geometric attack. This technique gives a Semi-Robust watermark which is perceptible unless the attack is dense. In Android, the watermark is sensitive to the attacks, if the target of attacks tends to be the watermarked bits. This method has the advantage of ease of implementation but also tends to be attacked easily when compared to other methods of watermarking.

REFERENCES

[1] Raghavendra K and Chetan K.R, "A Blind and Robust Watermarking Scheme with Scrambled Watermark for Video Authentication", Internet Multimedia Services Architecture and Applications (IMSAA), IEEE, 2009.
[2]Venugopala P S, Shravya jain, Sarojadevi H, Niranjan.N.Chiplunkar, " Study of Possible Attacks on Image and Video Watermark", 3rd International Conference on Computing for Sustainable Global Development, IEEE, INDIACom-2016.
[3] BorkoFurht and DarkoKirovski, "Multimedia Watermarking Techniques and Applications", Auerbach Publications, 2006.
[4] Prabhishek Singh, R S Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology (IJEIT), March 2013.
[5] Vandana Thakur and Monjulsaikia, "Hiding Secret Image in Video", International Conference on Intelligent Systems and Signal Processing (ISSP), IEEE, 2013.
[6] JianZhong Li, Yinghui Zhu, Ping Zhong and CaiGuo, "Robust Wavelet-Based Watermarking Scheme For Video Copyright Protection", 7th International Congress on Image and Signal Processing, IEEE, 2014.
[7] SanthoshiBhatt, ArghyaRay, AvishakeGhosh and AnanyaRay, "Image Steganography and Visible Watermarking using LSB Extraction Technique", IEEESponsered 9th International Conference on Intelligent Systems and Control (ISCO), 2015.
[8] MATLAB version 7.14.0.739, The MathWorks Inc., 2012.
[9] Venugopala P S, Ankitha.A.Nayak, Sarojadevi H, Niranjan.N.Chiplunkar, "Video Watermarking for Android Mobile Devices", 3rd International Conference on Computing for Sustainable Global Development, IEEE, INDIACom-2016.