Volume 5, Issue 11, November 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on Digital Watermarking Using LSB

Maninder Kaur, Nirvair Neeru
Department of Computer Engineering, Punjabi University,
Punjab, India

Abstract – The rapid growth in the area of networking made the exchange of data easy over internet but with this the risk of tampering of data, illegal copying and other security issues also increases. This arise needs of providing security to data. Cryptography, digital watermarking and steganography are all methods to secure data transmitting over internet. In this paper digital watermarking and some of the recent techniques based on Least Significant Bit (LSB) watermarking which are used to protect data against various attacks are discussed.

Keywords – Least Significant Bit, MSE, PSNR

I. INTRODUCTION

Digital watermarking is a technique of embedding or hiding information called watermark (also known as tag or label or digital signature) within the digital file (known host) without noticeably altering the file itself. Digital watermarking provides intellectual property right and tamper detection of data.

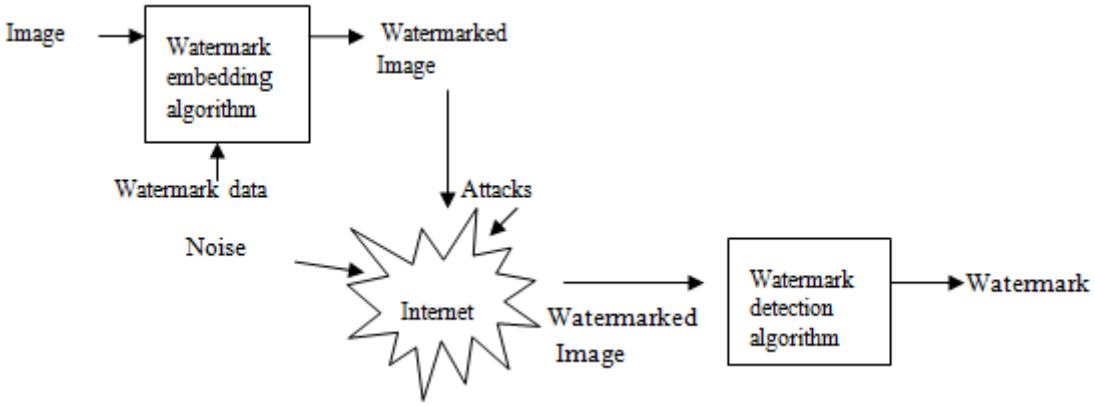

Fig. 1 Procedure of digital watermarking [4]

There are two types of watermarks one is visible watermark and other is invisible watermark. Visible watermark is an opaque or semitransparent sub image placed on the top of host image (original image). Example of visible watermark is logos used by various companies and television channels.

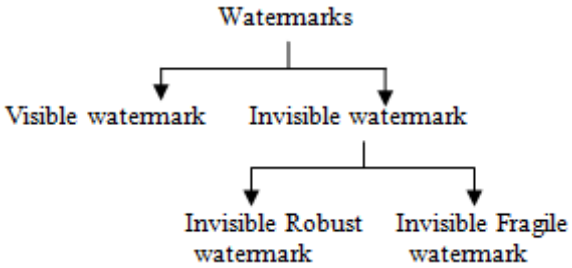

Fig. 2 Types of digital watermark

Invisible watermark cannot be perceived by human sensory system [1]. Invisible watermark can be categorized as invisible robust watermark and invisible fragile watermark. Invisible robust watermark are not sensitive to attacks (that is watermark cannot be removed or destroyed by any attack) like removal attack, modification attack and is generally used for copy right protection. Invisible fragile watermark are sensitive to the attacks, any small change in image can destroy the watermark. It is used for tamper detection [3]. The various techniques of digital watermarking are categorized into two domains:

- Spatial domain
- Frequency domain.

In the spatial domain watermark can be inserted into image by changing the pixel values of an image directly [8].

Frequency domain is also known as transforming domain and in this domain watermark first the image is transformed into spectral coefficients and then watermark is applied to spectral coefficients [8].

II. RELATED WORK

In this section of this review paper the previous work which has been done on the Least Significant Bit based digital watermarking is described. In LSB method watermark is embedded in the least significant bit of a pixel as it is considered that the LSB of a pixel of image.

Max Sobell [7] presents a robust and imperceptible Least Significant Bit digital watermarking algorithm. In this algorithm 7 – bit ASCII codes for encoding are used and a watermark is inserted by overwriting the least significant bit of the pixels of an original image with the bit of watermark image.

R. Aarthi et. al. [5] proposed a modified LSB embedding technique. This technique satisfies the reversibility feature which is not supported by simple LSB technique. In this third and fourth least significant bit is used for embedding data and a matrix is created whose dimension is equal to watermarked image and its values are obtained by XORing every pixel of original image and watermarked image. This matrix is used during extraction process of digital watermarking.

Puneet Kr Sharma et. al. [4] proposed a least significant bit algorithm in which embedded watermark is spreads over full image to avoid any damage to watermark by attackers.

Anum Javeed Zargar [2] proposed a technique in which he replaces the least significant bit of pixels of grey scale image with the most significant bits of watermark image. Before embedding the watermark both original and watermark images are cropped according to desired pixels.

Manoj Nagar et. al. [6] proposed a digital watermarking technique for detecting tampering in colored image. According to this technique watermark is generated with the help of Discrete Cosine Transform (DCT) or Discrete Fourier Transform (DFT) coefficient and then generated watermark is embedded in least significant bits of pixels of image.

III. EXISTING TECHNIQUES

In this section of paper a few of the existing techniques which are used now days to protect data are explained.

A. Traditional Least Significant Bit digital watermarking

In the basic least significant bit digital watermarking technique the image pixel's decimal values are first converted into corresponding binary values and then the least significant bit value of eight bit pixel of an image (host image) is overwritten with the watermark bit value [5]. For example, if a pixel value 24 is represented by 00011000 in binary and a watermark value is 100.

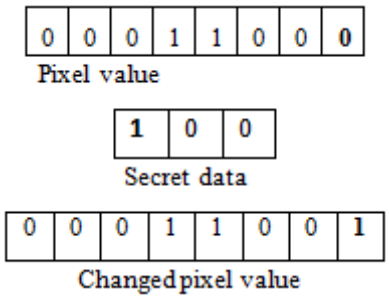

Fig. 3 Example of traditional LSB watermarking [11]

After applying Least Significant Bit technique the LSB of pixel value changed to 1 from 0 thus changing value 24 into 25. This difference of value 1 is so negligible that human eyes are not able to identify it.

Original Image Watermarked Image

Fig. 4 Example of LSB watermarking

Advantage of LSB technique is that it is simple, requires less computations and also changes occur in host image after watermarking are negligible. But disadvantage of this technique is that watermark can be easily destroyed by changing bits. And also watermark can be destroyed by noise introduced during transmission of image.

B. Inverse of Least Significant Bit

In inverse least significant bit technique value inverse to the value of least significant bit of pixel is inserted into the second LSB bit of pixel.

Amit Singh et. al. [10] presents a technique of digital watermarking according to which first watermark text binary bit is inserted in least significant bit of pixel of a host image and then inverse of least significant bit is inserted into second least significant bit of pixel of image. If first LSB is 1 then the second LSB will be 0 and vice versa. Similarly, in extraction phase first step is to change second LSB of pixel of an image according to the first LSB. If first LSB is 0 then change second LSB to 0 also and vice versa. Example of this proposed technique is:

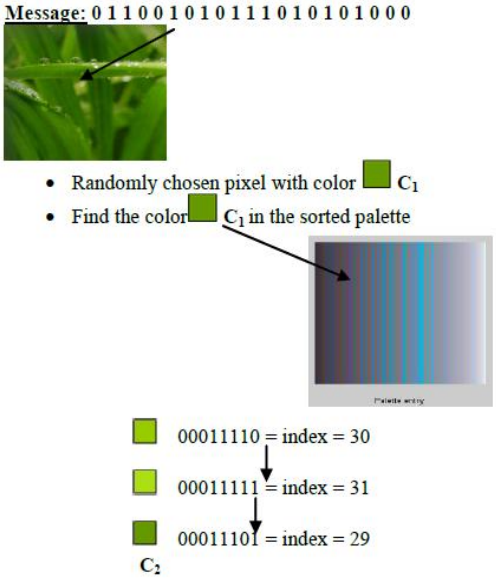

Fig. 5 Inverse LSB [10]

This technique provides better authenticity than simple LSB method because of use of second LSB in addition to first LSB. Also it is not very complicated.

C. Detection of tampering in color image

Manoj Nagar et. al.[6] proposed a technique for tampering detection in an image by using Least Significant Bit method which helps to solve the problem of integrity and authentication of an image. According to this method there are two stages, one is self embedding stage and other is authentication stage. In embedding stage, first step is to divide a colored image into three color stacks of red, green and blue color and then divide image into blocks of 8*8 or 4*4 or 2*2. After that take DFT or DCT without using LSB and generates watermark based on following equation:-

Wk = 0 if transformation coefficient is even

Wk = 1 if transformation coefficient is odd.

Then apply special lookup table and marking key and embed watermark into least significant bit of pixels of image. Last step after embedding watermark is to combine all blocks and color components of an image to form a complete image. In authentication and localization stage, again division of image into color components and blocks of 8*8 or 4*4 or 2*2 is done. Watermark is extracted based on following equation:-

Wk = 0 if transformation coefficient is even

Wk = 1 if transformation coefficient is odd.

After applying special lookup table and marking key extracted watermark is compared with LSB of original image. If both are equal then image is authentic but if both are unequal then image is unauthentic and tampered blocks are highlighted. At last all blocks and color components are combined to complete an image [6].

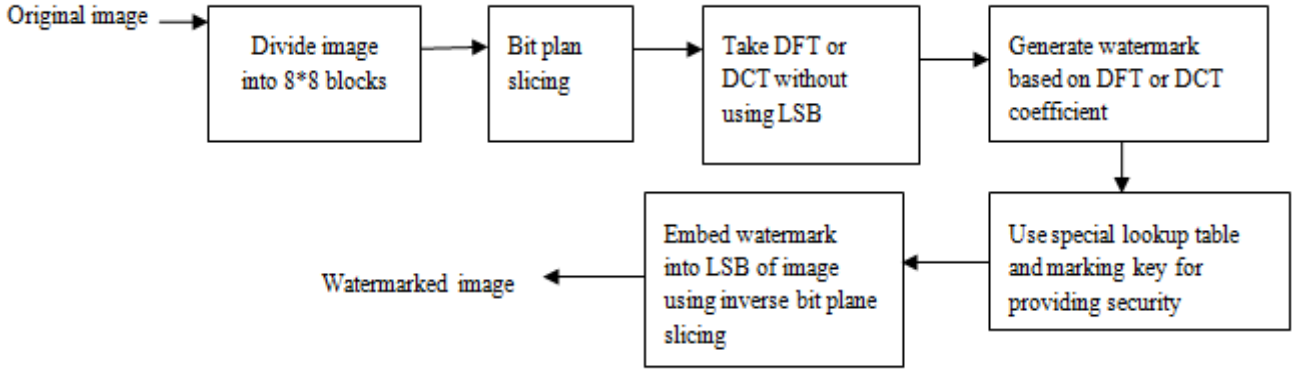

Fig. 6 Self embedding stages [6]

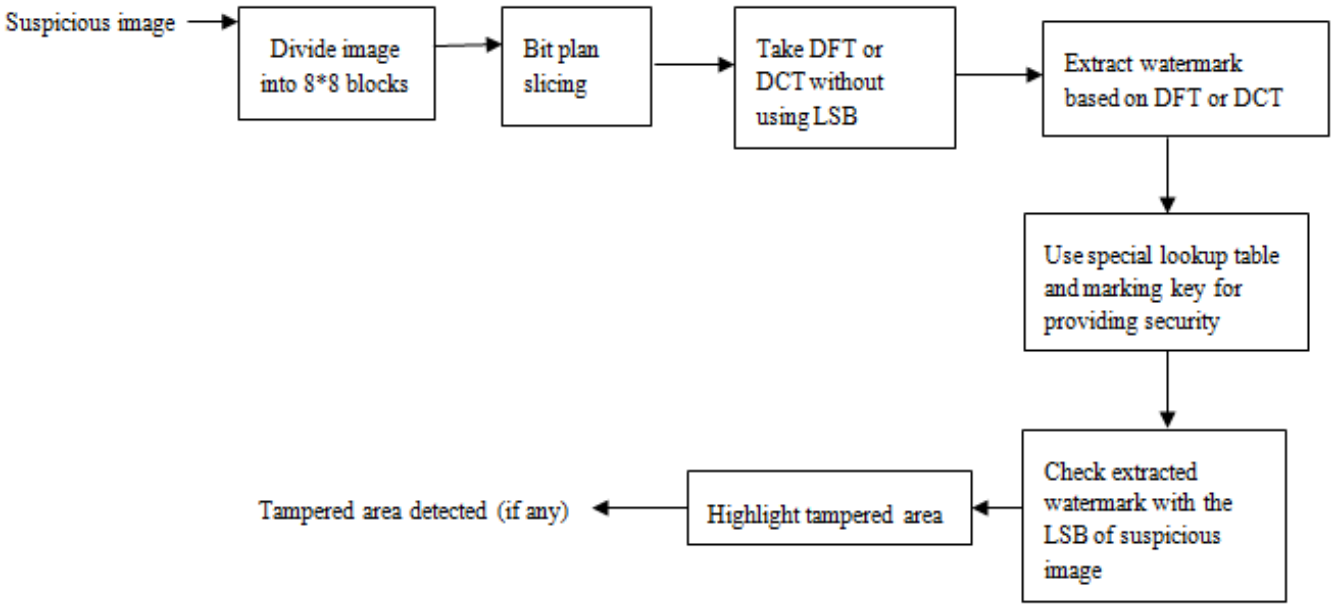

Fig. 7 Authentication and localization stage [6]

Positive points of this technique are that it is highly efficient. Second one is that it highlights the tampered location of image which makes detection of exact location of tampering easy for users.

IV. PERFORMANCE PARAMETERS

The performance of the various techniques of digital watermarking is evaluated by Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). These parameters evaluate the quality of the watermarked image obtained after applying digital watermarking.

Mean Square Error definition – Mean Square Error (MSE) is measured as average of square of errors that is difference between watermarked image and original image [9].

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

Where m and n are number of row and number of columns respectively and $\text{I}(i,j)$ is an original image and $\text{K}(i,j)$ is watermarked image.

Peak Signal to Noise Ratio (PSNR) – Peak Signal to Noise Ratio defined as ratio between maximum power of signal and power of corrupting noise. Generally PSNR is defined via MSE which for m*n images I and K where one of images is considered as noisy approximation of other [9].

$$\text{PSNR} = 10 * \log_{10} \left(\frac{Max^2}{MSE} \right)$$

$$= 20 * \log_{10} \left(\frac{Max}{\sqrt{MSE}} \right)$$

Max is maximum possible value of pixel of image. If pixels are represented by using 8 bits per pixel then Max is 255 (Max = 2^8 - 1 = 255) [9]. Typical values of PSNR are between 30 dB and 40 dB for 8 bit data and between 60 dB and 80 dB for 16 bit data. PSNR is used to measure amount of visual quality degradation between original image and watermarked image.

Some other parameters which can be used to measure the performance of different digital watermarking technique are – maximum difference (MD), mean absolute difference (AD), normalization on mean absolute difference (NAD), LP standard and Laplace mean square difference [12].

V. CONCLUSION

This paper provides a review of digital watermarking and some of the digital watermarking techniques based on simple and less computational Least Significant Bit (LSB) method. From the discussion in the different section of this paper it is concluded that traditional LSB method is simple and less computational but it provides less security than other LSB based digital watermarking techniques because if attacker identify watermark data than he will easily destroy watermark. Whereas inverse LSB techniques is also simple like traditional least significant bit technique but it provides more authenticity. Third discussed technique of tamper detection tells the exact location in an image where any kind of tampering is performed by an attacker thus providing high efficiency and providing more authentication than inverse LSB and traditional least significant bit method. It also provides more security than other two techniques as watermark is generated using DCT or DFT technique so it's difficult to identify the watermark.

REFRENCES

[1] Mohan Durvey, Devshri Satyarthi, "A review paper on digital watermarking", *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, Volume 3, Issue 4, July-August 2014.

[2] Anum Javeed Zargar,"Digital image watermarking using LSB technique", *International Journal of Science & Engineering Research*, Volume 5, Issue 7, July-2014.

[3] Keshav S Rawat and Dheerendra S Tomar,"Digital watermarking schemes for authorization against copying or piracy of color images", *Indian Journal of Computer Science and Engineering,* Vol. 1 No. 4 295-300.

[4] Puneet Kr Sharma and Rajni, "Analysis of image watermarking using Least Significant Bit algorithm", *International Journal of Information Sciences and Techniques (IJIST)*, Vol. 2, No.4, July 2012.

[5] R. Aarthi, V.Jaganya and S. Poonkuntran,"Modified LSB watermarking for image authentication", *International Journal of Computer & Communication Technology (IJCCT)* ISSN (ONLINE):2231–0371 ISSN (PRINT):0975- 7449,Vol.-3, Iss - 3,2012.

[6] Manoj Nagar, Pinky Brahmbhatt and Dr. M. Sarada Devi, "Detection of tampering in color image", *Internationl Research Journal of Engineering and Technology (IRJET),* Volume: 02, Issue: 02, May-2015.

[7] Max Sobell,"LSB digital watermarking", CPE 462, final project.

[8] Y.Shantikumar Singh, B. Pushpa Devi and Kh. Manlem Singh,"A review of different techniques on digital image watermarking scheme", *International Journal of Engineering Research*, Volume No. 2, Issue No3, pp: 193 – 199, 01 July 2013.

[9] Abdullah Bamatraf, Rosziati Ibrahim and Mohd. Najib Mohd. Salleh,"A new digital watermarking algorithm using combination of Least Significant Bit (LSB) and inverse bit", *Journal of Computing*, Volume 3, Issue 4, April 2011, ISSN 2151 - 9617.

[10] Amit Singh, Susheel Jain and Anurag Jain,"Digital watermarking method using replacement of second least significant bit (LSB) with inverse of LSB", *International Journal of Emerging Technology and Advanced Engineering,* Volume 3, Issue 2, February 2013.

[11] Rajni Verma and Archana Tiwari,"Copyright protection for watermark image using LSB algorithm in colored image", *Advance in Electronic and Electric Engineering*, ISSN 2231 – 1297, Volume 4, Number 5 (2014) pp. 499-506.

[12] Zhu Yuefeng, Lin Li,"Digital image watermarking algorithms based on dual transform domain and self - recovery", *International Journal on Smart Sensing And Intelligent Systems*, Vol. 8, No. 1, March 2015.

