

Digital Image Watermarking Using Different Levels of Intermediate Significant Bits with Zig-zag Embedding Approach

Ali Sharifara

*Dept. of Software engineering, faculty of computing
UTM – Malaysia – Skudai 81310*

a.sharifara@gmail.com

Ghazali Bin Sulong

*Dept. of Software engineering, faculty of computing
UTM – Malaysia – Skudai 81310*

ghazali@spaceutm.edu.my

Mehran Ranjbar Seraydashti

*Dept. of Software engineering, faculty of computing
UTM – Malaysia – Skudai 81310*

rsmehran2@live.utm.my

Abstract

The rapid growths of computer technologies have been increased over the last half century in terms of amount and complexity of data. Broadcasting of digital contents on the networks (especially Internet) has become more important and access to the data also has become much easier than before. Digital watermarking techniques are used to protect the copyrights of multimedia data by embedding secret information inside them. For example, embedding watermark in images, audios, and videos. Digital Image watermarking also has been using to detect original images against forged images by embedding an evidence of the owner of the digital image. Imperceptibility, on the other hand, is one of the problems in digital image watermarking which a repeated method in different bit planes of cover image has been presented to improve the imperceptibility of watermarking in both embedding and extracting processes. Moreover, embedding process aims to embed watermark in different bit planes by using a non-sequential method to improve security of image rather than simple sequential embedding.

Keywords: Digital Image Watermarking, Invisible Watermarking, Imperceptibility in Watermarking, Copyright Protection, Intermediate Significant Bits (ISB).

1. INTRODUCTION

Over the last half century the pace of change in the digital technologies has been widely increased. Digital images as one of the digital technologies also have been replaced with the analog images. Moreover, Internet also has become one of the most important tools to transfer digital images from one part to other parts of the world. For this reason, the security of digital documents became a challenging concern and digital image watermarking as a solution is use to decrease the number of digital forged documents.

There are lots of digital images on the Internet without having watermark which can be downloaded and modified by anyone illegally [1]. Furthermore, the ownership of the image cannot be traced without the watermarking [2]. Digital watermarking provides a solution in order to identify the owner of the digital images [3]. It has also been presented for purposes such as: copyright protection, data authentication, fingerprint, medical applications, and broadcast monitoring [4]. Image watermarking is the process of embedding an image into a host image [5]. For Instance, watermarks are embedded in bank cheque for preventing forgery. Consequently, unauthorized modification of data is the concern of researchers about copyright of documents and numerous image watermarking methods, which have been proposed with different

complexity and efficiency levels so far. Also all of image watermarking methods aimed to set up a balance between the quality and the robustness of the watermarked images.

One of the most important aspects about the digital image watermarking is to improve the robustness of the watermarked image [6]. Robustness is related to the ability of recovering the watermark after performing various processing attacks on watermarked image. The robustness must be sufficient to handle any kind of attacks occur. The watermarking scheme should be able to protect the watermark against any possible signal processing operations.

2. WHAT IS WATERMARKING

The growth of the Internet over the last several years has identified the techniques in order to protect the digital documents in the digital world [7]. Also the Internet has made it easy to distribute the digital documents such as images, video, and audio [8]. Hence, without having the powerful techniques for protecting the digital documents, it is impossible to identify the genuine owner and the plagiarist.

Therefore, the digital watermarking is one of the proper solutions to protect copyright of the digital documents against forgers. By using watermarking in digital documents, we can reduce the misusing against the documents such as Will, Cheque and etc. For instance, in the figure 1, an analog watermarking has been used to protect money against forgers.



FIGURE 1: Example of Analog Watermarking.

Unlike the analog images, all of the images on the Internet are provided as a digital content. Therefore, a desirable technique for protecting copyright is needed. Digital watermarking can authenticate the legal copyright and that cannot be removed or manipulated easily by forgers without having the secure key or other security restrictions. For instance, a duplication of a cheque can decrease confidence in its authenticity. For this reason, watermarks are employed in currencies to reduce the risk of forgery. However, the watermark technique is not the only technique that has been using for preventing forged and illegal uses.

2.1 Proposed Method

Least Significant Bit (LSB) is one of the first techniques for the watermarking purpose and it uses the lowest bit plane of image [9]. It can modify bits of both host and watermark images to embed the given watermark. The basic idea behind this technique is the substitution of the lowest bit plane of the host image with the watermark's bits. In other words, in the spatial domain, the watermark is embedded directly into the host image by altering the pixel values [10].

Although, LSB is extremely easy in term of implementation, it is difficult to detect watermark easily [11]. However, this method is imperceptible and there is no significant difference between watermarked image and original image, but it is not robustness enough to protect the authority of watermarked images. This means, in the spatial domain, embedding capacity can be large, but the watermark could be easily found by unauthorized forgers. The main primary concept of Most

Significant Bit (MSB) is the same as LSB that we have described. The only difference between them is that, LSB uses the least significant bit, meanwhile in the MSB is completely different and it uses most significant bits, instead.

When we can say that a watermark method is robust whereby the watermarked image suffers from different attacks and the embedded image (Watermark) still can be extracted from the watermarked image [12]. In other words, the attacks must not have any effects in the extraction process. For example, when a watermarked image is rotated, the algorithm still must identify the watermark that we have embedded inside the cover image and extract it as well.

2.2 The best quality of image

There is no doubt that the quality of the watermarked image is the most significant parameter in all invisible methods [13]. In all invisible watermarking methods, the watermark must be embedded with having the least effect on the quality of the host data. In order to improve the quality of the watermarked image, beside the security, an Intermediate Significant Bit (ISB) method has been presented. This means that only some bit(s) – between bit 2 and bit 7 – will be changed to guarantee the quality of watermarked image which will not have any effect on other bits.

2.3 The best robustness

Robustness as another concern in watermarking also must be improved [14]. In this research, the goal is achieved by repeating the embedded bits of watermark for certain times. This idea has tried to make the algorithm more robust against attacks. Hence, the watermark is encoded into main signals T times. For instance, in this case we have considered $T=3$ and image is divided into blocks with size of 3 pixels, moreover, all of the values of each block should be the same as it is demonstrated in the figure 2.

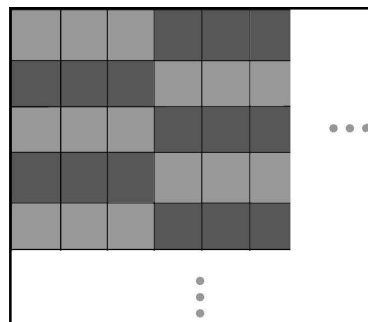


FIGURE 2: Divided Cover Image Into Blocks.

To clarify, figure 3 depicts how one pixel of watermark is embedded into the cover image; by this assumption that the first pixel of watermark contains (11011101), the pattern of embedding is sequential, and each bit of the watermark image is repeated into the cover image by three times. Figure 3 shows the result for one pixel of the watermarked image.

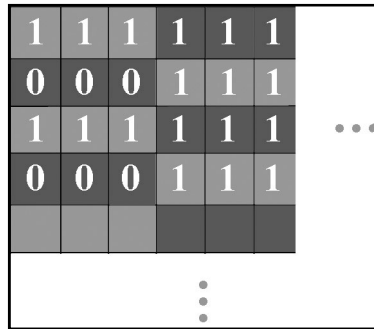


FIGURE 3: Repeating Bits in Each Block.

Extracting process must also be done in order to reverse this process. This procedure protects the watermark against attacks and it can decrease the risk of losing bits that can be damaged by the attacks. This process verifies the majority of bits while extracting watermark from the host image is to figure out the value of the watermark. In other words, the algorithms read all three bits for one pixel and makes decision between them. For example, if $T=3$, (000) represents 0, the (101) depicts 1, the (001) represents 0 and so on. To improve the robustness of the watermarked image, one bit in each pixel can be embedded in a block of pixels instead of embedding in only one pixel. This method has some advantages and disadvantages as well. The most important disadvantage of this method is the decreasing of the size of the watermark data which can be embedded in the host image. On the other hand, this approach makes an acceptable robustness by increasing the size of each block. Moreover, each block can be divided into 3, 5, 7, and 9 pixels as can be seen from the figure 4.

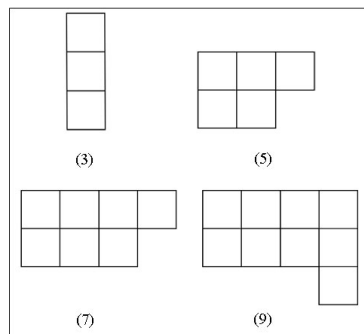


FIGURE 4: Repeating Bits in Each Block.

Beside the improvement of robustness in the watermarking system, other parameters also need to be improved such as security and capacity of image which can hide the information inside. Hence, a few steps are required to be developed which can provide guarantee that the proposed method is more robust and secure as well. Security beside the robustness is also another important point which may help to cut-off the attacks of malicious users. It is important to note that all of these stages can be executed separately. In the following section more details have been discussed.

2.4 Security in Watermarking

Security is a vital parameter in the watermarking system which must be considered as well [15]. The main aim of the attack in terms of security is to obtain the secret key of encoding process as well as decoding [16]. This means a strategy must be used to protect the watermark against malicious users and this strategy must be hidden. In other words, the watermark must be secured enough to be protected from the people those do not have the right to modify or manipulate the

watermarked image. In addition, the security in watermarking is represented same as security techniques which have been used in encryption methods [15].

2.4.1 Zig-Zag embedding matrix

To improve the security of watermarked image, a non-sequential algorithm is needed. A Zig-zag array is a square collection of the first N^2 integers and the numbers increase sequentially as can be seen from the figure 5. Therefore, the watermark pixels are not sequential and the watermark cannot be easily extracted by unauthorized users [17]. Beside, Zig-Zag embedding method we have used a secret key to guarantee through which our embedding method is secure enough.

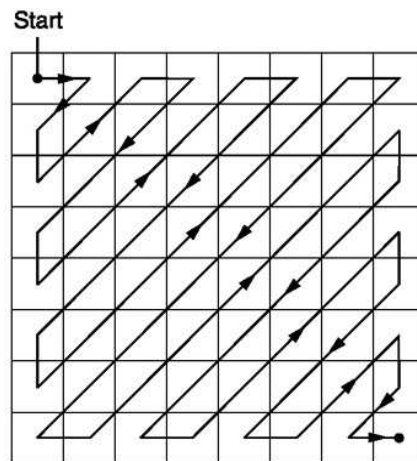


FIGURE 5: Zig-Zag Embedding Matrix [17].

2.5 The chosen attacks

Some attacks which might target the images and make effects on them. Some of them are provided. Such attacks include: Gaussian filter, Speckle noise, Salt and Pepper, Passion, and Blurring.

2.6 Experimental data analysis

By using two techniques, which have been mentioned above, for improving robustness and security, we have come up with results provided in the table 1. The result illustrates PSNR for different bit planes in proposed method.

Bit Planes	PSNR	Bit Planes	PSNR
1,2,3	45.7101	3,4,5	33.2965
1,3,4	39.8263	3,5,6	31.7147
2,3,4	39.6664	4,5,6	31.3294
2,4,5	33.4402	5,6,7	30.1412

Table 1: Different Bit Planes with Their PSNR Values of Proposed Method.

In the Table 2, some selected methods have been compared with one group of bit planes in the proposed method. As it can be seen from the table 2, the proposed method has the best quality among others after embedding the watermark.

Methods	PSNR
Proposed Method	45.71
HPDM	36.42
ST-SCS	36.42
color-based-encoding	30.48
Side match method	41.22
PVD	41.79
Conventional LSB	31.71
DCT	31.847
Vulnerability of PVD	45.1

Table 2: Comparison Between Different Methods [19].

2.7 Extracted Watermark after performing selected attacks

As it can be inferred from the table 2, the proposed method is more robust in comparison with conventional LSB and MSB methods. Nevertheless, most of the image attacks tend to destroy low bits (1, 2, and 3), but the proposed method can extract the watermark after the attacks by acceptable percentage of healthy pixels in the watermark even in the low bit-planes [18]. Surprisingly, as can be seen from the result of proposed method, the average PSNR in all of the 8 layers are approximately same by over 30 db. Hence, the above result proves that the watermark can embed into all bit-planes of cover image regardless of the visibility of the watermark.

The below figures also provides information about the PSNR of the watermark after extraction for proposed method compared to the conventional LSB method. The x-axis indicates 8 bit-planes and the PSNR is indicates on y-axis.

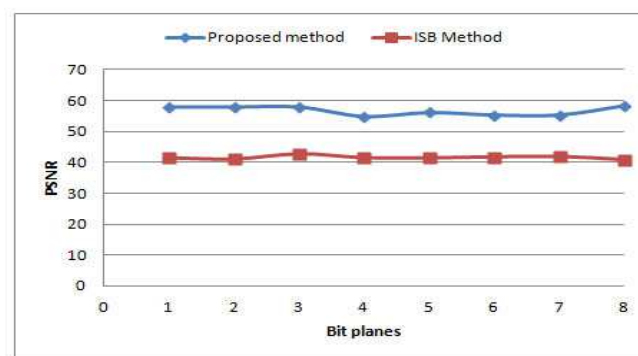


FIGURE 6: Applied Salt and Pepper Attacks for Both Proposed and Conventional LSB Method.

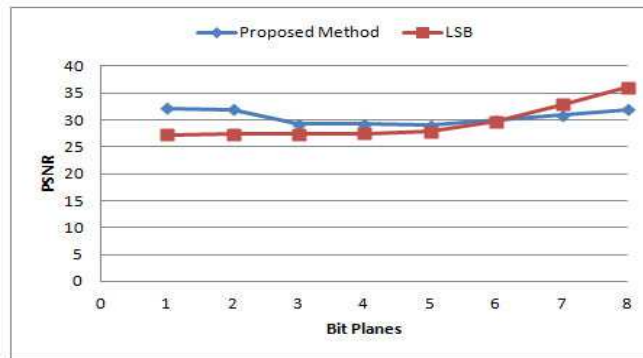


FIGURE 7: Applied Blurring Attacks for Both Proposed and Conventional LSB Method.

As can be seen from the figure 6 and 7, the selected attacks do not have any significant effect on the watermark and can be extracted by high PSNR (Peak signal-to-noise ratio). Furthermore, other two mentioned attacks also have less effect on the watermark image after extraction in all different 8 bit planes. Table 3 and 4 show the watermark images after extracting in both proposed method and the conventional LSB, respectively.

Bit- planes	Salt and Pepper	Gaussian	Speckle	Poisson	Blurring
1,2,3					
PSNR	57.8942	35.1767	35.1767	35.1211	35.1767
1,3,4					
PSNR	58.0278	33.1767	35.1767	31.9604	30.2204
2,3,4					
PSNR	58.0448	29.2292	28.8208	29.1933	28.9032
2,4,5					
PSNR	54.8024	29.1511	29.0914	29.2553	28.7651
3,4,5					
PSNR	57.1409	29.0285	29.7285	28.9973	28.2251
3,5,6					
PSNR	55.2978	28.9489	29.7255	29.9973	29.0686
4,5,6					
PSNR	55.2978	28.8878	31.5728	30.5728	28.9786

Table 3: Extracted Watermark After Attack in Proposed Method.

The result proves that the watermark can embed into all bit-planes of the cover image regardless of the visibility of the watermark. We also have performed similar tests to other images and we have achieved the same results.









































Bit- Planes	Salt and Pepper	Gaussian	Speckle	Poisson	Blurring
1					
PSNR	41.3402	27.2872	27.4521	27.2553	27.3459
2					
PSNR	40.9581	27.4718	27.5265	27.3376	27.4557
3					
PSNR	42.6408	27.2759	27.3816	27.3793	27.2623
4					
PSNR	41.3980	27.3839	27.5088	27.4279	27.7070
5					
PSNR	41.3206	27.4665	29.5288	27.8759	27.8265
6					
PSNR	41.6746	27.6354	32.2871	29.7421	28.2866
7					
PSNR	41.8143	29.4687	34.7684	32.8219	27.4516
8					
PSNR	40.7806	32.2926	39.5445	36.0818	27.4319

Table 4: Extracted Watermark After Attack in Conventional Method LSB.

3. CONCLUSION AND FUTURE WORK

Watermarking is a method that is being used to hide information or identify data within the digital documents. Moreover, digital documents can be divided into three categories: video, audio and image. In this research, we have focused primarily on the watermarking of digital images. Digital watermarking is becoming popular, mainly for embedding undetectable marks such as copyright information. In this research, gray scale images have been applied to embed as an evidence of the ownership for the digital images. The proposed method also used Intermediate Significant Bits (ISB) to improve the quality of the watermarked image.

In this research, we have proposed a new watermarking method to improve previous works in area of spatial domain in terms of robustness and imperceptibility. The proposed method has been aimed to improve robustness of the watermarked image by using repeated variable for each pixel of the watermark. Also, it improves the probability of extracting intact bits after attacks and the security guaranteed by using a secret key and none-sequential embedding method.

Although the proposed method is tried to achieve the best quality, robustness, and security for watermarking in grayscale images, but some other important parameters must be considered as well, such as: Capacity and Integrity. Also grayscale image has been used for this research, but the present study can also be extended for colored image (RGB).

4. REFERENCES

- [1] Chin-Shiuh Shieh, Hsiang-Cheh Huang, Feng-Hsing Wang, Jeng-Shyang Pan, "Genetic watermarking based on transform-domain techniques". *Pattern Recognition*,. 37(3): p. 555-565, 2004.
- [2] Golea, N.E.-H., "A blind RGB color image watermarking based on singular value decomposition", in *Proceedings of the ACS/IEEE International Conference on Computer Systems and Applications - AICCSA 2010*, IEEE Computer Society. p. 1-5. 2010.
- [3] Yongjian Hu, Guangzhou, China Kwong, S. "Using invisible watermarks to protect visibly watermarked images" ,p. 584-587. 2004.
- [4] Potdar, V.M., Han, S., Chang, "A survey of digital image watermarking techniques". 2005. p. 709- 716.
- [5] Bamatraf, A. Ibrahim, R. Salleh, M.N.B.M, "Digital watermarking algorithm using LSB", in *Computer Applications and Industrial Electronics (ICCAIE)*, Kuala Lumpur, 2010.
- [6] Dharwadkar, N.V., Amberker, B.B. Gorai, A., "Non-blind watermarking scheme for color images in RGB space using DWT-SVD", in *Communications and Signal Processing (ICCSP)*, 2011 International Conference, Calicut, 2011.
- [7] Dehkordi, A.B., Esfahani, S.N., Avanaki, A.N. , "Robust LSB watermarking optimized for local structural similarity", in *Electrical Engineering (ICEE)*, 2011 19th Iranian Conference. Tehran, 2011.
- [8] Arya, D., "A Survey of Frequency and Wavelet Domain Digital Watermarking Techniques". 2010. 1(2).
- [9] Zhao Xingyang, "A novel color image fragile watermarking based on the extended channel", in *Broadband Network & Multimedia Technology*, 2009. IC-BNMT '09. 2nd IEEE International Conference, Beijing, Oct. 2009.

- [10] Gil-Je Lee, "A New LSB Based Digital Watermarking Scheme with Random Mapping Function", in Ubiquitous Multimedia Computing. UMC '08. International Symposium: Hobart, ACT, Oct 2008.
- [11] Ker, A., "Improved Detection of LSB Steganography in Grayscale Images Information Hiding", J. Fridrich, Editor, Springer Berlin / Heidelberg, 2005.
- [12] Kumar, N.M., Manikandan, T., Sathagirivasan, V. , "Non blind image watermarking based on similarity in contourlet domain", in Recent Trends in Information Technology (ICRTIT), 2011 International Conference, Chennai, Tamil Nadu, 2011.
- [13] Maity, S.P. and M.K. Kundu, "DHT domain digital watermarking with low loss in image informations". AEU - International Journal of Electronics and Communications. 64(3): p. 243-257, 2010.
- [14] MohammadReza Keyvanpour, Farnoosh Merrikh Bayat, "Blind image watermarking method based on chaotic key and dynamic coefficient quantization in the DWT domain", Mathematical and Computer Modelling, Available online 27 July 2012, ISSN 0895-7177, 2012.
- [15] Hu, M.-C., D.-C. Lou, and M.-C. Chang, "Dual-wrapped digital watermarking scheme for image copyright protection". Computers & Security 26 (4) , 319-330, 2007.
- [16] Jian Cao; Jiwu Huang; , "Controllable Secure Watermarking Technique for Tradeoff Between Robustness and Security," Information Forensics and Security, IEEE Transactions on , vol.7, no.2, pp.821-826, April 2012.
- [17] M.Padmaa, "ZIG-ZAG PVD – A Nontraditional Approach". International Journal of Computer Applications. Volume 5– No.7, August 2010.
- [18] Mir Shahriar Emami , Ghazali Bin Sulong, "Set Removal Attack: A New Geometric Watermarking Attack" in 2011 International Conference on Future Information Technology IPCSIT. 2011, IACSIT Press: Singapore. 2011.
- [19] Akram M. Zeki. Khedher, Azizah Abdul Manaf. "Digital watermarking and data hiding techniques". Proceedings of the Postgraduate Annual Research Seminar p. 79-84, 2006.