NTU JOURNAL OF ENGINEERING AND TECHNOLOGY
EISSN: 2788-998X

RESEARCH ARTICLE
Open Access

Improved Watermark Criteria Through Mark image

Abdulkreem Mohammed Salih [1], Karam M.Z. Othman[2], Shayma Wail Nourildean[3]
abdulkreem86@ntu.edu.iq , karam.mz@ntu.edu.iq , coe.visit.08@uotechnology.edu.iq

[1,2] Northern Technical University, [3] Communication Engineering Dept., University of Technology
Co-authors: Abdulkreem Mohammed Salih, abdulkreem86@ntu.edu.iq
Received: 27-10-2021, **Accepted:** 07-02-2022, **Published online:** 22-02-2022

Abstract. With many applications using digital multimedia technologies, the need to protect digital multimedia data from hackers is emphasized. Copyright holders are concerned about protecting any kind of unlawful duplication of their information. With all these kinds of problems, technology development is very important. Digital watermarks are an important requirement to protect multimedia data. There are important criteria to measure the success of a watermarking process, its confidentiality, capacity and reliability. In this paper, the logo mark was relied upon to achieve these criteria by taking advantage of the symmetry characteristic of the logo image, which is often used this type of logo images. Symmetry reduces the size of the embedded data, reduces the location of the embedded within the image, and increases confidentiality by encrypting less data in various ways.

Keywords: logo, NC, symmetry image.

Introduction

As a result of the wide development in the field of the Internet and multimedia in the past years, which led to the rapid increase in the provision of digital knowledge such as video, audio, images and written texts, as a result, the problem of secure transmission of that data became necessary. The solution to this vulnerability is digital watermarking, which is considered the most typical and most powerful technology to protect the digital media [1]. Some papers focused on frequency domain by using DCT and WL transform as the method for watermarking presented in [2] This algorithm masks the watermark as an image encoded in the frequency domain using discrete cosine transform. By encode a repeating logo in a color image of the cover. This ensures that it is difficult to detect and gives it greater reliability through the process of its repetition. paper [3] deals with a method depends on the discrete cosine transformation to transform image to a frequency domain and select the suitable areas in a cover image where the logo can be embedded without affecting the image. Two conversion DCT and WL were combined in [4] where the original image is rearranged by use the zigzag sequence transform, DWT is used on the re-arranged image. Then DCT and SVD processing are applied over all the high bands LH, HL and HH. Spatial domain applied in [5] where this a Least Significant Bit (LSB) algorithm was used to embed watermark images using Message/logo in the image. New method presented in paper [6] by hide the mark image in frequency domain through combined the DCT with principle of the spread spectrum communication. All the previous works mentioned above and other research papers relied on logo, which is an binary image that has the property of symmetry, that is, half of the image is views of the other half, and this was the idea behind this paper.

Criteria of watermarking process:

The important criteria that are used to measure the acceptability or success of the watermark algorithm [7] and among these criteria that were discussed are:

1- Image quality: It is achieved by calculating the value of PSNR peak signal-to-noise ratio value [2] as shown in the equation. (1):

$$\mathrm{PSNR} = 10\log 10 \frac{255^2}{\mathrm{RMSE}} \qquad (1)$$

The RMSE is root mean square error and can be expressed as:

$$\mathrm{RMES} = 1/(\mathrm{M} * \mathrm{N}) \sqrt{\sum_{i=1}^{M} \sum_{j=1}^{N} [I(i,j) - f(i,j)]^2} \qquad (2)$$

The values, M , N refer to the image dimensions (number of pixels) (M equal to N). If the number of variable bits in the cover image is reduced, the PSNR value will be better.

The correlation ratio can also be calculated by finding the normal correlation coefficient NC as in equation (3):

$$\mathrm{NC} = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} w(i,j) w'(i,j)}{\sum_{i=1}^{M} \sum_{j=1}^{N} w(i,j)^2} \qquad (3)$$

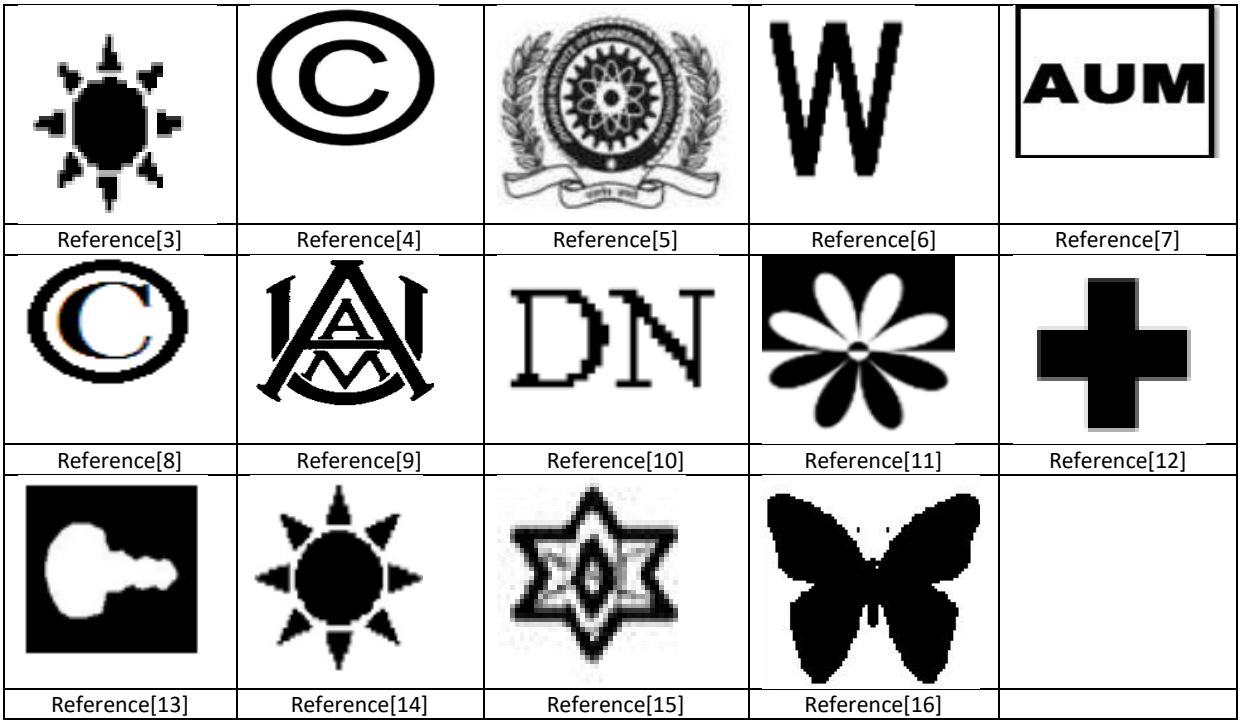
w(i,j) and w'(i,j) represent the origin and extracted logo alternately, and It's value equal to 1 for ideal state[14].

2- Security: It is a term that indicates that the pixels within which the logo is hidden cannot be detected, or that the method of hiding the logo cannot be detected [15].

3- Capacity and Robustness: Capacity is defined as a measure of the amount of data hiding in the cover image, while the term Robustness refers to the extent of the ability to be immune from attacks

Symmetry Characteristic of the Logo Image

The logo image is the data that is included within the image. Often this logo is an image comprises a number of bits and is in the form of a symmetric image. This characteristic gives us a lot of permission through which we can achieve the required and important criteria for watermarking image process. Figure (1) shows samples of the symmetric watermark used in this papers [1-15].



Reference[3]	Reference[4]	Reference[5]	Reference[6]	Reference[7]
Reference[8]	Reference[9]	Reference[10]	Reference[11]	Reference[12]
Reference[13]	Reference[14]	Reference[15]	Reference[16]	

Figure(1) samples of the symmetric watermark used in papers

For further investigation a specific image has been chosen from the above images and convert its values into a series of bits (0-1)
a repetition of the bits can be noticed and this repetition is distributed in a symmetric manner, as shown in Figure (2).

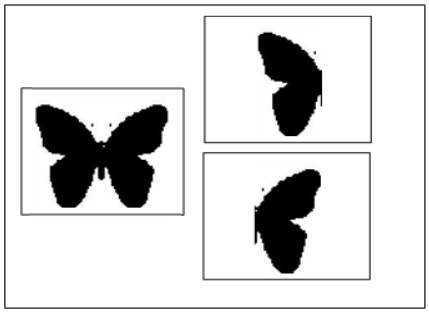


Figure (2) Symmetric Property for Logo Image

Thus, half of these data can be dealt with as the other half can be generated through the first half. This improves the capacity at which can embed the image as well as increases the reliability of watermarked image and reduce manipulation and alteration in the original values of the cover image by reducing the number of embed sites.

Process of Embedding

The embedding process adopted in this proposed algorithm. Consists of the following steps : -

1- Divide the binary logo image consisting of a (64*64= 4,096 bits) bit into two images (image1 and image2) each image (32*64=2,048 bits) bits and each image is the same as the other.
2- One of these two images (image1 or image2) is credited for embedding in the cover image.
3- The string consisting of (2,048) bits is fed to a processing stage using the XOR gate with a series of selected values [0 1] to give randomness to the data, which increases security.
4- The obtained data represent the new logo image will be inserted.

Simulation and Results

To ensure that results are achieved through the use of the adjective symmetry; a logo image is included in an image in two cases. The first case without using the symmetrical adjective for the logo and the second case is using the symmetry of the logo. PSNR and capacity are calculated, also the watermarked image is exposed to an attack, and the results are observed for both cases. Standard images of (512*512) gray scale image used as cover image, and the logo of binary image (64*64) used for insertion. Table (1) shows the differences in results when two cases are used (case(1) without symmetry property, case(2) using symmetry property).

Table (1) :(PSNR ,NC, No.Pixels used) for two cases

Image	 Lena	 Peppers	 barbara
Logo Image			
PSNR for Case (1)	48.332 db	48.5767 db	48.1579 db
PSNR for Case (2)	48.876 db	48.765 db	48.343 db
NC for Case (1) with attack	0.952	0.941	0.932
NC for Case (2) with same attack	0.967	0.95	0.944
No. of pixels used for insertion in Case (1)	4096	4096	4096
No. of pixels used for insertion in Case (2)	2048	2048	2048

Conclusion

In this proposed paper, it was mainly relied on dealing with the image logo more than dealing with the mechanism of embedding inside the cover image, and through dealing with this logo it was ensured that the values of the criteria used in the approved watermark were improved. Reducing the size of the data embedded within the cover image contributes to increase the capacity by reducing the size of the bits that are embedded within it to half of what it was. Reliability has been increased by reducing the embedded pixels and as a result the number of pixels exposed to attack is reduced by half as well. The final parameter is the security has been improved by reducing the bits that are embedded, and therefore there is greater tolerance in its encryption. Table (1) proves what was mentioned above through the results obtained during the use of the measurements of the standards.

References

[1] Namita Tiwari and Sharmila, "Digital Watermarking Applications, Parameter Measures and Techniques", IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.3, March (2017), page 184-194.

[2] Abdulkreem Mohammed Salih, Baraa T. Sharef, Fahad Layth Malallah, "Optimal Area Algorithm For Data Hiding In Digital Image", The International Journal of Engineering and Science (IJES), Volume 8 , Issue 11, Series I ,PP 58-63,(2019).

[3] Jobin Abraham, Varghese Paul," A DCT Based Imperceptible Color Image Watermarking Scheme", International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol.9, No.7 (2016), pp.137-146.

[4] Md. Maklachur Rahman," A DWT, DCT AND SVD BASED WATERMARKING TECHNIQUE TO PROTECT THE IMAGE PIRACY", Department of Computer Science and Engineering, Chittagong University of Engineering and Technology, Bangladesh,(2013).

[5] Deepshikha Chopra, Preeti Gupta, , Gaur Sanjay B.C., Anil Gupta," Lsb Based Digital Image Watermarking For Gray Scale Image", IOSR Journal of Computer Engineering (IOSRJCE), ISSN: 2278-0661, ISBN: 2278-8727 Volume 6, Issue 1 (Sep-Oct. 2012), PP 36-41.

[6] Abdulkareem Mohammed Salih," Secured Watermarking Image Using Spread Spectrum", Tikrit Journal of Engineering Sciences 23 (3) (2016) 71-78.

[7] Ersin Elbasi, "M-SVD based Quality Measurement in Hybrid non-blind Watermarked Medical Images", The American University of the Middle East, Conference Paper July 2020, DOI: 10.1109/TSP49548.2020.9163558 .

[8] Abdulkareem Mohammed Salih, Salih Hassan Mahmood, " Digital Color Image Watermarking Using Encoded Frequent Mark". Journal of Engineering, Number 3 Volume 25 March (2019).

[9] SONYA INNA LYATSKAYA, " DIGITAL WATERMARKING TECHNIQUES IN IMAGE PROCESSING" thesis, Department of Computer Science , Alabama A&M University, January (2006).

[10] Agus Winarno, De Rosal Ignatius Moses Setiadi, Adli Azhar Arrasyid, Christy Atika Sari, Eko Hari Rachmawanto," Image Watermarking using Low Wavelet Subband based on 8×8 Sub-block DCT", International Seminar on Application for Technology of Information and Communication,(2017).

[11] Singamaneni Kranthi Kumar, Pallela Dileep Kumar Reddy, Gajula Ramesh, Venkata Rao Maddumala," Image Transformation Technique Using Steganography Methods Using LWT Technique", international information and engineering technology association, Vol. 36, No. 3, June, (2019), pp. 233-237.

[12] Ajib Susanto, De Rosal Ignatius Moses Setiadi, Christy Atika Sari, Eko Hari Rachmawanto," Hybrid Method using HWT-DCT for Image Watermarking", Conference Paper August (2017) DOI: 10.1109/CITSM.2017.8089252.

[13] Usman Sudibyo, Fatma Eranisa, Eko Hari Rachmawanto, , De Rosal Ignatius Moses Setiadi, Christy Atika Sari," A Secure Image Watermarking using Chinese Remainder Theorem Based on Haar Wavelet Transform", Conference Paper October 2017 DOI: 10.1109/ICITACEE.2017.8257704

[14] Jobin Abraham, Varghese Paul," An imperceptible spatial domain color image watermarking scheme", Journal of King Saud University – Computer and Information Sciences 31 (2019) 125–133.

[15] Kaiser J. Giri, Mushtaq Ahmad Peer and P. Nagabhushan, " A Robust Color Image Watermarking Scheme Using Discrete Wavelet Transformation" , I.J. Image, Graphics and Signal Processing,(2015), 1, 47-52, DOI: 10.5815/ijigsp.2015.01.06

[16] LI Hui-fang, CHANG Ning, CHEN Xiao-ming," A study on image digital watermarking based on wavelet transform" , The Journal of China Universities of Posts and Telecommunications, July 2010, pp 122–126.