A New Digital Watermarking Algorithm Based on Image Comparison Technique

Prof. Dr. Abdul MonemS.Rahma[1], Assist.Prof.Dr. Matheel E.Abdulmunim[2], Rana J.S. Al-Janabi[3]

Abstract – *Recently, the Rapid growth of Internet and the revolution of digital multimedia technology have brought important changes in people's lives. It has made it possible to share multimedia fast and easily. The digital information sharing have also created the problem of copyright protection for original data. Watermarking are the proposed solutions to protect the copyright and to prove the ownership of data. In this research, new watermarking algorithm is created. The watermark is embedded into two stages. The first one is by taking the secret key that consists of eight number from (0..7) each number in it determines the particular bit position in specific pixel of cover image. If that bit is similar to the bit in watermark ,(0)it will be stored in the LSB of the watermarked image, otherwise (1) it will be stored .The second one is that it can provide multiple secret keys using shift and rotate operation. The watermark is embedded redundantly over all extracted blocks in image to increase image protection. This research provide high security for two reasons, the embedded bit will not be stored in LSB directly and this approach will use multiple secret keys.* ***Copyright © 2014 Praise Worthy Prize S.r.l. - All rights reserved.***

Keywords*: Watermark algorithm, Least Significant Bit Improvement, Watermark and Comparison Technique, Copyright Protection Watermarking image in spatial Domain.*

I. Introduction

Because of rapid growth in network distributions of images and video, there is an insisting need for copyright protection against plagiarism. Different digital image and video watermarking schemes have been proposed to address this issue of ownership identification [1]. Although, it not recognizable by human senses, easily, watermarking can be discovered by software detectors, and it would remain unchanged through multiple actions like editing, compression, decompression, encryption, decryption and broadcast — without affecting the quality of the content [2].

This technology relies on the fact that our eyes has very limited ability to observe minor changes in the color values of an image and even if they are observable they are subconsciously corrected so that no difference would be noticed by the observer[3],[4].

Steganography methods hide the presence of an arbitrary digital message by encoding it into other digital media, thus making its discovery process very difficult. The importance of steganography was recently reconsidered by governments with regard to Internet security [5].

On the other hand, digital watermarking focuses on the protection of intellectual property rights and the authentication of digital media. Similar to steganography methods, digital watermarking methods hide information in digital media. The distinction in the purpose of the hidden information – it pertains to the digital medium itself and contains information about its owner, its buyer, the integrity of the content, etc. Digital watermarking methods provide quick and inexpensive distribution of digital information over the Internet as well as new ways of ensuring the adequate protection of copyright holders in the intellectual property distribution process [6].

The format of this research is as follows. In section II, the related work is explained, the Traditional Least Significant Bit are outlined in section III, and section IV will explain the proposed algorithm. Section V discuss the results of proposed algorithm, section VI contains conclusion.

II. The previous watermark works

Technology is evolving at a staggering pace, it is having significant influence on our work, social life and overall quality of life. The internet and digital signal are much more widely used to transmit information due to this rapid evolution of technology, and as a result the use of digital watermarking is increased for a wide range of applications such as: copyright protection, provenance tracking, broadcast supervision, covert communication, bill security, and authenticity identification is more prominent than ever in recent history [7].

In (2010), a new method for embedding message in 6th, 7th and 8th bits of pixel values of an image is improved. A method to retrieve the message is also given. The advantage offered by this technique is that the message can be retrieved even if the intruder changes the least

Manuscript received January 2007, revised January 2007

significant bit of all the image pixels in which message has been embedded [8].

In (2012), a new watermark algorithm on the spatial domain of digital images is suggested to embed and extract invisible watermark and secret key is used. The watermark, according to the secret key, determines in a random manor vertically or horizontally across the base-image [9].

III. Traditional Least Significant Bit Technique

Watermarking systems usually have very important and desirable properties. These properties are often conflicting and might be forced to accept some trade-offs amongst these properties depending on the watermarking system application [10].

Effectiveness is the first and perhaps most important property. It is the probability of the message in a watermarked image might be correctly detected. Ideally the numeric value of this probability should be 1. Image fidelity is another very important property. Considering that watermarking is the process of altering an original image to add a message to it, it will inevitably affects the image's quality. It is highly desirable that this degradation of the image's quality be kept to a minimum, therefore no obvious differences in the image's fidelity may be noticed. The third property is the payload size, typically a watermarked work is a means to carry a message. The size of the message is often important as many systems would require a relatively big payload to be embedded in a cover work. There are of course certain applications that would only need a single bit to be embedded. Finally, robustness is extremely important for most watermarking systems.

Withstanding additive compression, printing and scanning, rotation, scaling, cropping and many other operations should be a hallmark of a robust watermark [11].

In basic Least Significant Bit (LSB) watermarking method, the visual impact is typically at a minimum. That is due to the technique used in which each pixel is modified to carry only 1 bit of information by changing the LSB to the required value, and since changing the LSB alters its value by 1 unit at most, this will keep visual impact at minimum. A large number of commercial steganography programs use the LSB as the method of choice for message hiding wide range of images. Due to noise that is always present in digital images, changes to the LSBs of the colors are very difficult to detect. Some of the advantages of LSB can be summarized as follow:-[12]

1. Simple to implement.
2. Since LSB techniques embed the message bits directly into the least-significant bit plane of the cover image in a deterministic sequence. This results in a change with too low of an amplitude to be human-perceptible. LSB embedding is simple, common and many techniques use these methods.

IV. The Proposed Watermarking Algorithm

This method depends on comparing between specific bits in pixels of the extracted blocks in cover image and bits of the watermark if they are equal, (0) it will be stored in watermarked image otherwise, (1) it will be stored in watermarked image. The positions of these bits are determined by key, where the key consist of eight digit from (0..7). Table (1) gives four pixels as an example before embedded of the bit stream,

TABLE I
EXPLAIN THE DATA BEFORE EMBEDDED

	Red Channel	*Green Channel*	*Blue Channel*
Pixel1	*11110010*	*10101111*	*10101000*
Pixel2	*10001001*	*11110000*	*10100001*
Pixel3	*10101000*	*10111000*	*10001111*
Pixel4	*11100101*	*11101110*	*11110011*

Assuming the key is (01234567) after one shift and rotate operation, the key become (70123456). And the embedded stream (ES) is (011110111010). Where Key is abbreviated by (K) and channel is (Ch.). The result of embedded into these pixels are explained into table II

TABLE II
EXPLAIN THE PIXEL AFTER EMBEDDING ELEMENTARY STREAM

	Red Ch.	K	ES	Green Ch.	K	ES	Blue Ch.	K	*ES*
Pixel1	*1111001<u>0</u>*	*0*	*0*	*1010111<u>0</u>*	*1*	*1*	*1010100<u>1</u>*	*2*	*1*
Pixel2	*1000<u>1</u>000*	*3*	*1*	*111<u>1</u>0000*	*4*	*1*	*10<u>1</u>00000*	*5*	*0*
Pixel3	*1<u>0</u>101001*	*6*	*1*	*<u>1</u>0111000*	*7*	*1*	*<u>1</u>0001111*	*7*	*1*
Pixel4	*1110010<u>1</u>*	*0*	*0*	*1110111<u>0</u>*	*1*	*1*	*1111001<u>0</u>*	*2*	*0*

To highlight tables above we'll take pixel3 as a sample of pixels. By comparing pixel3 in table one and two. It is noted that the LSB of Red channel in pixel3 become (1) because watermark bit (ES) is different from (bit with underline (0)) which is determined by key (6) that locate the position of bit in that channel of pixel. While, LSB of Green channel in pixel3 still the same(0) , because watermark bit (ES) is equal to last bit in green channel of pixel3.The following steps explain the proposed algorithm in details:-

Proposed Algorithm

Input: - Original image (BMP image), Watermark

Output: Watermarked Image (BMP image)

Step1:-Divide BMP image into several blocks (8x8) pixel for each one.
Step2:-Test each block in image to determine the blocks that doesn't loss informatin.
Step3:-Select key that consist from (0 to 7) for example (10235476).
Step4:-Use the extracted block in step (2) to embed watermark.
Step5:-Compare each pixel in the extracted block with one number key to determine the location of bit in pixel. If that bit similar to the one in watermark image. (0) will be stored in the LSB in that pixel. Otherwise (1) will be stored instead.
Step6:- After complete the key of step (3) another key can be created. This can be done by shift and rotate the first key by one.
Step7:- Repeat steps from (3-6) until complete all extracted blocks.

V. Fidelity Criteria

To evaluate the performance of our new algorithm, two metrics can be used. First one is Mean Square Error (MSE), second is Peak Signal to Noise Ratio (PSNR). These metrics are used to measure the quality of reconstructed image as compared to the original one. MSE is used to calculate differences between watermarked image and original one. PSNR, is a term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation.[13]

$$PSNR=10.\log_{10}\left(\frac{MAXI^2}{MSE}\right) \quad (1)$$

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

Here, MAXI is the maximum possible pixel value of the image. Its value is 255, if the pixels are represented using 8 bits per pixel. For color images with RGB values per pixel, the definition of PSNR is the identical except the MSE is the sum over all squared value differences divided by image size and by three.[13]

VI. Result of the proposed algorithm

Typical values for the PSNR in lossy image and video compression are around from 30 to 50 dB, where higher is better. Table (III) shows that the result of watermark in this algorithm gives a higher quality of watermarked image (PSNR is high) and store watermark in non-direct way (by comparing process that mentioned in the proposed algorithm) which provides high security, it prevent attacker from even detect there is watermark store in it.in this paper, payload capacity depends on the extracted block in the cover image. If the extracted blocks is high, the capacity is high.

TABLE III: - EXPLAIN PSNR AND MSE AFTER EMBED WATERMARK INTO IMAGE

Image no.	*Image size (KB)*	*Size of embedded Data (Bytes)*	*MSE*	*PSNR*
Image 1	*230400*	*35008*	*0.0257*	*64.017*
Image2	*773*	*2080*	*0.0029*	*73.504*
Image3	*396*	*149*	*0.0004*	*81.94*

Fig1, Fig2 and Fig3 give results that there is no visual distortion in watermarked image.


Image1 A: Original image


Image1 B: Watermarked Image

Fig.1:- Explain that there is no visual difference between these images


Image2 A: Original image


Image2 B: Watermarked Image

Fig.2:- Explain that there is no visual difference between these images


Image3 A: Original image


Image3 B: Watermarked Image

Fig.3:- Explain that there is no visual difference between these images

VII. Conclusion

This approach provide a perfect result which gives high similarity between watermarked image and original one. Multiple key is used through changing key using shift and rotate operation which gives high level of security.
This method solve the problem of the traditional LSB technique, by preventing attacker from watermark extraction by accumulating LSB in pixels of watermarked image (because of the embedding in LSB is done based on the comparison between embedded bit and bit in pixels of cover image that is determined by key), as well as, watermark destroying prevention, watermark is repeated on all extracted block of watermarked image. MSE is low and PSNR is high cause of using only one bit in LSB.

References

[1] Sundararajan Madhavan, Yamuna," A Wavelet Based Scheme for Video Watermarking", International Review on Computers and Software (IRECOS), Vol 8, No.4,2013.

[2] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom,"Digital Watermarking",2002.

[3] Juergen Seitz, "Digital Watermarking for Digital Media", 2005.

[4] Ching-Sheng Hsu , Shu-Fen Tu," An Imperceptible Watermarking Scheme Using Variation and Modular Operations", International Journal of Hybrid Information Technology, Vol. 1, No. 4, pp. 9-16, 2008.

[5] Mrs. Kavitha, KavitaKadam, AshwiniKoshti, PriyaDunghav," Steganography Using Least Signicant Bit Algorithm", International Journal of Engineering Research and Applications (IJERA), Vol. 2, pp. 338-341, 2012.

[6] Manpreet Kaur, Sonika Jindal and Sunny Behal," A Study of Digital Image Watermarking", International Journal of Research in Engineering & Applied Sciences, Volume 2, pp. 126-136, 2012.

[7] SATHAWANE M.S. AND BORA P.P., "Various Media Type and its application using Digital Watermarking", World Research Journal of Pattern Recognition, Volume 1, pp.-09-11,2012.

[8] Sudhir Batra, Rahul Rishi, and Rajkumar," Insertion of message in 6th, 7th and 8th bit of pixel values and its retrieval in case intruder changes the least significant bit of image pixels",International Journal of Security and Its Applications, Vol. 4, No. 3, 2010.

[9] Mustafa Osman Ali, Elamir Abu Abaida Ali Osman, RameshwarRow,"Invisible Digital Image Watermarking in Spatial Domain with Random Localization", International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, 2012.

[10] Mohan Durvey, Devshri Satyarthi," A Review Paper on Digital Watermarking", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3,2014.

[11] Aparna S. Kulkarni, S. S. Lokhande,"Digital Watermarking Using DWT And DCT", International Journal of Scientific & Engineering Research, Volume 5, 2014.

[12] Champakamala .B.S, Padmini.K, Radhika .D. K," Least Significant Bit algorithm for image steganography", International Journal of Advance Computer Technology, Vol3, No.4, 2014.

[13] Naitik P Kamdar, 2Dipesh G. Kamdar 3Dharmesh N.khandhar," Performance Evaluation of LSB based Steganography for optimization of PSNR and MSE", Journal of information, knowledge and research in electronics and communication engineering, Vol2, 2013.

Auther's information

[1,2] Computer Science Department, University of technology, Iraq.
Computer Science Department, Al-Qadisiyah University, Iraq

Dr. Abdul Monem S. Rahma Ph.D Awarded his M.Sc. from Brunel University and his Ph.D. from Loughborough University of technology United Kingdom in 1982, 1984 respectively. He taught at Baghdad university department of computer science and the Military Collage of Engineering, computer engineering department from 1986 till 2003. He fills the position of Dean Asst. of the scientific affairs and works as a professor at the University of Technology computer Science Department.
He published 88 Papers, 4 Books in the field of computer science, supervised 28 Ph.D. and 57 M.Sc. students. His research interests include Computer graphics image processing, Biometrics and Computer Security. And he attended and submitted in many scientific global conferences in Iraq and many other countries. From 2013 he fills the position of Dean of the computer Science Department at the University of Technology.

.Dr. .Matheel E.Abdulmunim 1995 B.Sc. in computer science in Department of computer science of technology of university, Baghdad – Iraq.2000.M.Sc. in computer science in Department of computer science of technology of university, Baghdad – Iraq. 2004 Ph.D. of philosophy in computer science in Department of computer science of technology of university, Baghdad –Iraq.

Rana J.S. Aljanabi is currently Ph.D. student at university of technology in Baghdad /Iraq. Her B.Sc. from Babylon University/ Iraq. Her M.Sc. from Baghdad University in Baghdad /Iraq. Her carrier as a Lecturer in computer Science Department of Al-Qadisiyah University, Al-Qadisiyah- Iraq.