

Strengthen mark image by downsampling some adjacent pixels

Abdulkreem Mohameed Salih

Northern Technical university, abdulkreem86@ntu.edu.iq

Abstract: Multimedia is a mode of communication that blends various types of content, including image, audio, text, animations, and video, and the digital watermark is one of these kinds of marker to protect this multimedia. This Mark is intercepted by many of threats that are intended to be removed, destroy, or detected. To determine the success or failure of this process, there are certain criteria are used to make this decision. In this research, some features of the logo image were taken advantage of to achieve the best values for those criteria that determine the quality and success of the watermarking process. The method used is to insert some of the watermark and leave others, and rely on similar values for adjacent pixels while keeping a secret key to arrange the pixels after deleting part of the mark image, and using this key between sending and receiving . Paper foxed on the adjacent pixels have same zero value property contribute to reduce number of pixels of mark image that will be injected after splitting the logo to blocks. By separate the mark into blocks and the segments whose adjacent bit values are different will be injected into the cover image it facilitates the injection process. Reducing the number of bits injected means reducing the time needed for injection bits into the cover image and reducing the number of bits that are vulnerable to attack, Consequently the values of these criteria (quality-security- Capacity and Robustness) improved according to the results obtained.

Keywords: logo, Adjacent pixel, similarity, PSNR, NC

1. Introduction

With the rapid development of today's Internet and multimedia fields, as a result, this has led to a significant increase in digital multimedia such as video, audio, images and written text. On the other side, there is a problem in the transmission of this multimedia because there are hackers and thieves. The first of the most important solutions to this vulnerability is digital watermarking [1]. There are many papers focused on the field of watermark; some of these papers used the field frequency domain by converting images with Discrete Cosine Transform (DCT) and wavelet transform. Some papers concentrate on the spatial domain for embedding the mark image, as in [2] depend on energy in least significant bit by hide the text in high density area.. A new method was suggested in [3] by finding the direct current in the spatial domain without of the true 2D-DFT in spatial domain where a novel spatial domain color image watermarking technique is proposed for protecting the copyright of color image.

On the other side, a frequency domain, as in[4][5], depends on frequent and encoded mark images and is then inserted in the cover image after converting the frequency domain using DCT. Ref [6] used two masks for mark image to ensure the embedded bits are less distracting to the human eyes.

A new design scheme of copyright management system based on digital watermarking and its information, such as blockchain, is proposed, which combines digital watermarking with another technique presented in [7].

Authors in Ref [8] rearrange the form of the mark image by using the symmetry property in the mark image, and this process reduces the number of pixel injection. Symmetry properties in



Copyright: © 2023 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

logo image decreases the quantity of data embedded and minimizes its placement within the image, resulting in the highest level of perplexity. Use a noisy image as a secondary carrier for a watermark, represented in the form of a bit vector.

An algorithm for the construction of a noisy image carrying a watermark sequence is used in [9]. also method was used to embed the hidden text in the least significant bit (LSB) of the discrete cosine transform (DCT) using a linear modulation algorithm as in [10].

Paper [11] applied a new form of watermarking in through embedding Cubic-spline interpolation inside the image by Bit Plane Slicing. The main objective of this proposed paper was to present the watermark hiding in the colored cover image by injecting the least possible number of bits and including the remaining number by means of a code through which the bits can be known without actual inclusion. The remainder of this paper is included by explaining the criteria that are used for the success of this algorithm, as well as the method of reducing the number of bits for the watermark, and simulating and discussing the results.

2. Watermarking Criteria

There are many important criteria used for measuring the success of watermark processing [10]; some of these criteria are mentioned below:

2.1 The quality of the image

This is done through calculating the peak signal-to-noise ratio PSNR [20] as given in the equation. (1):

$$\text{PSNR} = 10 \log_{10} \frac{255^2}{\text{RMSE}} \quad \dots(1)$$

RMSE refers to the Root Mean Square Error and is computed as:

$$\text{RMSE} = \frac{1}{(M * N)} \sqrt{\sum_{i=1}^M \sum_{j=1}^N [I(i,j) - f(i,j)]^2} \quad \dots(2)$$

Where (M-N) refer to the image row and columns (pixels number) (M equal to N). Reducing the number of variable bits in the cover image gives a better value for PSNR.

Process of calculation of the parameter of correlation ratio through finding the Normal Correlation coefficient NC as in equation (3):

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

w(i,j) and w'(i,j) refer to the pixel value of the original and extracted logo alternately, and its value is 1 in the ideal case[14,15].

2.2 Security

In image watermarking, the security parameter is a value that is used to control the strength of the cryptographic protection of the watermark. It is a measure of the level of security that is required for the watermark to be protected against unauthorized modifications or removals [9][16].

2.3 Capacity and Robustness

Capacity refers to the maximum amount of data that can be embedded within the image without significantly degrading the quality of the image. The higher the capacity, the more data that can be hidden. Robustness, on the other hand, refers to the ability of the watermark to withstand intentional or unintentional attacks such as image compression, scaling, cropping, and

other image processing techniques. A robust watermark can survive these attacks and still be detected and extracted from the watermarked image [17,21].

3. Process of Neglecting Pixels

A logo image is a two-dimensional binary image consisting of (64×64) bits, and these bits have a value of either 0 or 1. If this image is divided into blocks, each block size is 8×8 bits, most of these blocks have similar bits. Figure 1 represents a diagram for a binary image and how to divide it into blocks having the similarities in the adjacent bits for each block.

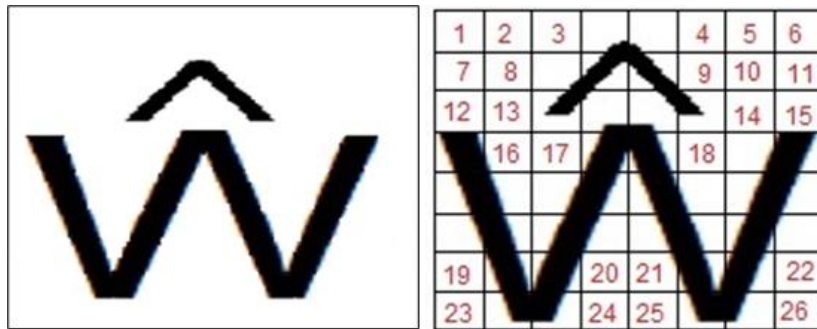


Figure 1: Diagram for a binary mark image.

As shown in Figure1, the logo image is divided into 64 blocks, 26 blocks out of a total of 64 blocks its bits value are the same. As a result, more than (0.33) of mark image can be sorted and not embedded in the cover image as in Figure2 and Figure3. Abbreviations of bits that are embedded contribute to the achievement of criteria of watermarking images, Figure3 It shows that the number of pixels being injected reduced after applied proposed algorithm.

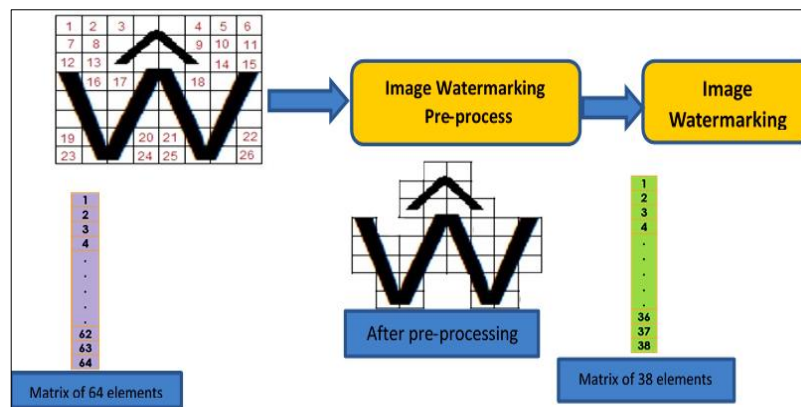


Figure 2: Neglected of some adjacent pixels.

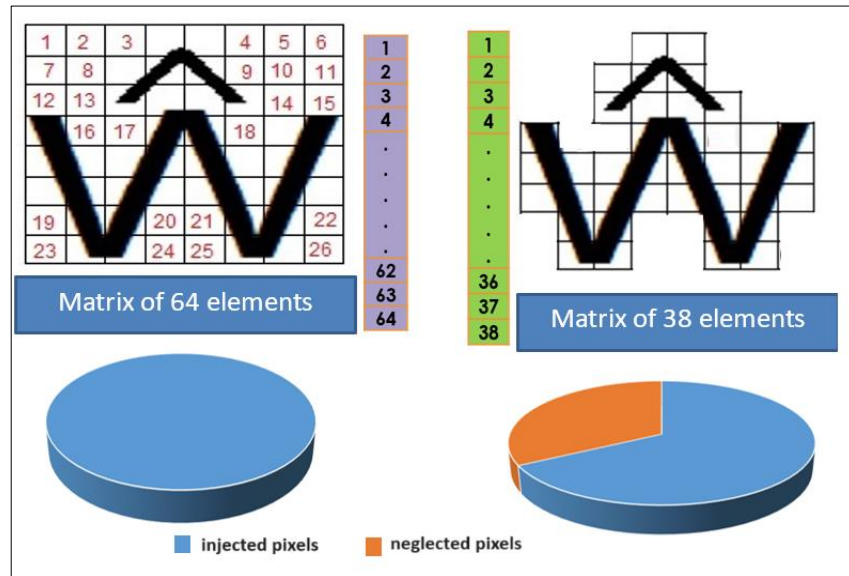


Figure 3: Pixel ratio reduced after deleting adjacent bits

4. Process of Embedding

The proposed embedded algorithm consists of a set of sequential steps, as shown: -

1. Divide the mark binary image into a group of blocks, each block contains (8*8) bits.
2. Check the similarity for each block (if bits value for the selected block are zeros) then assigned that the block is similar.
3. Create an array of (64) elements; the value of each element depends on the corresponding block number of mark image. this array, called Array1
4. If the block is similar then assigned "0" in the element else, assign "1".
5. For non-similar blocks, store their value bits in an array called Array2.
6. Embed the bits of array2 in the 2nd bits of cover image.
7. Create key1= hexadecimal of stream of array1 (where the 64 bits convert to 16 digits only).
8. Create key2=number of non-similar blocks. Figure 4 show flow chart for an algorithm represent the steps of embedded process.

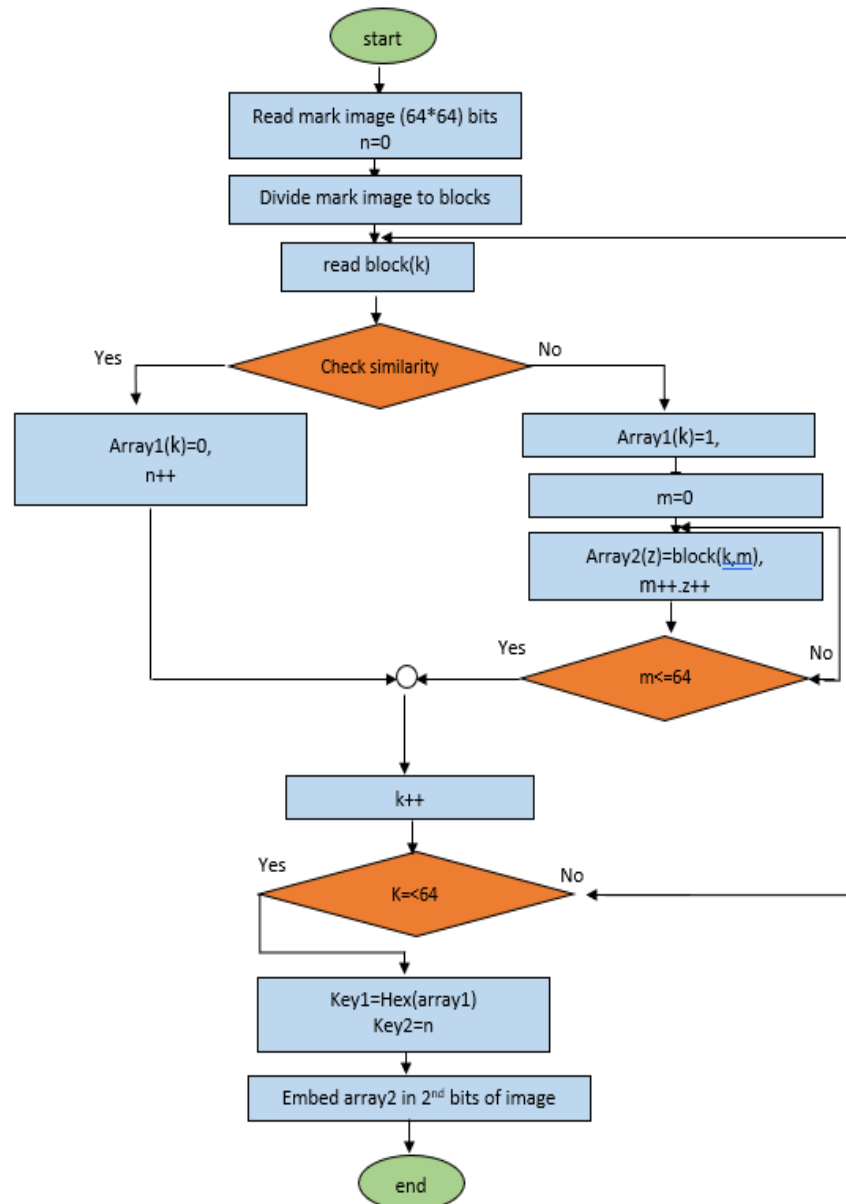


Figure 4: Algorithm of embedded process

5. Experimental Discussion

To ensure the results are improved when using the proposed algorithm, the same data (logo and cover image) that was used in Ref [4], color (512*512) pixels images and a binary images size (64x64) pixels are used. Three type of comparison are used in this paper, two tables were used to compare the results, Table 1 contains a comparison of the PSNR value while in Table 2 the normal correlation coefficient is compared and the amount of its affected when transmitted or attacked by hackers (used same mark image).

Table 1: Compared PSNR for watermarked color image.







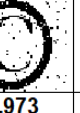
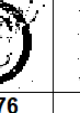



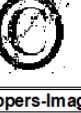

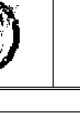





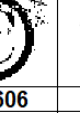
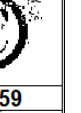





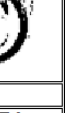
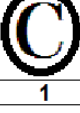



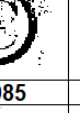
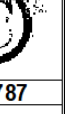




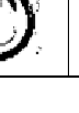

Image			
	Lena	Peppers	Airplane
PSNR in ref. [4]	35.332 dB	35.1734 dB	34.7786 dB
PSNR in proposed algorithm	35.421 dB	35.2901 dB	34.9043 dB

Table 2: NC compared between proposed algorithm and other previous work.

Covered-image	Lena-Image						
	Attacks	Without-attack	Cut part from image	L.P.F.	Salt and Peppers	Mean Filter	Gaussian Filter
Ref[4]	NC	1	0.998	0.996	0.953	0.966	0.972
	Extracted-mark image						
Proposed algorithm	NC	1	0.998	0.997	0.973	0.976	0.979
	Extracted-mark image						
image	Peppers-Image						
Ref[4]	NC	1	0.999	0.952	0.946	0.9592	0.9743
	Extracted-mark image						
Proposed algorithm	NC	1	0.997	0.986	0.973	0.9606	0.9759
	Extracted-mark image						
image	Airplane-Image						
Ref[4]	NC	1	0.990	0.963	0.948	0.959	0.974
	Extracted-mark image						
Proposed algorithm	NC	1	0.995	0.9789	0.9712	0.985	0.9787
	Extracted mark image						

Other comparison used through the Gaussian noise and salt and pepper attacks on the cover image (Lena image) compared to other related works show how efficient the proposed algorithm is through the NC value as in the Figure4.

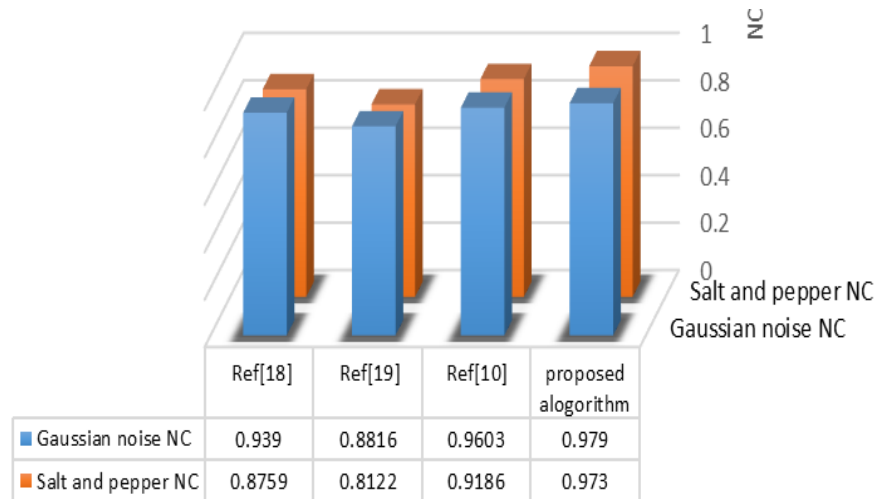


Figure 4 :NC compared between proposed algorithm and other previous work.

6. Conclusion

With the aim of improving the criteria of the watermark process, the proposed algorithm focused on mechanism of dealing with the mark. The number of embedded bits is reduced by isolating the blocks that contain zero value for all bits after dividing the mark into a group of blocks. Reducing the data series that is included inside the cover image increases the capacity by reducing the number of bits. The process of reducing and redistributing the mark bits adds a kind of security by creating secret keys where two secret keys were obtained without them the mark cannot be read and there is a specific algorithm to include and read the mark. The reliability criterion also improved As a result of reducing the number of pixels that can be attacked, and thus we get the least number affected by the attacks. The results in Tables 1, Table 2, and Figure 4 show better results compared to previous work, which supports the strength and efficiency of this algorithm in its use in the watermarking process.

References

- [1] L.Hui-fang, CH. Ning, CH. Xiao-ming, 2010, " A study on image digital watermarking based on wavelet transform", The Journal of China Universities of Posts and Telecommunications, pp 122–126.
- [2] Oh-Jin Kwon, S. Choi , and B. Lee, " Watermarking Using Energy-LSB Embedded Method ", Wasit Journal of Computer and Mathematic Science, Vol. (1) No. (3) pp(140-148)(2022).
- [3] Q. Su,D. Liu,Zihan Yuan,Cang Wang, X. Zhang, B. Chen, and T. Yao, 2019, " New Rapid and Robust Color Image Watermarking Technique in Spatial Domain", IEEE Access, Vol.7, pp. (30398 – 30409).
- [4] A. M. Salih, S. H. Mahmood, 2019,"Digital Color Image Watermarking Using Encoded Frequent Mark". Journal of Engineering, Number 3 Vol.25 March.
- [5] M. Ali, Ch. W. Ahn, M. Pant, S. Kumar, M. K. Singh and D. Saini, 2020 ,"An Optimized Digital Watermarking Scheme Based on Invariant DC Coefficients in Spatial Domain", Computer Science & Engineering, Electronics (ISSN 2079-9292), 9(9), 1428.
- [6] J. Abraham, V. Paul," A DCT Based Imperceptible Color Image Watermarking Scheme,2016 , "International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol.9, No.7, pp.(137-146).
- [7] M. Zhaoxiong, M. Tetsuya, M. Sumiko, and K. Hirotsugu," Design scheme of copyright management system based on digital watermarking and blockchain", 2018 42nd IEEE International Conference on Computer Software & Applications.
- [8] A. M. Salih, K. M. Othman., & Sh. Wail Nouraldain , 2022 "Improved Watermark Criteria Through Mark image", NTU Journal of Engineering and Technology, 1(2), pp. (36–39)

-
- [9] Y. Vybornova and V. Sergeev, 2019 , “Method for Vector Map Protection based on using of a Watermark Image as a Secondary Carrier”, Proceedings of the 16th International Joint Conference on e-Business and Telecommunications (ICETE 2019), pp. (284-293).
- [10] W. Alomoush, O. A. Khashan, A. Alrosan. et al. 2023, “ Digital image watermarking using discrete cosine transformation based linear modulation. J Cloud Comp 12, 96. <https://doi.org/10.1186/s13677-023-00468-w>.
- [11] H. Dh. Najeeb, 2019 , ” New Techniques of Watermark Images using Bit Plane Slicing and Cubic-spline Interpolatio “, Ibn Al-Haitham Jour. for Pure & Appl. Sci. 32 (3) .
- [12] T. K. Araghi, and A. A. Manaf, 2019 ,“An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD”, Future Generation Computer Systems, Vol. 101, pp. (1223-1246).
- [13] S. P. Ambadekar, J. Jain, and J. Khanapuri, 2018 , ”Digital Image Watermarking ThroughEncryption and DWT for CopyrightProtection”, Advances in Intelligent Systems and Computing book series (AISC), vol. 727, pp. (187-195).
- [14] E. Maiorana, and P. Campisi,2016” High-capacity watermarking of high dynamic range images”, Maiorana and Campisi EURASIP Journal on Image and Video Processing.
- [15] M. Zulqarnain, M. Gh. Ghouse, W. Sharif, G. Jilanie, And Amna Shifa, 2021 ”An Efficient Method of Data Hiding for Digital Colour Images Based on Variant Expansion and Modulus Function”, Journal of Engineering Science and Technology , vol.16, No. 5, pp. (4160 – 4180), School of Engineering , Taylor’s University.
- [16] S. P. Vaidya, and Ch. M. P.V.S.S.R., 2015,” Adaptive Digital Watermarking for Copyright Protection of Digital Images in Wavelet Domain”, Procedia Computer Science, vol. 58, pp. (233–240).
- [17] B. A. Wijaya, A. J. Manalu, B. A. Tarigan, and S. Silitonga, 2021, ”Steganography Text Message Using LSB and DCT Methods”, Institute of Computer Science (IOCS), Journal Mantik, vol. 5, No. 3 pp. (1825-1832).
- [18] . SH A. Parah , J.A. Sheikh , N. A. Loan, et.al , 2016, ”Robust and blind watermarking technique in DCT domain using inter-block coefcient diferencing”. Digital Signal Process 53:11–24.
- [19] Ch. Das , S. Panigrahi , V. K. Sharma , et al , 2014,”A novel blind robust image watermarking in DCT domain using inter-block coefcient correlation”. AEU-International Journal of Electronics and Communications , Vol. 68, No. 3,pp.(244-253).
- [20] H. A.Hilal, 2019, ” Digital Watermarking Under DCT Domain According to Image Types” Iraqi Journal of Information Technology. Vol.9 No.4.pp.(30-42).
- [21] I. M. Zeebaree, H. A. Abdullah , F. M. Khalifa , et.al , 2023” Copyright Protection System Based Watermarking ” Journal of University of Duhok., Vol. 26, No.2 (Pure and Engineering Sciences), pp.(1-12).
- [22] Kh. M. Hashim ,S Sh. Baawi ,and B. K. Hilal, 2021, ” An Image Watermarking Technique Proposed Based onDiscrete Cosine Transformation and Pseudo-Random Generator”, Journal of Education for Pure Science- University of Thi-Qar Vol.11, No1 pp.(108-118).
- [23] Oh-Jin Kwon, S. Choi , and B. Lee, 2018, ”A Watermark-Based Scheme for Authenticating JPEG Image Integrity “, IEEE Access ,Vol. 6, pp. (46194 – 46205), Electronic ISSN: 2169-3536.