Properties of Digital Image Watermarking

Mohammad Abdullatif
Kulliyyah of Engineering, International Islamic University Malaysia, Malaysia
mohasalah86@gmail.com

Akram M. Zeki
Kulliyyah of Information & Communication Technology, International Islamic University Malaysia, Malaysia
akramzeki@iium.edu.my

Jalel Chebil
Kulliyyah of Engineering, International Islamic University Malaysia, Malaysia
jalel@iium.edu.my

Teddy Surya Gunawan
Kulliyyah of Engineering, International Islamic University Malaysia, Malaysia
tsgunawan@iium.edu.my

Abstract*— Digital image watermarking techniques have been developed widely in recent years to maintain the broadcasting media and content authentication, broadcast monitoring, copy control, and many other applications. Therefore, many studies have used digital image watermarking to solve these problem. This paper highlights digital image watermarking. It starts with a basic model of digital image watermarking, it discusses the main requirements and applications. Moreover, it reviews some of the techniques and algorithm used in image watermarking. In addition, digital image watermarking attacks are discussed. Lastly, Watermarking evaluation system is described.

Keywords: Digital Image Watermarking, Watermarking Model, Watermarking Attacks.

I. INTRODUCTION

Since the Internet has become very popular, and people can share whatever they want to share such as images, videos, documents, etc., there has been a need to protect publishing copyright. In addition, there has been also a significant demand for information security. For these reasons and other reasons, digital image watermarking has become very popular recent years as a good solution for these cases. Many researches have gone through this field to create new techniques, and to enhance current techniques as proper solutions for previous problems.

Digital image watermarking techniques stand on embedding a host image with information which is called watermark, then the watermarked image will be transmitted, and can be extracted at the receiver. There are two kinds of detection types at the receiver. The first type is called blind watermarking, because the detector doesn't need the original cover image to detect the watermark. The second type is called non-blind and it needs the original cover image to extract the watermark [1].

This paper is organized as following: Section 2 describes the basic model of digital image watermarking process. This is followed by Section 3 that explains the requirements of digital image watermarking. In Section 4, the main applications of digital image watermarking are presented. In Section 5, some of the techniques used in digital image watermarking are reviewed. In Section 6, watermarking attacks are discussed. Then watermarking evaluation system is discussed in Section 7. Section 8 concludes the paper.

II. BASIC MODEL OF DIGITAL IMAGE WATERMARKING

The basic model of digital image watermarking consists of two parts; the first part is the watermark embedding process which shown in Figure 1, and the second part is the watermark detection process which shown in Figure 2.

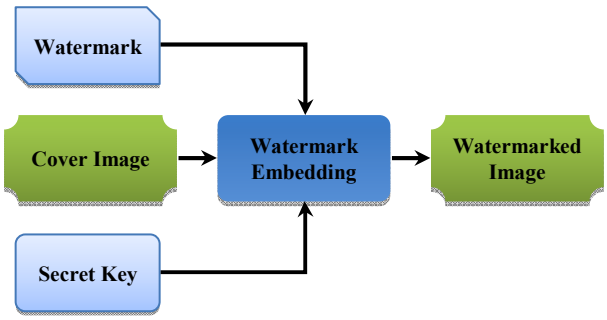

Figure 1 Watermark Embedding

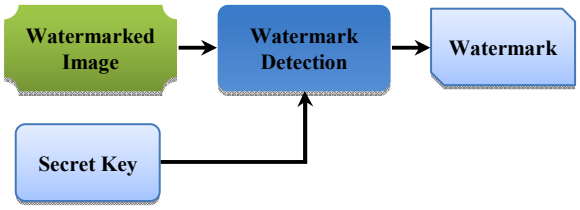

Figure 2 Watermark Detection

In Figure 1, which represents sender, the *Watermark* is embedded into the *Cover Image* with the *Secret Key* that ensures the security of watermarking process. The output is the Watermarked Image. In Figure 2, at the receiver side, the *detector* detects the watermark from the

Watermarked Image by using the *Secret Key* to recover the *Watermark* [2].

III. Requirements of Digital Image Watermarking

Digital image watermarking concerns to solve some issues properly, thus, this paper highlights the main requirements of watermarked image as following:

A. Robustness:

The robustness is the ability of detecting the watermark after some signal processing modification such as spatial filtering, scanning and printing, lossy compression, translation, scaling, and rotation [1], and other operations like digital to analog (D/A), analog to digital (A/D) conversions, cutting, image enhancement [3]. In addition, not all watermarking algorithms have the same level of robustness, Some techniques are robust against some manipulation operations, however, they fail against other stronger attacks [4]. Moreover, it's not always desirable for watermark to be robust, in some cases; it's desired for the watermark to be fragile [1]. Therefore, the robustness can be classified as following:

- Robust: The watermark is designed to be able to survive against incidental and intentional attacks [5]. This kind of watermarking can be used in broadcast monitoring, copyright protection, fingerprinting, and copy control [6].
- Fragile: The watermark in this type is designed to be destroyed at any kind of modification, to detect any illegal manipulation, even slight changes, involving incidental and intentional attacks. Fragile watermarks are mainly used in content authentication and integrity verification. They use *blind* detection type [6], as it will be discussed in *Detection Types*. In addition, the implementation of fragile techniques is easier than the implementation of robust ones [7].
- Semi-fragile: The watermark in this type is robust against incidental modifications, but fragile against malicious attacks [8]. And it is used for image authentication [9].

B. Imperceptibility:

Imperceptibility (also known as *Invisibility* and *Fidelity*) is the most significant requirement in watermarking system, and it refers to the perceptual similarity between the original image before watermarking process and the watermarked image [1]. In other words, the watermarked image should look similar to the original image, and the watermark must be invisible in spite of occurrence of small degradation in image contrast or brightness. However, the challenge is that imperceptibility could be achieved, but the robustness and the capacity will be reduced, and vice versa, imperceptibility may be sacrificed by increasing the robustness and the capacity [4]. Moreover, the watermark not always desired to be invisible, sometimes, it is preferred to have visible watermark into the image [6].

C. Capacity:

Capacity (also known as Payload) refers to the number of bits embedded into the image. The capacity of an image could be different according to the application that watermark is designed for [1]. Moreover, studying the capacity of the image can show us the limit of watermark information that would be embedded and at the same time satisfying the imperceptibility and robustness [4].

D. Security:

Security is the ability to resist against intentional attacks. These attacks intended to change the purpose of embedding the watermark. Attacks types can be divided into three main categories: unauthorized removal, unauthorized embedding, and unauthorized detection [1]. According to the specific usage of watermarking, the specific feature should be available in the watermark to resist the attacks. Therefore, for unauthorized removal, the watermark should be robust and not to be removed, and for unauthorized embedding (also known as forgery), the watermark should be fragile or semi fragile to detect any modification. Lastly, for unauthorized detection, it should be imperceptible watermark [10].

E. Low Complexity:

The cost is the reason behind studying the complexity, so it should be at a reasonable cost [5]. It describes the economics of using watermark embedders and detectors, because it can be very complicated and depends on business model that is used. The main two issues of complexity are the speed of embedding and detection, and the number of embedders and detectors [1].

IV. Applications of Digital Image Watermarking

A. Copyright Protection:

The copyright information can be embedded as a watermark into the new production. Once there is a dispute on the ownership, the watermark can be extracted to provide the evidence of who is the owner of this product [6].

B. Content Authentication:

The watermark is embedded to detect if the image has been modified or not, this process can be used for authentication [2].

C. Broadcast Monitoring:

This type of monitoring is used especially in the advertisements to make sure that the content broadcasted as the contract between the advertisement company and the customer [2].

D. Owner Identification:

To achieve owner identification, there was a traditional form for intellectual ownership verification which was a visual mark. However, nowadays, this is easily overcome by the use of some softwares that modify images. For example, the images with the copyright registration symbol *c* which have this mark is removed by specialized software. To solve this problem, invisible watermarks are used in order to overcome the problem [8].

E. Fingerprinting:

The main purpose of fingerprinting is to protect customers. If someone got a legal copy of a product, but redistributed illegally, fingerprinting can prevent this [6]. This can be achieved by tracing the whole transaction by embedding unique robust watermark for each recipient. Thus, the owner can identify who redistributed this product by extracting the watermark from the illegal copy [4].

F. Copy Control:

The watermark contains owner data and specifies the corresponding amount of copies allowed. This presupposes hardware and software for updating the watermark whenever it has been used. It also provides copy tracking for unauthorized distribution since the owner of data is embedded in the watermark [8].

G. Medical Applications:

Image watermarking can be used in medical images for several purposes. It's used to protect the patient's information from unauthorized people. In addition, it can be used for authentication if the patient lost the image. Moreover, it is needed to protect the copyright of the medical image [11]. For example, mammograms contain diagnostic information which can be used for early detection of breast cancer diseases and breast abnormality. Protection and authentication of such images are now becoming increasingly very significant in telemedicine field where images are easily distributed over the internet. For mammogram medical image, it should be sure that embedding watermark does not affect the diagnostic information of the mammogram [12].

V. DIGITAL IMAGE WATERMARKING TECHNIQUES

A. Spatial Domain

This type of embedding relies on that information is inserted directly into the image [4]. There are many algorithms and techniques that use spatial domain such as: and Least Significant Bit (LSB), Intermediate Significant Bit (ISB), Patchwork, etc.

1. Least Significant Bit (LSB)

LSB algorithm is considered as the simplest approach, because the least significant bits carry less relevant information and their effect does not cause visible changes [8]. And this technique is used for simple operation to embed information into a host image. The idea behind LSB is very simple; the host image pixels are changed by no of bits of the secret message. Despite of the number was embedded into the first 8 bytes of the grid, the 1 to 4 least bits needed to be modified according to the embedded secret message. On the average, only half of the bits in an image will need to be changed to hide a secret message using a host image. Because the quality of the Watermarked image is low, less than over the 4 least significant bits, changing the LSB of a pixel results in small changes in the intensity of the colors. These changes cannot be recognized by the human visibility system. However, a passive attacker can easily extract the changed bits, because it has performed very simple operation. For instance, Figure 3 shows the 4-bit LSB. In Figure 3, the pixel value of the cover image is 150 (10010110) and the secret data are 1100. Then the changed pixel value of the cover is 156 (10011100). LSB can store 4-bit in each pixel. If the cover image size is 256 x 256 pixel image, it can thus store a total amount of 65,536 bits or 8,192 bytes of embedded data [13].

Pixel value	1	0	0	1	0	1	1	0
Secret message					1	1	0	0
Watermarked pixel	1	0	0	1	1	1	0	0

Figure 3 an example of 1-bit LSB digital image watermarking

Theoretically, the worst case in the simple LSB substitution method occurs when the watermark bit and original bit are different all the time. In other words, the difference between the original pixel and watermarked pixel is (2k-1), where k is the level of different bit-planes.

The PSNR for the worst case of embedding one bit within k bit-plane and embedding the watermark within k-rightmost of host image are presented in Table 1, in addition to most common distribution embedding for k bit-plane. Notice that the worst case of k-rightmost bit-plane can be obtained only when they are all zeros and the embedded bits are ones or the original bits are ones and the embedded bits are zeros.

Table 1 shows three PSNR values for different k bit-planes. The first is the worst case by embedding in the k bit-plane only. The second is for embedding the watermark into the k bit-plane, only for the most common case and the third is for embedding the worst case in the k-rightmost bit-planes. It could be seen that the image quality of the watermarked image had been drastically degraded when k > 4, in case of using one bit-plane only for hosting the watermark. In case of k right-most bit-

planes, the image quality of the watermarked image was drastically degraded when k > 3.

Table 1: The PSNR values of the worst embedding case and the most common one for different bit-planes by a simple LSB substitution

k	PSNR (Worst case in k bit-plane only)	PSNR (Most common case in k bit-plane only)	PSNR (Worst case in k-rightmost bit-planes)
1-LSB	48.1308	51.1411	48.13
2	42.1102	45.1205	38.59
3	36.0896	39.0999	31.23
4	30.0690	33.0793	24.61
5	24.0484	27.0587	18.30
6	18.0278	21.0381	12.1440
7	12.0072	15.0175	6.0547
8-MSB	5.9866	8.9969	0

2. *Intermediate Significant Bit (ISB)*

Although embedding watermark, within LSB gives the best image quality, embedding within the Most Significant Bit MSB gives the worst image quality. When starting from the MSB towards the LSB, embedding will improve the quality of watermarked image [14]. Recently, [15] improved LSB to a new technique called intermediate significant bit (ISB). In the new method, the watermark pixel's location has been tested according to the range of each bit-plane. Thus, if the location of watermarked pixel is in the middle of the range, any effect on the pixel by attacks will make it difficult to move the selected bit to other range. Meanwhile, if the pixel value is located at the edges of the ranges, any small change caused by attacks will move the pixel from a range to other range, and the watermark cannot be extracted. [16] tried to find the best pixel value, in between the middle and the edge of the range that can protect the watermark object from several kinds of attacks, and at the same time keep the watermarked image at the minimum distortion. This was achieved by positioning the watermarked pixel away from the edge of the range, all possible positions of pixel between the middle and the edge of the range were tested to find the best pixel value (threshold value), which was found to be at the 4^{th} bit-plane with a bias value = 6 (the bias value is the distance between the position of the watermarked pixel and the edge of the range) [16].

3. *Patchwork*

Patchwork algorithm inserts the information into the brightness of pixels by changing the statistical properties of the image. Patchwork selects randomly number of pairs of pixel points (a_i, b_i), and the difference between two randomly selected pixels equals zero centered at Gaussian distribution. Then the brightness value of the pixel point a_i increases by 1, the brightness value of pixel point b_i reduces by 1. In this case, the distribution center will be changed, but the average brightness of the image will not be changed. For the goal of resisting the attack of loss compression and filtering process, it extends the pixels to pairs of blocks; thus, the brightness of pixels in one block will be increased, while the brightness of pixels in corresponding block will be reduced [17].

B. *Transform Domain*

This type of embedding uses the transform coefficients to embed the watermark. Moreover, transform domain techniques are very robust against attacks, because the watermark is spread in whole image [4]. The main techniques used in transform domain are: Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT), and many other techniques.

1. *Discrete Cosine Transform (DCT)*

DCT is widely used in digital image watermarking since it has strong robustness. In addition, many frequency coefficients are obtained from DCT, such as single direct current DC coefficient, low frequency coefficients, mid frequency coefficients, and high frequency coefficients. By the different characters of these coefficients, we can obtain different effects upon digital watermarking system. Moreover, JPEG standard and Watson visual model are based on DCT with block size 8×8, which is commonly used in image watermarking.

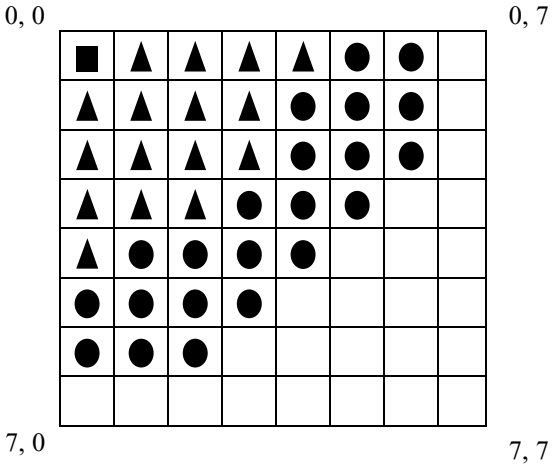

Figure 4 Coefficients of block DCT

Figure 4 shows various DCT coefficients. The coefficient in the coordinate (0,0) which is represented by a square is the DC coefficient, low frequency coefficients are represented by triangles, mid frequency coefficients are represented by circles, and the rest are the high frequency coefficients [18]. Despite of DCT watermarking techniques have strong robustness; they also have their own drawbacks, such as low watermarking capacity [17]. More data can be embedded when low frequency

coefficients are used compared to DC coefficient. On the other hand, DC has more robust than low frequency coefficients [18].

2. Discrete Wavelet Transform (DWT)

Wavelet Transform has been used widely since it has been adopted in the established image coding standard JPEG 2000 [2], and it produce considerably better quality for decoded image than JPEG. The main advantage that DWT has over Fourier transforms is temporal resolution. It captures both location and frequency information .The basic idea of DWT is to separate frequency detail, which is multi-resolution decomposition. One time of decomposition can divide the image to four sub images at a quarter sizes. They are a low frequency approximate sub image, and three horizontal, vertical, and diagonal direction high frequency details sub images [19].

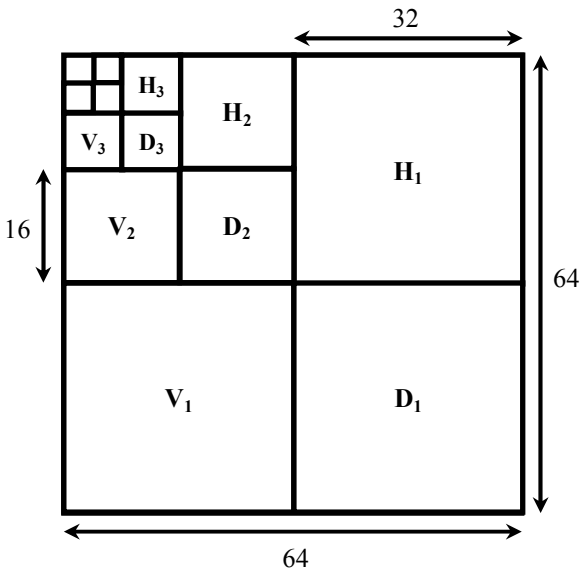

Figure 5 Four level DWT

Figure 5 is an example diagram of four-level DWT decomposition. In the wavelet transform domain, high frequency parts represent detailed information of image's edge, contour and texture and so on. It's not easy to detect the watermark in these places as people are not easily able to recognize it. But after processing or attacking, it doesn't have good stability. Most energy of image is centralized in low frequency. Low frequency coefficients are nearly not changed by common attacks so that watermarking information embedded in low frequency coefficients has better robustness [19].

VI. Watermark Attacks

Digital image watermarking attacks can be classified to intentional attacks and non-intentional attacks. An attack succeeds in overcome a watermarking scheme if it weakens the watermark less than acceptable limits. On the other hand, recall the differentiation between achieving robustness and imperceptibility at the same time, it should be a balance to achieve them together. However, this paper highlights the attacks that affect the robustness directly, it highlights some common attacks such as JPEG compression attack, Noise, and Geometric attacks. First, JPEG is a standard compression technique, and it reduces the size of images for the goals of storage and transmission. As the compression rate increases, the quality of the image decreases. Second, Noise attacks are the data that are not part of the original image which caused by other sources. There are many types of noise such as Gaussian noise, and blurring noise [20]. Lastly, Geometric attack is a set of parameters that can be applied on the image. There are many types of geometric attacks such as rotation, cropping, and other transformations [21].

VII. The Evaluation System of Watermarking Technology

The objectives of using image watermarking set several requirements on the algorithm. There are some functionality that are used to evaluate the image watermarking system. The basic functionalities contain imperceptibility, robustness, capacity, speed, and security. A good evaluation has to provide a certain level of assurance for all the selected requirements. Therefore, there are number of levels of assurance for each requirement to assess this functionality separately. Moreover, some criteria are assigned for each level of the particular functionality. However, levels number of assurance cannot be selected accurately, and large number of them makes the evaluation so complicated and unusable for some purposes [22].

VIII. Conclusion

This paper reviewed the latest research work done on digital image watermarking. It presented the basic model of digital image watermarking for embedding and detection. Next, it mentioned the requirements of any digital image watermarking system. Then it listed some of the applications of digital image watermarking. Next, it showed the most significant techniques in both domains spatial domain and frequency domain. Then it mentioned the common attacks of digital image watermarking. Finally, it highlighted the evaluation system of watermarking technology.

References

[1] M. L. M. Ingemar J. Cox, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker, *Digital Watermarking and Steganography*: Morgan Kaufmann Publishers, 2008.

[2] Y. Yusof and O. O. Khalifa, "Digital watermarking for digital images using wavelet transform," in *Telecommunications and Malaysia International Conference on Communications, 2007. ICT-MICC 2007. IEEE International Conference on*, 2007, pp. 665-669.

[3] Z. Yanqun, "Digital Watermarking Technology: A Review," in *Future Computer and Communication, 2009. FCC '09. International Conference on*, 2009, pp. 250-252.

[4] R. F. Olanrewaju, "Development of Intelligent Digital Watermarking via Safe Region," PHD, Electrical and Computer Engineering, International Islamic University Malaysia, Kulliyyah of Engineering, 2011.

[5] J.-S. Pan, H.-C. Huang, and l. C. Jain, Eds., *Intelligent Watermarking Techniques* (Series on Innovative Intelligence. World Scientific, 2004, p.^pp. Pages.

[6] L. Jian and H. Xiangjian, "A Review Study on Digital Watermarking," in *Information and Communication Technologies, 2005. ICICT 2005. First International Conference on*, 2005, pp. 337-341.

[7] N. Cvejic, "Algorithms for Audio Watermarking and Steganography," Department of Electrical and Information Engineering, University of Oulu, 2004.

[8] A. G. Charles Fung, Walter Godoy Junior, "A Review Study on Image Digital Watermarking," presented at the The Tenth International Conference on Networks, St. Maarten, The Netherlands Antilles, 2011.

[9] S. Jun and M. S. Alam, "Fragility and Robustness of Binary-Phase-Only-Filter-Based Fragile/Semifragile Digital Image Watermarking," *Instrumentation and Measurement, IEEE Transactions on,* vol. 57, pp. 595-606, 2008.

[10] C. De Vleeschouwer, J. F. Delaigle, and B. Macq, "Invisibility and application functionalities in perceptual watermarking an overview," *Proceedings of the IEEE,* vol. 90, pp. 64-77, 2002.

[11] A. M. Zeki, A. A. Manaf, C. F. M. Foozy, and S. S. Mahmod, "A Watermarking Authentication System for Medical Images," presented at the World Congress on Engineering and Technology (CET 2011), Shanghai, China, 2011.

[12] R. F. Olanrewaju, O. O. Khalifa, A.-H. Hashim, A. M. Zeki, and A. A. Aburas, "Forgery Detection in Medical Images Using Complex Valued Neural Network (CVNN)," *Australian Journal of Basic and Applied Sciences,* 2011.

[13] A. Bamatraf, R. Ibrahim, and M. N. B. M. Salleh, "Digital watermarking algorithm using LSB," in *Computer Applications and Industrial Electronics (ICCAIE), 2010 International Conference on*, 2010, pp. 155-159.

[14] A. M. Zeki, A. A. Manaf, and M. Zamani, "Bit-Plane Model: Theory and Implementation," in *Engineering Conference (EnCon)* 2010.

[15] A. M. Zeki and A. Abdul Manaf, "A novel digital watermarking technique based on ISB (Intermediate Significant Bit)," *World Academy of Science, Engineering and Technology,* vol. 50, pp. 989-996, 2009.

[16] A. M. Zeki, A. A. Manaf, and S. a. S. Mahmod, "Analysis of ISB watermarking model: block based methods vs embedding repetition methods," presented at the Proceedings of the 9th International Conference on Advances in Mobile Computing and Multimedia, Ho Chi Minh City, Vietnam, 2011.

[17] Z. Jiang Yong, L. Dong Hong, L. Jiang Zeng, and J. Miao, "A DCT-BASED Digital Watermarking Algorithm for Image," in *Industrial Control and Electronics Engineering (ICICEE), 2012 International Conference on*, 2012, pp. 1217-1220.

[18] X. Jun and W. Ying, "Toward a Better Understanding of DCT Coefficients in Watermarking," in *Computational Intelligence and Industrial Application, 2008. PACIIA '08. Pacific-Asia Workshop on*, 2008, pp. 206-209.

[19] R. Dubolia, R. Singh, S. S. Bhadoria, and R. Gupta, "Digital Image Watermarking by Using Discrete Wavelet Transform and Discrete Cosine Transform and Comparison Based on PSNR," in *Communication Systems and Network Technologies (CSNT), 2011 International Conference on*, 2011, pp. 593-596.

[20] O. O. Khalifa, Y. binti Yusof, A. H. Abdalla, and R. F. Olanrewaju, "State-of-the-art digital watermarking attacks," in *Computer and Communication Engineering (ICCCE), 2012 International Conference on*, 2012, pp. 744-750.

[21] V. Licks and R. Jordan, "Geometric attacks on image watermarking systems," *MultiMedia, IEEE,* vol. 12, pp. 68-78, 2005.

[22] F. A. P. Petitcolas, "Watermarking Schemes Evaluation," *Signal Processing Magazine, IEEE,* vol. 17, pp. 58-64, 2000.