IMPERCEPTIBLE IMAGE WATERMARKING SCHEME

Su Su Maung, and Myint Myint Sein

Abstract— *Interest in digital watermarks is growing and seems to be motivated by the need to provide copyright protection to digital works. The digital watermark should not degrade the image to a degree that interferes with its usefulness. In this paper digital watermark is decompounded into a series of binary bitplanes by bit decomposition, and each bitplane being viewed as an ordinary two-dimensional binary watermark for watermarking. The results demonstrate that the enhanced quality of the watermarked image is obtained.*

Keywords— **Image processing, and watermarking.**

1. INTRODUCTION

The growth of digital media and the fact that unlimited numbers of perfect copies of such media can be illegally produced is a threat to the rights of content owners. A copy of digital media is an exact duplicate of the original. It may be copied and retransmitted without the permission of the author. An issue facing electronic commerce on the Internet for digital information is how to protect the copyright and intellectual property rights of those who legally own or posses digital works. Most electronic commerce systems use cryptography to secure the electronic transaction process. Encryption provides data confidentiality, authentication, and data integrity. However, the unencrypted data may still be copied and distributed (i.e., videotapes, DVD, and pay-per-view broadcasts). In some cases, these samples may be the images used on a web site or the publication of information on the Internet. Copyright protection involves ownership authentication and can be used to identify illegal copies. One approach to copyrighting is to mark works by adding information about their relationship to the owner by a digital watermark. Watermarking can be used to identify owners, license information, or other information related to the cover carrying the watermark. Digital watermarking provides a means of placing information within digital works. This information may be perceptible or imperceptible to the human senses. Digital watermarks have several desirable characteristics. The watermark should not degrade the image to a degree that interferes with its usefulness. The watermark should require no additional image formats or storage space. The watermark should be integrated with the image content so it cannot be removed easily without severely degrading the image. The watermark should be fairly tamper-resistant and robust to common signal distortions, compression, and malicious attempts to remove the watermark. The watermark can be made invisible to the human eye, but still readable by computer. The paper is organized as follows: Section 1 provides an introduction to digital Watermarking. Watermarking in transform domains is discussed in Section 2. Section 3 contains decomposition of gray level image to binary images. In Section 4 we describe the proposed watermarking scheme. The experimental results are shown in Section 5. Conclusions and suggestions about future research are presented in Section 6.

2. WATERMARKING IN TRANSFORM DOMAINS

Watermarks are embedded into images by changing some bits in image representation. Some methods operate on least significant bits, while others embed information into perceptually more significant image components. Current image-based digital watermarks may be grouped under two general classifications: those that fall into the image domain and those that fall into the transform domain. Tools used in the image domain include methods that use bit-wise techniques such as least significant bit (LSB) insertion and manipulation.

The transform domain classification of watermarks includes those that manipulate image transforms. Transforms such as the fast Fourier transform (FFT), discrete cosine transform (DCT), and wavelet transform hide information in the transform coefficients. These methods hide messages in relatively significant areas of the cover image. Transform domain watermarking and masking techniques are more robust against attacks such as lossy compression, cropping, and image processing techniques in which significant bits are changed.

The wavelet transform is identical to a hierarchical subband system, where the subbands are logarithmically spaced in frequency. The basic idea of the DWT for a two-dimensional image is described as follows. An image is first decomposed into four parts of high, middle, and low frequencies (i.e., LL1, HL1, LH1, HH1 subbands) by critically subsampling horizontal and vertical channels using subband filters. The subbands labeled HL1, LH1, and HH1 represent the finest scale

Su Su Maung was with Mandalay Technological University, Mandalay, Myanmar. She is now with the department of Information Technology, e-mail: susuelar@gmail.com)

Myint Myint was with University of Computer Studies, Yangon, Myanmar. email chuchu0228@gmail.com)

wavelet coefficients. To obtain the next coarser scaled wavelet coefficients, the subband LL1 is further decomposed and critically subsamped. This process is repeated several times, which is determined by the application at hand. An example of an image being decomposed into seven subbands for three levels is shown in Fig.1. Each level has various bands information such as low-low, low-high, high-low, and high-high frequency bands.

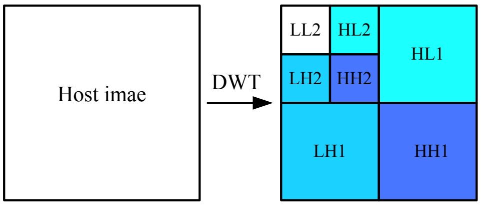
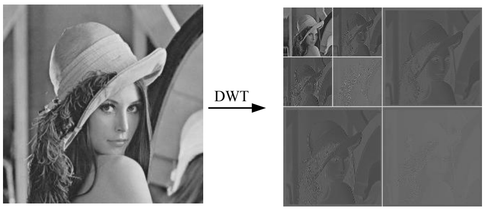


Fig.1. DWT decomposition of an image

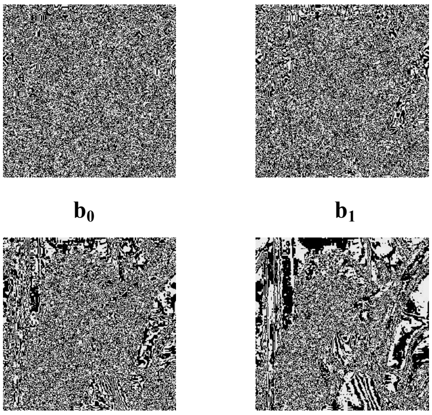


(a) **(b)**

Fig.2. DWT Decomposition. (A) Original Image. (B) 2 Scale Decomposition

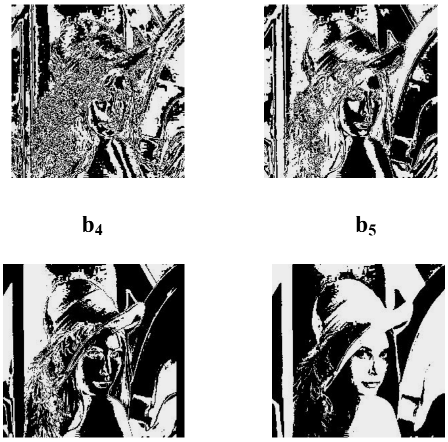
3. BIT PLANES DECOMPOSITION

Grayscale images can be transformed into a sequence of binary images by breaking them up into their bit-planes. If we consider the gray value of each pixel of an 8-bit image as an 8-bit binary word, then the zeroth bit plane consists of the last bit of each gray value. Since this bit has the least effect in terms of the magnitude of the value, it is called the least significant bit, and the plane consisting of those bits the least significant bit plane. Similarly the eighth bit plane consists of the first bit in each value. This bit has the greatest effect in terms of the magnitude of the value, so it is called the most significant bit, and the plane consisting of those bits the most significant bit plane. The bit plane images are shown in Fig.3. Note that the least significant bit plane, b_0, is to all intents and purposes a random array and that as the index value of the bit plane increases, more of the image appears. b_7 is the most significant bit plane.



b_0 **b_1**

b_2 **b_3**



b_4 **b_5**

b_6 **b_7**

Fig.3. The Bit Planes of An 8-Bit Grayscale Image

4. THE PROPOSED WATERMARKING SCHEME

In this paper, we propose a watermarking scheme that allows a user with an appropriate key to verify the ownership of the image. Using the correct key, we can extract a watermark from a watermarked image that can be identified to be associated with an owner. The embedded watermark must be invisible to human eyes and robust to most image processing operations. To meet these requirements, image is hashed into a bit array of length 128 by using hash function. The hash value and watermark image are then encrypted. The deterministic chaotic sequences are generated through chaotic maps to encrypt. The encrypted watermark signals are embedded in the image to form watermarked image. In most images, the energy is concentrated on the lower frequency range. In order to invisibly embed the watermark, it is expected that the lowest frequency components are left unmodified. On the other hand, watermarking technique is robust common image processing operations and lossy data compression. The important information of the watermark should not be embedded into the higher frequency components. In this paper, watermark signals are embedded into middle frequency components. The input image is transformed by the discrete wavelet transform into frequency domain. The position for embedding is selected by pseudo-random numbers generated using chaotic function. Since this watermarking scheme requires a user key during both the insertion and the extraction procedures, it is not possible for an unauthorized user to insert a new watermark or alter the existing watermark.

The detailed procedures of watermarking scheme are given as follows:

[1] Select the host image of size $M\times N$ pixels. We want to insert an invisible watermark to form a watermarked image of the same size. The watermark insertion procedure is shown in Figure 3. Design the copyright information of the author, watermark image or message. If the watermark signal is message of the author, such as author name, issue date, etc, it is converted to ASCII codes. Consider a cryptography hash function

$$H(S)=(d_1,d_2,\dots,d_p) \qquad (1)$$

Where

S string of data of binary length;

d_i binary output bits of the hash function;

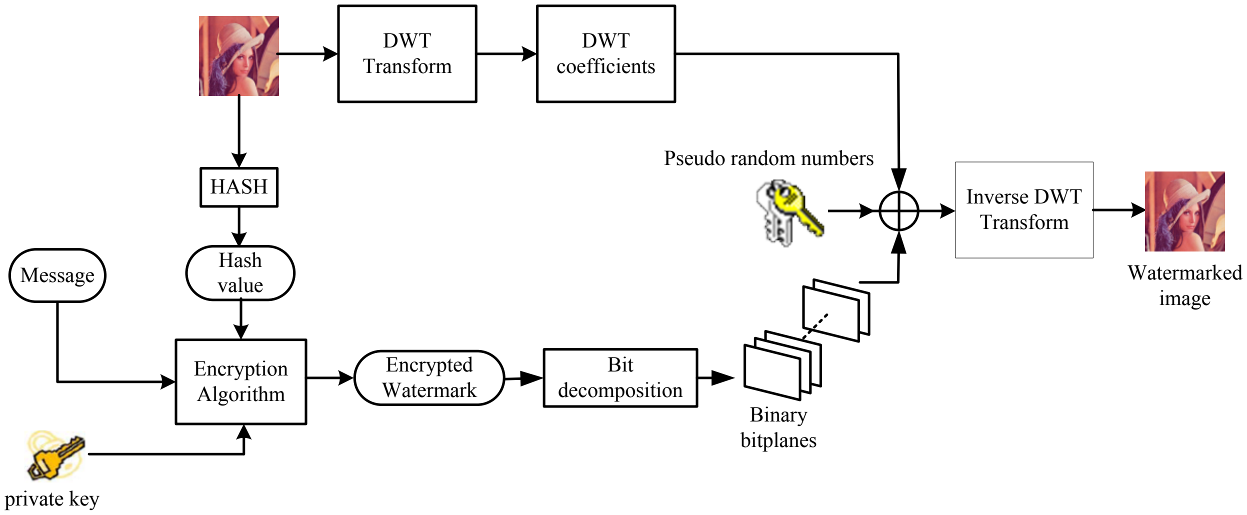


Fig.4. The Proposed Watermarking Scheme

p size of the output bit string.

A cryptographic hash function has the property that given an input bit string *S* and its corresponding output ($d_1,\dots,d_p$). it is computationally infeasible to find another input bit string of any length that will be hashed to the same output ($d_1,\dots,d_p$). An example is the well known MD5 where any string of data is hashed into a bit array if length 128, i.e., p=128. We use MD5 as our hash function. It is obvious that any other cryptographic hash function can also be used in our watermarking scheme. We compute finger print of host image using hash function. Then any private key encryption algorithm is used to encrypt the original watermark image and the hash value of the host image. These encrypted watermark signals are random-like and uncorrelated; however, the same sequence will be presented after decrypting.

[2] Decompose the host signal (original image) into frequencies domain by using 2-D discrete wavelet transform. Fig.2 gives an illustration of different scales 2D wavelet decomposition of an image. To trade off between the transparence and robustness of the watermark, the middle frequency coefficients of wavelet domain (HL2, LH2, and HH2) are chosen as host signal *X*. HL2, LH2, HH2 are reordered to fill the 2D area of $L \times L$.

[3] The encrypted watermark is decomposed into digital binary images. Embed these digital binary images chaotically in the middle frequency coefficients of the host image, keeping the parameters as a private key.

[4] Retransform the watermarked host signal to generate a watermarked image.

[5] Repeat steps 3 and 4, we may get a set of watermarked images which include different encrypted information.

The retrieving procedures are notably symmetrical to that of the above embedding watermark procedures.

[1] Retrieve the middle frequency coefficients of wavelet domain i.e. the host signal of a test image.

[2] Extract the encrypted watermark signal according to the embedded position which is determined by private key.

[3] Decrypt the extracted watermark signal we may get the original copyright information.

5. THE RESULTS OF IMPERCEPTIBLE WATERMARK EMBEDDING

The experimental results are obtained by using a 256×256 lena image. The original watermark information is 64×64 logo image of MTU. Fig.4 shows the original image of size 256×256 and the watermark image of size 64×64. The embedding process is applied to the middle frequency coefficients of wavelet domain (HL2, LH2, HH2) of host image X. First, we embed the mixed chaotic watermark signal into the middle frequency coefficients of the host image without decompositing it into binary digital images. The results demonstrate that the lower quality of the watermarked image is obtained (see Fig.6). Then digital watermark is decompounded into a series of binary bitplanes by bit decomposition, each bitplane being viewed as an ordinary two-dimensional binary watermark for watermarking. Fig.8 shows the watermarked image after enhancing by bit decomposition.

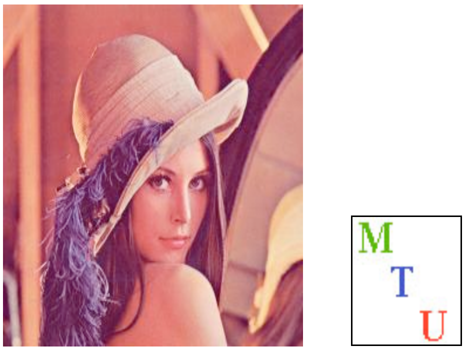


Fig.5. The Original Lena Image and The Watermark Image

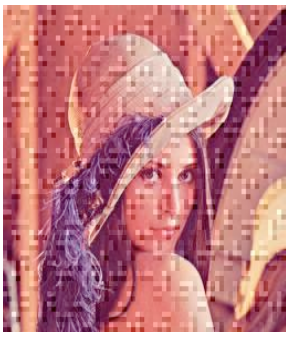


Fig.6. The Watermarked Image Before Bit Decomposition

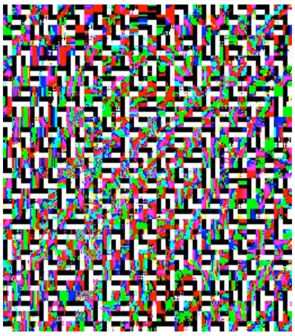


Fig.7. The Difference Between Original Image and Watermarked Image

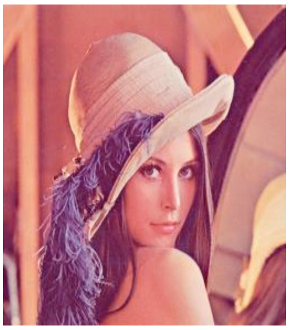


Fig.8. The Watermarked Image After Bit Decomposition

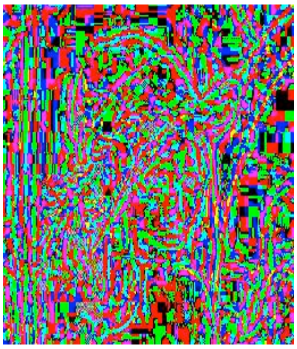


Fig.9. The Difference Between Original Image and Watermarked Image

6. CONCLUSION

In this paper the lower quality of the watermarked image is enhanced by decompositing the logo image into sequences of binary images. To improve the security of the watermarking algorithm, the watermark is added to the middle frequency coefficients of wavelet domain randomly by exploiting chaotic system, keeping the parameters of chaotic system as a private key can prevent the watermark from removing illegally. The encryption to the embedding position results in that the watermark cannot be detectable by an unauthorized user. Superposition randomly improves the robustness and security of the watermarking algorithm. . The encryption to the embedding position using chaotic system improve the security of the watermarking algorithm, and also, the imperceptibility of the watermarking algorithm is improved better by decompositing the watermark image into sequences of binary images.

REFERENCES

[1] Wolfgang, R.B., Podilchuk, C.I., and Delp, E.J. 1999. Perceptual watermarks for digital images. In *Proceedings of IEEE*. 7(7), 1108-1126.

[2] Swanson, M., Kobayashi, M. and Tewfik, A. 1998. Multimedia data-embedding and watermarking strategies. In *Proceedings of IEEE*. 86(7), 1064-1087.

[3] Su, J., Hartung, F. and Girod, B. 1999. Ditigal watermarking of text, image, and video documents. In *Proceedings of IEEE*. 22(6), 687-695.

[4] Wolfgang, R.B. and Delp, E.J. 1996. A watermarking for digital images. In *Proceedings of IEEE*. 3(9), 215-218.

[5] Boland, F.M., O'Ruanaidh, J.J.K. and Dautzenberg, C. 1995. Watermarking digitals images for copyright protection. In *IEEE Int. Conf. Image Proc. And its Applications*. 321-326.