Ibn Al-Haitham Journal for Pure and Applied science https://doi.org/ 10.30526/2017.IHSCICONF.1790

Securing digital documents using digital watermarking

Awad Kadhim Hammoud
Awad_kh2017@yahoo.com
Hatem Nahi Mohaisen
Qusay Samir Shaker
Ministry of Science and Technology/Information Technology Directorate.

Abstract

The intellectual property of digital documents has been protected by using many methods of digital watermarking. Digital documents have been so much of advantages over print documents. Digital documents are less expensive and easy to store, transport, and searched compared to traditional print documents. But it has its owner limitation too. A simple image editor can be used to modify and make a forged document. Digital documents can be tampered easily. In order to utilize the whole benefits of digital document, these limitations have to overcome these limitations by embedding some text, logo sequence that identifies the owner of the document.

In this research LSB technique has been used to embedding Digital watermarking, the proposed method consists of two major part: the embedding part and extraction part. The BMP picture type has been used in embedding process for accuracy and uncompressed image, and it is the best type in embedding process. This technique used to discover the genuine documentThe experiments show the proposed technique has 100% accuracy in authenticating the genuine document and Multimedia content security.

Keywords: Multimedia content security, Digital watermark, LSB, Digital image, Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE).

 https://doi.org/ 10.30526/2017.IHSCICONF.1790

1. Introduction

The rapid development of technologies has led to the significant increase of digital information, specially multimedia such as image audio, video and text. The advances in these technologies have led to the easy in which, it is possible to illegally share, distribute and copy intellectual property (IP).

Digital watermarking is the process of embedding relevant ownership information (such as logo, fingerprint and serial number), into a media in order to protect the ownership of different media format. This technique can be applied to different media type. For this purpose of copyright protection and ownership identification, robust watermarking schemes are mainly used as they can tolerate a host of signal processing attacks that can be both unintentional and intentional. Figure (1), shows the techniques and mechanism which are being used in security system, special focus on information hiding techniques.

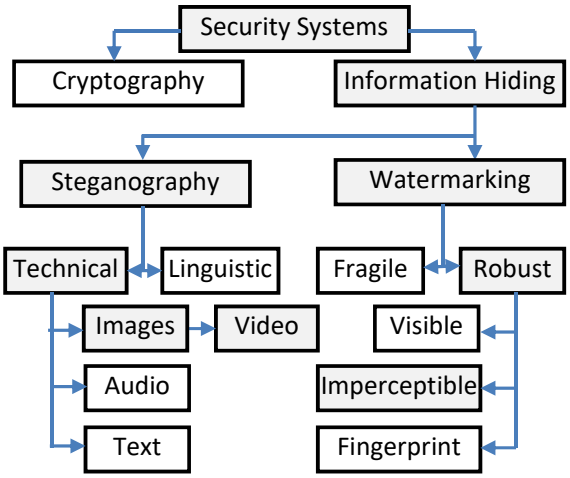

Figure (1): The different disciplines of security system.

Many papers are published [2-11] to promoting mechanisms and algorithms embedded secret data into cover media such as text, image, audio and video.

2. General Watermarking Framework

Mathematically, watermark concealing can be putting in Equation (1).

$$\beta' = \beta + \alpha\ \beta m \quad \ldots\ldots (1)$$

Equation (1) shows watermark concealing operations. The original image β, watermark βm input to the system, α is a degree factor and a K is the secret key of process. The image β' is the output of the watermarking scheme. The concealing process may be message inside image, or image inside image, as shown in figure (2).

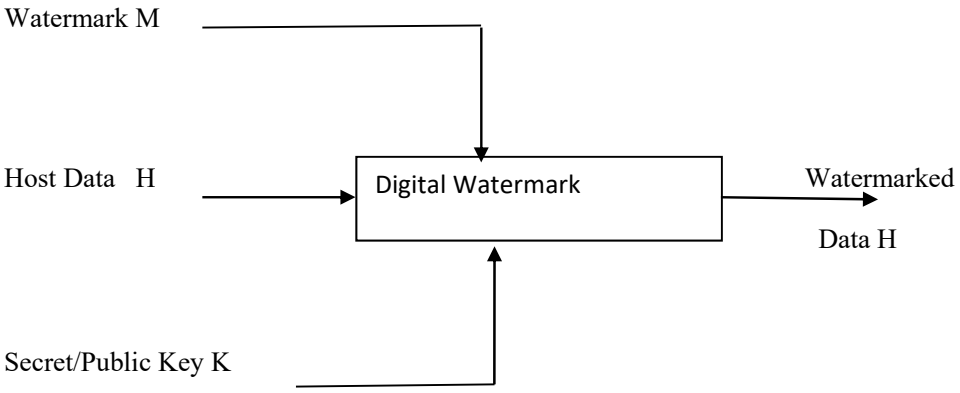

Figure (2): Generic digital watermarking Scheme.

There are two ways or more can be extracted later the embedded watermark, either by using the original image to compare and find out the watermarking (non-blind watermark) or using correlation measure to detect the watermarking (blind watermarking).

For extraction of the concealing watermarking in non-blind watermarking, can simply compassing by applying Equation (2), the original image can be simply obtained by subtract from the watermarked, then divided it by the gain factor.

$Bm = (\beta' - \beta)/ \alpha$ …..……(2)

For extraction of the blind watermarking, can simply compassing by similarity measure as shown in figure (3).

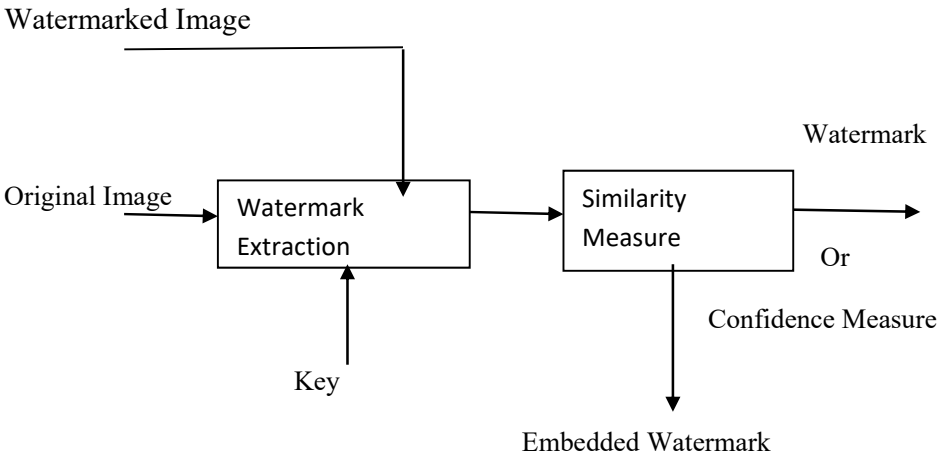

Figure (3): Watermarking extraction and discovery.

Many techniques can be used to assessing the coinciding among the genuine and extracted watermarking. Frequently used similarity admeasurements are the correlation-based method. Equation (3), is broadly used as a watermarking similarity admeasurements. In general, the extracted watermarking will not be similar to the genuine watermarking. Equation (3) computes the identically between the βm and β'm as follows:

$sim(\beta m, \beta' m) = (\beta m * \beta' m) / \sqrt{(\beta m * \beta' m)}$ ……(3)

To decision whether βm and β'm are match, one may compute, sim (βm, β'm)

> T, Where T a Threshold.

Watermark applications:

Many fields of applications may be used digital watermarking:

1- Owner identification.
2- Copyright conservation.
3- Broadcast monitoring (Tv and radio news is also monitoring by watermarking).
4- Medical implementation.
5- Fingerprinting and digital signature.
6- Information authentication.
7- Proprietor identification.

3. Watermarking classification

Digital watermarking techniques can be classified into four types:

1- Text.
2- Image.
3- Video.
4- Audio.

4. The Proposed System

The implementation of using watermark to secret digital document system consist of two major parts: hiding part as shown in Algorithm1and extraction part shown in Algorithm2. To start up with hiding part, it is hiding the specific watermark into digital document which will represented by image, in such a way that the hidden watermark is imperceptible to human eye. The hidden technique should be kept the perceptible information of image without changed which must have founded by extraction module. Embedding the watermark requires compatibility of the dimension of the watermark image. The Evaluation part is expressed in algorithm 3. The bmp format will be used in all images for easy used and uncompressed format. the system has been implemented by using MATLAB software version 10.

Algorithm1: Hide of Watermark.

1- Prepare the original image and watermark for reading.
2- Convert the information of watermark into binary, replace it into ASCII.
3- Measure the size of information (in bits). Determine the number of height and width for both image and watermark.
4- Hide bit by bit of watermark into least significant bit (LSB) of each byte of image.
5- Repeat step 5 until complete hiding of all data of watermark.
6- Save the watermarked image (document) in new file named(lsb_watermarked.bmp)
7- End.

Algorithm2: Extract of Watermark.

1- Read watermarked image.
2- Using LSB method to extract the watermark from image.

 https://doi.org/ 10.30526/2017.IHSCICONF.1790

3- Compare between the original watermark and extracted watermark to decide if watermark is not chanced to prove the original document.
4- End.

Algorithm 3: Evaluation

1- Read both the original image and watermarked image.
2- Calculate MSE, PSNR for both images.
3- Find histograms for both original image and watermarked image.
4- End.

5. The Experimental results

When running the system, the input to system are: the original document represented by image named (Jellyfish.bmp), figure (1), and the watermark named (awad.bmp), figure (2). the output of the system is watermarked image named (lsb_watermarked.bmp), as shown in figure (3). The authentication has been done thru calculate the difference between original image and watermarked image. Calculate the MSE and PSNR as shown in table 1). The value of PSNR= 55.2713, that mean matching between original image and watermarked image. The watermark has been extracted from watermarked image as shown in figure (4). The histogram of original image and the histogram of watermarked are draw to show there is no differences between original image and the watermarked image, figure (5) (a) and (b).

Figure (1): The original image.

Ibn Al-Haitham Journal for Pure and Applied science https://doi.org/ 10.30526/2017.IHSCICONF.1790

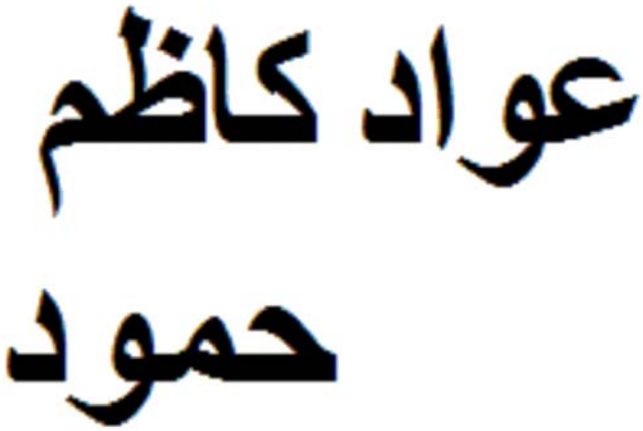

Figure (2): the watermark.

Figure (3): The watermarked image.

Figure (4): The extracted watermark

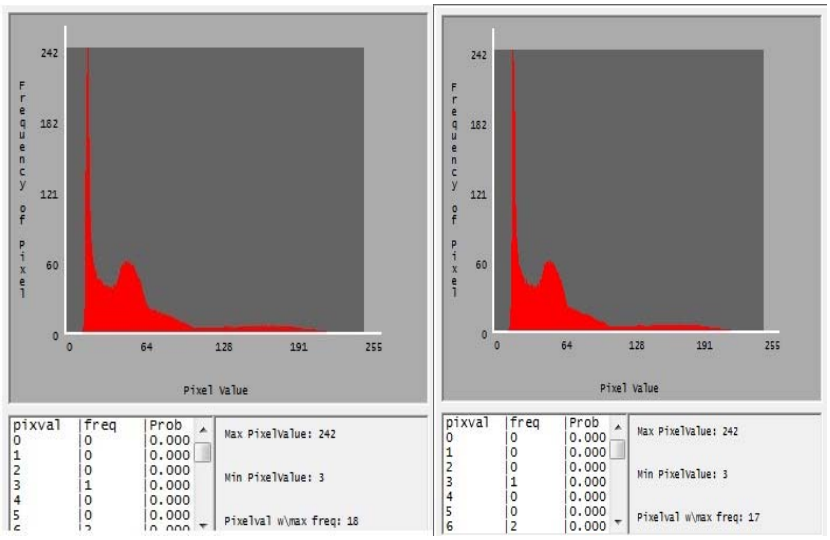

Figure (5): (a) Histogram for original image & (b) Histogram for watermarked image.

Table (1): The value of MSE and PSNR.

Image name	MSE	PSNR
Jellyfish.bmp Lsb_watermarked.bmp	0.1932	55.2713

6. Conclusions

1- This paper presented new method to protect the copyright of digital media by using digital watermark.
2- Digital watermarking technique has been used to identify the owner of the document.
3- Least Significant Bit (LSB), is a good way to implement the embedding of watermark.
4- The degree of comparison of matching between the original document and watermarked image is very good. (PSNR > 50).
5- The extraction of embedded digital watermark is very well.

References

[1]. Alaa H. Al_Hammami, Steganography and watermark. University Bookshop. 2007.
[2]. C. S. Lu" Steganography and Digital Watermarking for Protection of Intellectual Property. Idea Group Publishing, 2005.
[3]. Ensaf Hussein, Mohamed A. Belal,. Digital watermarking techniques, Applications and Attacks Applied to Digital Media. International journal of communication network security,. 1, 7. 2012
[4]. Firas Adel Seddek ,Image Steganography Using Least Significant Bit Insertion Method. Msc. Thesis, College of Science of Al_Nahrain University. 2001

[5]. Hatem Nahi Mohaisen, Secure Data Hiding Technique using Steganography and Watermark. Msc. Thesis, College of Science Baghdad University. 2016
[6]. Methaq Talib Gaata, Developing Metrics Evaluator for Digital Image Watermarking Techniques. PhD Thesis, University of Babelon. 2011.
[7]. Shivani Khosla, Paramjeet Kaur. Secure Data Hiding Technique Using Video Steganography and Watermarking. International Journal of Computer Applications, 95,. 20, 2014
[8]. Sin-Joo Lee, Sung-Hwan Jung, A Survey of Watermarking Techniques Applied to Multimedia. ISIE publishing. 2001.
[9]. V. Anitha ,R. Leela Velusamy, Authentication of digital Documents Using Secret Key Biometric Watermarking. International journal of communication network security, 1, 4. 2012.
[10]. Wafaa Hassan Alwan. Dynamic Least Significant Bit Technique for Video Steganography. Journal of Kerbala University. 11. 4. 2013