Robust Distance-Based Watermarking for Digital Image

A. S. Abdul-Ahad[1], Baran Çürüklü[1], and Waleed A. Mahmoud[2]
[1]School of Innovation, Design and Engineering, Mälardalen University, Västerås, Sweden
[2]Department of Electrical Engineering, Al-Isra Private University, Amman, Jordan

Abstract- *In this paper, an algorithm is developed to invisibly watermark a cover object (color image) using watermark object (iconic image). The algorithm is based on the distances among the addresses of values of the cover object. These distances use to make the embedding. The order of manipulating these distances are specified by the values of the watermark data which is dealt with serially. The algorithm serves and achieves self encryption key. Each watermark object has its unique pattern of distances at different possible lengths of distance bits. This enhances the complexity of sequential embedding. The algorithm is tested using direct and single level and double level of Two-Dimensional Discrete Wavelet Transform (2D DWT) embeddings. Two important issues are addressed. Firstly is to achieve a high Peak Signal to Noise Ratio (PSNR). The ratio was found to increase with an increasing of distance bits. Secondly is that the watermarked object retains the same properties of cover object. The algorithm shows resisting and withstanding against the most important attacks. Some of these include the lossy compression, blurring, resize and some types of Noise.*

Keywords: cover object, watermark object, distance bits, watermarked object, 2D DWT and attacks.

1. Introduction

The world of digital communication encounters nowadays an outburst of malicious interventions such as piracy, forgery, copying and so forth to the original version of document. This situation necessitates the design of reliable and robust systems to protect and preserve the integrity and safe passage of any form of data. Invisible watermarking technique is one of these systems that are available. This technique is widely used in different areas of our life such as wireless communication, internet, documentation, copyright, proprietorship, trade mark ™ and others. Generally, all these areas need to have an integrity system against smart and variant attacks [1, 2, 5].

The integrity system must include authorization, authentication, privacy, encryption and copyright policies. These policies can be entirely or partially watermarked in original version of any multimedia application that need to be maintained against any snoopers. Watermarking applications such as signature, trade mark, logo, biometrics like fingerprint, iris, voice and so on, are forming the main tools to achieve these policies.

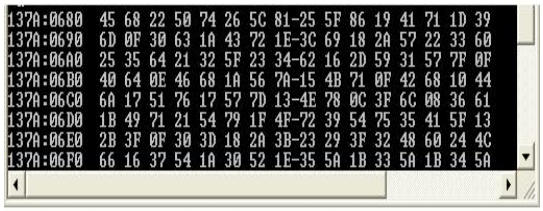
The robustness of the watermarking algorithm as proposed in this paper, aims to keep the properties of the watermarked object the same as that of the cover object, particularly with regards to keeping PSNR as high as possible, and 100% correlation. This leads to more withstandable and resistible behavior of an algorithm against the attacks. The challenge is to ensure that the watermarked object be perceptually indistinguishable from the cover object [3, 4].

2. Important properties of color image

In multimedia applications like color images, the properties of the file after the watermarking are considering an important concern. Any change in watermarked object size, dimensions or pixel color from that of the cover object means change in properties. These changes represent good parameters for others to suspect that there is an embedded data [1, 6].

This paper deals specifically with color images having the properties of 24 bits per pixel (8 bits for each primary color (Red, Green and Blue)). Each primary color has fixed range of 256 hexadecimal values as shown in Table 1.

Table 1Hexadecimal numbering representation of digital image read directly from main memory.



These allowable 256 hexadecimal numbers of each primary color can be read with 256 floating point numbers. Generally, each value is either 0 or multiples of 0.0039216. Table 2 illustrates the linear relationship between these two different numbering formats. Mathematically, the linear relationship can be modeled as follows:

$$Y(x) = 0.0039216*x, \quad 0 \le x \le 255.$$

Where ***Y(x)*** represents the function of the weights of each one of the three primary colors which are laminating the pixel, and ***x*** is a variable, and its boundary ranges between [0 255].

Table 2 Floating point representation

Hexadecimal values read in main memory	Equivalent floating point values
00h	0.0
01h	0.0039216
7Fh	0.5
AFh	0.68628
FFh	1.0

3. Direct embedding

The cover object used in this paper is 512*512*3 color image. Image's format can be BMP, JPG or PNG as shown in Figure 1. The watermark data may be an iconic image (the image may contain logo, signature, fingerprint, trade mark, serial number, and so on), text or both. Figure 2 shows an iconic image with dimension of 32*32*3 (1024 pixels) to be watermarked to cover object.

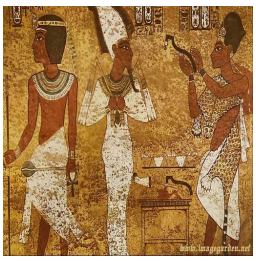


Figure 1 Original image (cover object)

Figure 2 Iconic image (watermark object)

The embedding process is implemented by dividing the pixel values of iconic image into nipples. Thereby, for 4 bits distance, each pixel consists of 6-nipples. The total number of watermark data is 6144 and their sixteen values are ranged between [1 16]. For 8 bits distance, each pixel consists of 3-bytes. The total number of watermark data is 3072 and their 256 values are ranged between [1 256].

To overcome changes in properties of watermarked files, an algorithm is proposed depending mainly upon the values of watermark data. These values can be considered as addresses to locate the embedding positions in cover object. These values are accumulated to get the next address. The difference in accumulated values of the watermark data can be thought of as distances among addresses of the cover object. This operation can be termed as Distance-Based Embeddor. The operation of this process is illustrated in Figure 3. and can be explained as follows: the value of the 1st watermark data points to the address of the 1st modified content. The 1st and 2nd watermark data are accumulated to get the 2nd address of the 2nd modified content and so forth. The distance between 1st address and 2nd address is equal to the value of 2nd watermark data. This accumulation goes on to the end of the last value of watermark data. The contents of positions which are addressed by the watermark data can be modified with a factor of ε to obtain the watermarked object. This factor is selected to be the smallest value (zero is not selected) among the values of color image of the cover object. In case of direct embedding, ε is selected to be equal to 0.0039216. This value has very little effect of distortion on the watermarked image. Figures 4a and 4b show the watermarked image using 4 bits and 8 bits distances, respectively. Thereby, the effect of uniquely distance-based distribution of watermark data in cover object helps in encryption.

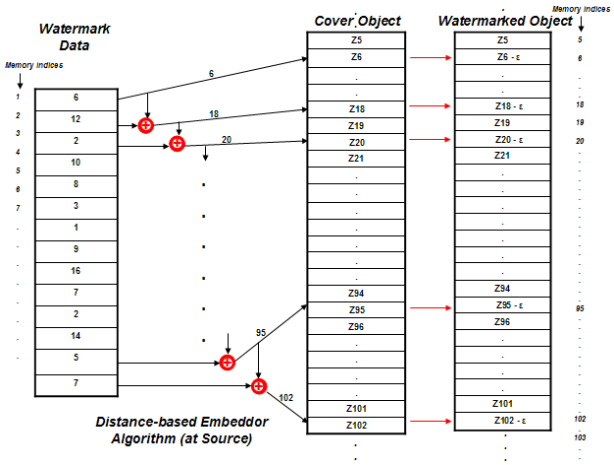


Figure 3 Illustrates the work of Distance-Based Embeddor

PSNR is apparently improved with an increase of distance bits. The reason is that for 4 bits distance, to embed 32*32 pixels, 6144 locations are required, while for 8 bits distance, only 3072 locations are required. It is obvious that the number of modified values of watermarked object when using 8 bits distance is less than 4 bits distance. For 4 bits distance, the maximum and minimum distance between any consecutive addresses is 16 and 1 location(s), respectively, and the size of image file must be at least 46594 bytes (sum the numbers of 4-bits 6144 values of iconic image) to totally embed an iconic image. For 8 bits distance, the maximum and minimum distance

between any consecutive addresses is 256 and 1 location(s), respectively, and the size of image file must be at least 401777 bytes (sum the numbers of 8-bits 3072 values of iconic image) to totally embed same iconic image. Consequently, different iconic image in Figure 2 gives different lengths. It is clear that for the same watermark object, the 8 bits distance needs large cover object size to embed all watermark data in comparison to 4 bits distance. This restriction plays an important role in deciding and selecting which properties of watermark object are appropriate and usable. For small size of cover object, grayish or less dimensional watermark object can be used.

(a) **(b)**

Figure 4 Shows watermarked image using direct distance-based embedding with CORR=100% (a) 4 bits, PSNR = 64.466 dB (b) 8 bits, PSNR=67.459 dB

4. Embedding using 2D DWT

The wavelet transform is suitable for the watermarking because it provides a good representation of the image data in terms of both spatial and frequency localization (multilevel (multiresolutional) independent information). The wavelet transform is used to decompose the image data into different frequency sub bands. Therefore, the wavelet transform is equivalent to computing the output of a band-pass filter bank specified by the wavelet coefficients. Accordingly, by "traveling" from the large scales toward the fine scales, one "zooms in" and arrives at more and more extra representations of the given signal [8, 9]. However, the original image can be transformed into four sub-images.

Firstly, the least significant byte of pixel's color (blue color) of the 512*512 color image is decomposed into four sub bands using 2D DWT technique LL1(approximate sub band), LH1 (horizontal sub band), HL1 (vertical sub band) and HH1 (diagonal sub band). Each sub band has dimension of 256*256 as shown in Figure 5. The blue color is better than green and red for watermark embedding. This behavior results from the fact that the human visual system (HVS) is subjectively less sensitive to this color [7]. This is the case even though the PSNR is nearly the same objectively in case of embedding in blue, green or red colors. That it worked actually in section 3. It is important to mention that the cover object is chosen where most values of blue color are zeros and small in comparison with red and green colors. This choice adds a type of challenge in testing the algorithm with worst cases.

Most energy of the primary color is concentrated in first decomposition (LL1). The remaining energy is distributed into the other three sub bands of the 2D DWT decompositions. The process of decompositions is also applied for red and green colors. Figure 6 illustrates the two level decompositions for the cover object shown in Figure 1. Four bits distance- based algorithm is applied to LH1 decomposition to embed an iconic image. Figure 7a shows the watermarked image after using 2D IDWT to LL1, HL1, HH1 and embedded LH1 decompositions. The red or green colors' decompositions can be used for watermark embedding. The process of primary colors' decompositions LH, HL and HH offers useful and protected areas for watermark embedding.

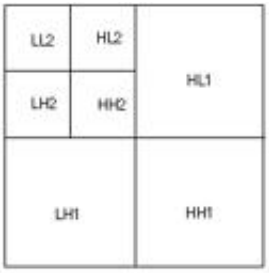


Figure 5 Two level 2D DWT sub bands

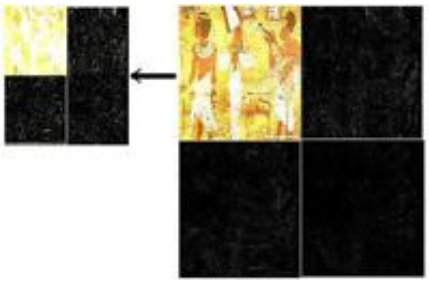


Figure 6 Two level image decompositions

Secondly, another test was carried out by taking the 2D DWT to the first decomposition of the previous 2D DWT. This process decomposes the energy of the previous first sub band (LL1) into another four sub bands (LL2, LH2, HL2 and HH2; each of these secondary sub bands has dimension of 128*128). The iconic image is embedded in the second LH2 sub band. Figure 7b shows the double level of 2D IDWT watermarked image. Using 2D DWT

increases the complexity of extracting an iconic image from watermarked image directly.

In case of single level and double level of 2D DWT embedding, the value of ε is chosen to be 0.0039216. As such, it is considered the basic component to build other values in same list. This value of ε is recommended to guarantee that the generated values of the watermarked image at different embeddings are within the allowable 256 values.

Figure 8 shows a nonlinear increasing of PSNR with an increasing of distance bits for direct embedding, and for single level and double level of 2D DWT embedding. It is worthy to note that Daubechies wavelet function (db4) is used throughout this work.

(a) **(b)**

Figure 7 Shows watermarked image using 4 bits distance-based 2D DWT (db4) with CORR=100% (a) single level, PSNR=63.9905 dB (b) double level, PSNR=57.776 dB

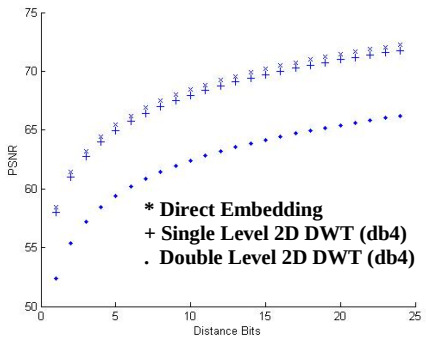


Figure 8 Relationship between Distance Bits and PSNR at different techniques of embedding

5. Some of attacking models

Table 3, 4, and 5 illustrate important results of attacking the watermarked object with some effective and popular attacks [5, 10]. The algorithm is tested by compressing the watermarked object to the levels where the size changes from 769 Kbyte to 60Kbyte. Also, some types of noise attacking are tested. The worst type is the Additive White Gaussian Noise (AWGN) where the extracted watermark image is strongly distorted. Blurring attack using 'Motion' filter type and geometric attack which is represented by 256*256 dimensional resize are applied on the watermarked object. In spite of all signal to noise ratio (PSNR) readings are low as shown in Table3, 4, and 5, and attacks' types have direct and visible effectiveness of distortion on the watermarked object. The proposed algorithm has the ability of high resilience of extracted watermark object regardless of what type of embedding technique is used. It is important to mention that all embeddings are implemented with 4 bits distance. The relevant results in tables are so closed to each other. This means that all embeddings are robust. Consequently and according to the PSNR readings, the double level 2D DWT is more withstandable than the other embeddings.

Table 3 Type of attack and extracted watermark image using direct embedding

Type of Attack	Extracted Watermark Image
JPG COMPRESSION PSNR = 21.9462 CORR = 0.9987 Compression Ratio = 12:1	
JPG COMPRESSION PSNR = 25.0581 CORR = 0.9996 Compression Ratio = 8:1	
GAUSSIAN NOISE Variance = 0.01 PSNR = 15.4580 CORR = 0.9888	
SALT & PEPPER NOISE Variance = 0.05 PSNR = 13,2429 CORR = 0.9144	
POISSON NOISE PSNR = 22.5470 CORR = 0.9991	
Blurring Attack 'Motion' Type PSNR =14,1552 CORR = 0.9653	
Resize Attack 512*512 to 256*256 PSNR = 16,6699 CORR = 0,9871	

Table 4 Type of attack and extracted watermark image using single level 2D DWT

JPG COMPRESSION PSNR = 21.9339 CORR = 0.9987 Compression Ratio = 12:1	
JPG COMPRESSION PSNR = 25.0382 CORR = 0.9996 Compression Ratio = 8:1	
GAUSSIAN NOISE Variance = 0.01 PSNR = 15.0743 CORR = 0.9868	
SALT & PEPPER NOISE Variance = 0.05 PSNR = 13,2502 CORR = 0.9146	
POISSON NOISE PSNR = 22.5186 CORR = 0.9992	
Blurring Attack 'Motion' Type PSNR =14,1531 CORR = 0.9654	
Resize Attack 512*512 to 256*256 PSNR = 16,6624 CORR = 0,9871	

Table 5 Type of attack and extracted watermark image using double level 2D DWT

JPG COMPRESSION PSNR = 21.9608 CORR = 0.9987 Compression Ratio = 12:1	
JPG COMPRESSION PSNR = 25.0863 CORR = 0.9996 Compression Ratio = 8:1	
GAUSSIAN NOISE Variance = 0.01 PSNR = 15.4647 CORR = 0.9888	
SALT & PEPPER NOISE Variance = 0.05 PSNR = 13,2508 CORR = 0.9144	
POISSON NOISE PSNR = 22.5568 CORR = 0.9992	
Blurring Attack 'Motion' Type PSNR =14,1596 CORR = 0.9654	
Resize Attack 512*512 to 256*256 PSNR = 16,6742 CORR = 0,9871	

6. Recovering process

The cover object must be available during the recovering process. Figure 8 illustrates the work of distance-based Extractor.

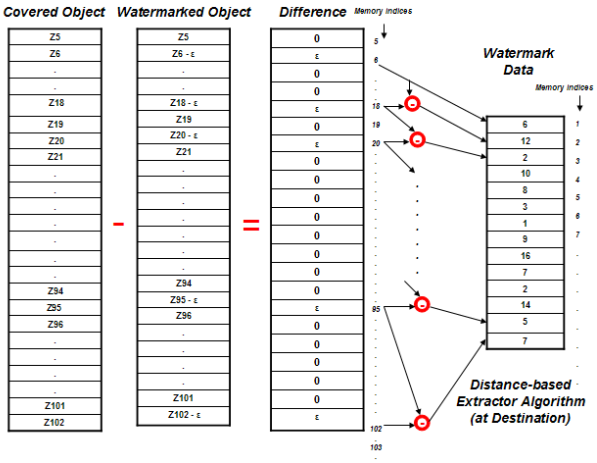


Figure 8 Illustrates the work of Distance-Based Extractor

The watermark data is extracted during the difference between the cover and watermarked images. The difference contains numbers of zeros and **Ɛs** in case of direct embedding or single level and double level of 2D DWT embedding. The nonzero values indicate the addresses that the modification has taken place. The difference between any consecutive addresses of nonzero content is recovering the data of the iconic image. The recovered data must be 6144 nipples for 4 bits distance embedding, 3072 bytes for 8 bits distance embedding. The direct embedding algorithm is directly implemented on the content of the cover image and the amount of distortion depends upon Ɛ and length of distance bits. While in distance-based 2D DWT embedding, in addition to Ɛ and length of distance bits, the amount of

distortion is affected by the order and level of wavelet selection.

7. Conclusion

This new approach (distance-based algorithm) of watermark embedding has many advantages. The most important advantage is that the n-bits distance-based algorithm shortens the impact of distortion on the cover object. Where n represents an integer number and is selected to be equal to 4 or 8 during the measurements. The relationship between the n-bits and distortion is inversely proportional. Consequently, the increasing of n-bits will increase the PSNR and maintain 100% correlation. This increases the withstandability and resistibility against the actual trials of attacks and the resilience of the watermark object can easily be recovered. Besides that the distribution of the watermark object over the cover object needs not the key for encryption the watermark data before embedding. This distribution depends on the unique pattern of the data of an iconic image. This, in turn, does not add any extra time which is required in case of using a security key to encrypt the watermark data before embedding. Accordingly, this decreases the processing time required in both embedding and extracting processes.

8. References

[1] Luigi Rosa, "DCT-Based Watermark Recovering without Resorting to the Uncorrupted Original Image," URL: http://www.advancedsourcecode.com, 2005.

[2] Bret Dunbar, "A Detailed Look at Steganographic Techniques and Their Use in an Open-System Environment," Sans Institute 2002.

[3] M. Kutter and F. A. Petitcolas, "A Fair Benchmark for Image Watermarking Systems." Security and Watermarking of Multimedia Content, SPIE-3657:226-239, 1999.

[4] C. Fei, Analysis and Design of Watermark-based Multimedia Authentication Systems. PhD Thesis, University of Toronto, Toronto, Ontario, Canada, 2006.

[5] S. P. Mohanty, P. Guturu, E. Kougianos, and N. Pati, "A Novel Invisible Color Image Watermarking Scheme using Image Adaptive Watermark Creation and Robust Insertion-Extraction", in Proceedings of the IEEE International Symposium on Multimedia (ISM), pp. in Press, 2006

[6] Watermark Factory Unregistered Version 2.0, URL:http://www.watermarkfactory.com, 2004.

[7] M. Kutter, F. Jordan, F. Bossen, "Digital Watermarking of Color Images using Amplitude Modulation." Journal of Electronic Imaging 7(2), PP. 326-332, April 1998.

[8] C. Sidney Burrus, Ramesh A. Gopinath, and Haitao Guo, "Introduction to Wavelets and Wavelet Transforms," Printice hall, 1998.

[9] G. Lekutai, "Adaptive Self-Tuning Neuro Wavelet Network Controllers", PhD dissertation, Virginia Polytechnic Institute and State University, Electrical Engineering Department, March, 1997.

[10] Michael E. Osadebey and Apostolos A. Georgakis,"Spread Spectrum Wavelet Watermarking System", Department of Applied Physics and Electronics, Umeå University, Sweden. ISSN: 1652-8441. December 26, 2005.