OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

A Robust Watermarking Technique Based On Dwt on Digital Images

B. Mohan Swaroop, Assistant Professor,
Potti Sriramulu Chalavadi Mallikharjunarao College of Engg & Tech

ABSTRACT: *In this paper a robust watermark scheme for copyright protection is proposed. By modifying the original image in transform domain and embedding a watermark in the difference values between the original image and its reference image, the proposed scheme overcomes the weak robustness problem of embedding a watermark in the spatial domain. Besides the watermark extraction does not require the original image so it is more practical in real application. The experimental results show that the proposed scheme provides not only good image quality, but also robust against various attacks such as compression and noise addition.*

Many image transforms have been considered and the most prominent among them us the discrete cosine transform (DCT) which has also been favored in the early image and coding standards. Hence, there is a large number of watermarking algorithms that use either a block based or global DCT. But the disadvantage in DCT is that it has only frequency resolution and no time resolution.

A new multi resolution watermarking method for digital images has been introduced. Wavelets are mathematical functions that cut the data into different frequency components and then study each component with a resolution matched to its scale. The method is based on the discrete wavelet transform (DWT). Pseudo-random codes are added to the large coefficients at the high and middle frequency bands of the DWT of an image. It is more robust to proposed methods to some common image distortions, such as image compression, image rescaling/stretching.

Keywords: *Digital Watermarking, Discrete wavelet transform, Information security, Encryption, Stegonagraphy.*

I. INTRODUCTION

A great deal of information is now being created, stored, and distributed in digital form. Newspapers, and magazines, for example, have gone online to provide real-time coverage of stories with high-quality audio, still images, and even video sequences. The growth in use of public networks such as the Internet has further fueled the online presence of publishers by providing a quick and inexpensive way to distribute their work. The explosive growth of digital media is not limited to news organizations, however. Commercial music may be purchased and downloaded off of the Internet, stock photography vendors digitize and sell photographs in electronic form, and Digital Versatile Disc (DVD) systems provide movies with clear images and CD quality sound.

Unfortunately, media stored in digital form are vulnerable in a number of ways. First of all, digital media may be simply copied and redistributed, either legally or illegally, at low cost and with no loss of information. In addition, today's fast computers allow digital media to be easily manipulated, so it is possible to incorporate portions of a digital signal into one's own work without regard for copyright restrictions placed upon the work. Encryption is an obvious way to make the distribution of digital media more secure, but often there is no way to protect information once it has been decrypted into its original form. The ability for pirates to easily copy works is one of the last hurdles that keep publishers from completely adopting online distribution systems.

Digital watermarking is seen as a partial solution to the problem of securing copyright ownership. Essentially, watermarking is defined as the process of embedding sideband data directly into the samples of a digital audio, image, or video signal. Sideband data is typically “extra” information that must be transmitted along with a digital signal, such as block headers or time synchronization markers. It is important to realize that a watermark is not transmitted in addition to a digital signal, but rather as an integral part of the signal samples. The value of watermarking comes from the fact that regular sideband data may be lost or modified when the digital signal is converted between formats, but the samples of the digital signal are (typically) unchanged.

The earliest forms of information hiding can actually be considered to be highly crude forms of private-key cryptography; the "key" in this case being the knowledge of the method being employed (security through obscurity). Steganography books are filled with examples of such methods used throughout history. Greek messengers had messages tattooed into their shaved head, concealing the message when their hair finally grew back. Wax tables were scraped down to bare wood were a message was scratched. Once the tablets were re-waxed, the hidden message was secure. Over time these primitive cryptographic techniques improved, increasing speed, capacity and security of the transmitted message.

II. WATERMARKING

Although steganography and watermarking both describe techniques used for covert communication, steganography typically relates only to covert point to point communication between two parties. Steganographic methods are not robust against attacks or modification of data that might occur during transmission, storage or format conversion.

Watermarking, as opposed to steganography, has an additional requirement of robustness against possible attacks. An ideal steganographic system would embed a large amount of information perfectly securely, with no visible degradation to the cover object. An ideal watermarking system, however, would embed an amount of information that could not be removed or altered without making the cover object entirely unusable.

As a side effect of these different requirements, a watermarking system will often trade capacity and perhaps even some security for additional robustness. The working principle of the watermarking techniques is similar to the steganography methods. A watermarking system is made up of a watermark embedding system and a watermark recovery system. The system also has a *key* which could be either a public or a secret key. The *key* is used to enforce security, which is prevention of unauthorized parties from manipulating or recovering the watermark. The embedding and recovery processes of watermarking are shown in below figures.

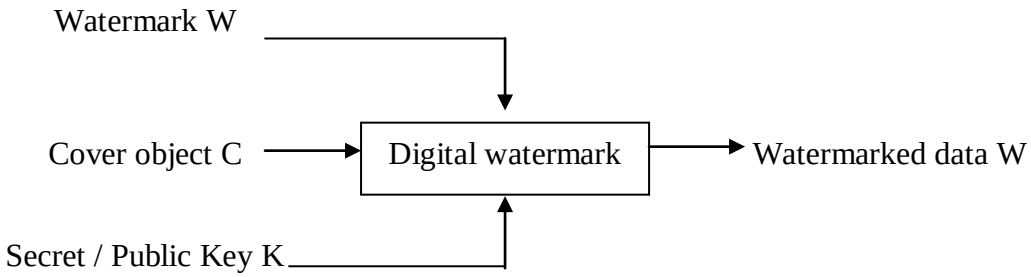


Fig-1.1 Digital watermarking – Embedding/Encryption

For the embedding process the inputs are the watermark, cover object and the secret or the public key. The watermark used can be text, numbers or an image. The resulting final data received is the watermarked data *W.*

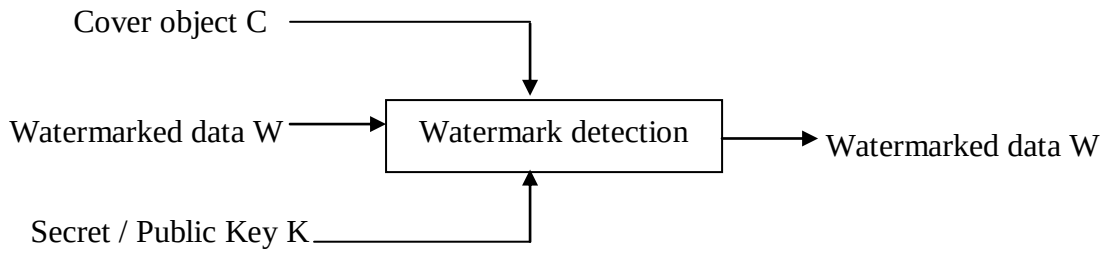


Fig-1.2 Digital watermarking – Decoding

The inputs during the decoding process are the watermark or the original data, the watermarked data and the secret or the public key. The output is the recovered watermark W.

III. THE PROPOSED SCHEME

The proposed scheme utilizes the concept of Joo et al.'s scheme to embed a watermark into an image.

Motivation for the proposed scheme

In 2002, Joo et al. proposed a robust watermark scheme by embedding a watermark into wavelet low frequency sub-band. It is briefly introduced as follows. First, an image with size of 512 by 512 pixels is transformed into wavelet coefficients by three-level wavelet transform and extract the sub-band LL_3. The

extracted sub-band LL_3 is further decomposed into four sub-bands and then three high frequency sub-bands (LH_4, HL_4, HH_4) are set to zero.

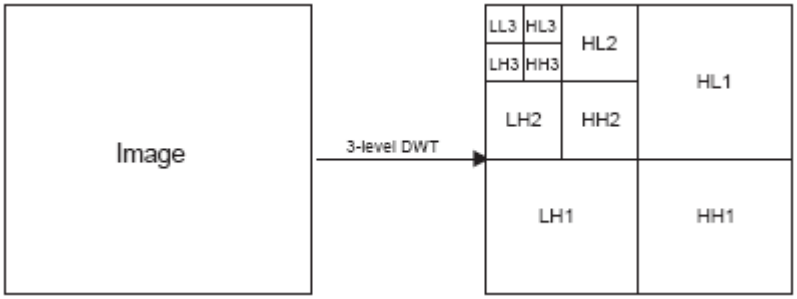


Fig. 1.3 Three-level wavelet decomposition of an image

After performing inverse wavelet transform, its reference sub-band $LL_3^{'}$ is obtained. The information idx of embedding location in the watermark embedding process is obtained by sorting $LL_3 - LL_3^{'}$. Finally, the watermark information is embedded into the sub band LL_3 by $LL_3 = LL_3^{'} \pm k \times w(idx(i))$, where k is a factor for controlling embedding intensity and w is a pseudo-random binary sequence with the length of 1000 bits generated by using a seed, w belongs to{1,1}. Besides, due to the fact that change to LL_3 values also cause some change to its reference $LL_3^{'}$ values, hence, the embedding process is repeated. As the embedding process is repeated, the image quality is decreased but its reliability is increased.

In watermarking extraction process, the original image is required for obtaining the watermark embedding location. According to the embedding location, the watermark can be extracted by comparing the two sub-bands LL_3 and $LL_3^{'}$. Finally, the extracted watermark is compared with the original watermark by similarity measure formula. We know that, for an image, most of energy is concentrated on low-frequency and human eyes are sensitive to the change of low-frequency. Although the above scheme provides the characteristics of robustness and imperceptibility, but the embedding process is quite time-consuming. Besides, the original image is required in the watermark extraction process, which is impractical in real application.

The watermark embedding

The original image X is a gray-level image with M by N pixels. The watermark W is a pseudo random bit-sequence generated by using a seed. They are defined as follows:

$$X = \{x(i, j) \mid 0 \le i \le M-1, 0 \le j \le N-1, 0 \le x(i, j) \le 255\} \text{ and}$$
$$W = \{w(k) \mid 1 \le k \le n, w(k) \in \{1, -1\}\}$$

First, the original image is modified in transform domain. Then, a watermark is embedded into the original image according to the difference values between the original image and its reference image.

Input: An original image X and watermark W.

Output: A watermarked image X_w and a sequence idx of embedding location.

1. **Step 1:** Transform the original image into wavelet coefficients by one-level wavelet transform.
2. **Step 2:** Set three high-frequency sub-bands LH_1, HL_1 and HH_1 to zero.
3. **Step 3:** Perform inverse wavelet transform and obtain its reference image.
4. **Step 4:** Compute the differences between the original image X and its reference image $X^{'}$. Then obtain location $idx(i, j)$ such that $s < |x(i, j) - x^{'}(i, j)| < t$, where s and $t \in Z^{+}$.
5. **Step 5:** According to the result of Step 4, randomly select some locations to embedding. The watermark is embedded as follows.

Note that the embedding process does not require repeat. Furthermore, the sequence idx of embedding locations should keep as the secret key for subsequent watermark extraction. The watermark embedding block diagram is shown as Fig. 1.4.

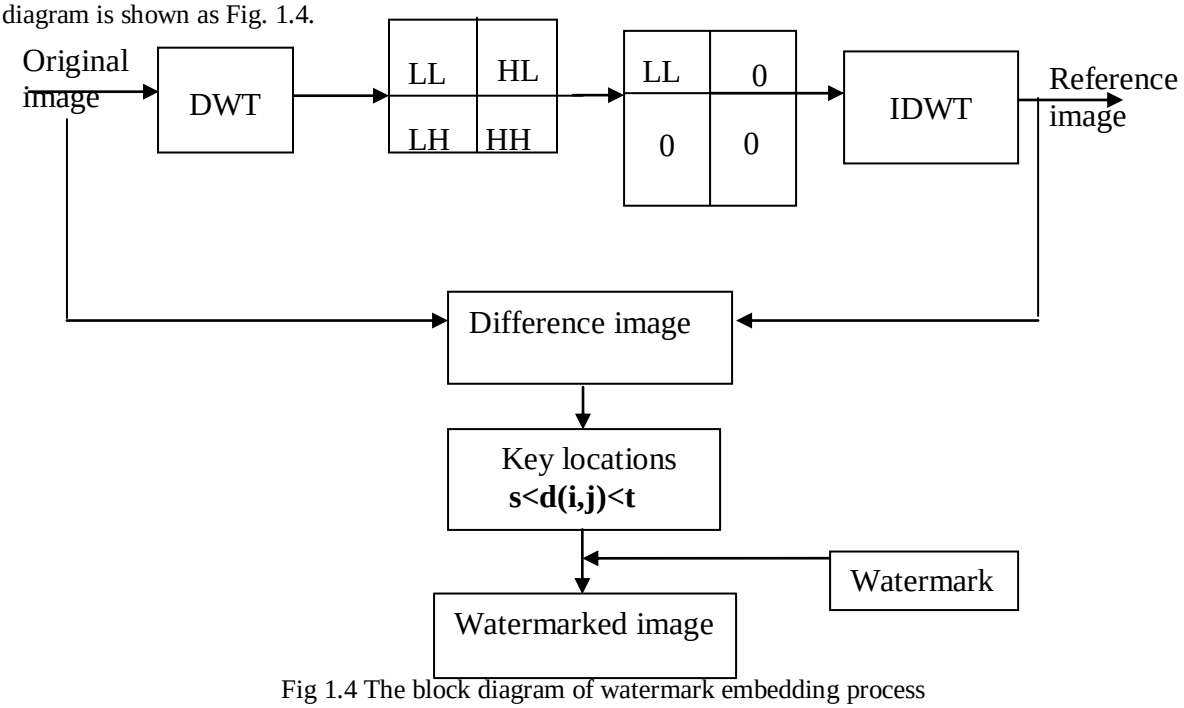


Fig 1.4 The block diagram of watermark embedding process

MATLAB code for watermark embedding

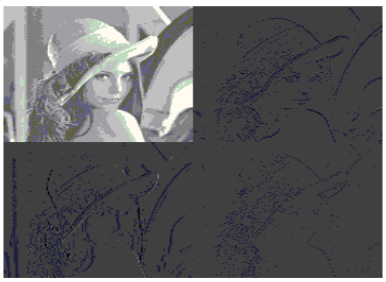
```
function aw=embedd(w,a,a1,idx,s,t)
[m,n]=size(a);
[p,q]=size(idx);
alpha=round((s+t)/2);
for z=1:1:length(w)
   i=idx(z,1);
   j=idx(z,2);
   if w(1,z)==1
      a(i,j)=a1(i,j)+ alpha;
   else
       a(i,j)=a1(i,j)- alpha;
   end
end
aw=a;
end
```

MATLAB code for watermark extraction

```
function w=extract(a,a1,idx,n)
 for z=1:1:n
   i=idx(z,1);
   j=idx(z,2);
   if a(i,j)>=a1(i,j)
      w(1,z)=1;
   end
   if a(i,j)< a1(i,j)
      w(1,z)=0;
   end
 end
```

IV. OUTPUT IMAGES

In the following experiments, two gray-level images with size of 256 by 256, Lena is as the test image. The watermark is a pseudo random bit-sequence with length of 1000 bits generated by using the seed number 250. We choose $\alpha = 7$ to balance the trade off between the robustness and imperceptibility.



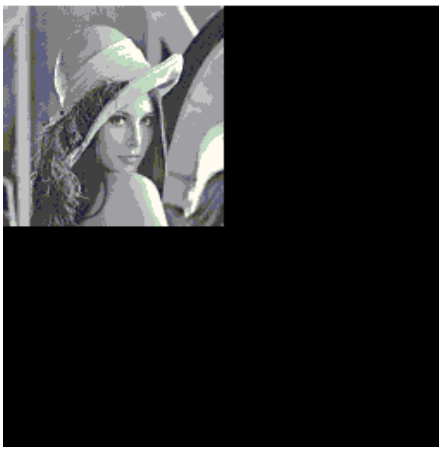


Fig 1.7 Modified DWT Image

Fig 1.8 IDWT Image

Fig 1.9 Difference Image

V. CONCLUSION

Although the above scheme provides the characteristic of robustness and imperceptibility, but the embedding process is quite time-consuming. Besides, the original image is required in the watermark extraction process which is impractical in real application. The concept of Joo et al.'s scheme and propose a robust watermark scheme using self-reference image. By transforming the original image in wavelet domain and embedding a watermark in the difference values between the original image and its reference image, the proposed scheme overcomes the weak robustness problem of embedding a watermark in the spatial domain. Besides, the watermark embedding does not require repeat in the watermark embedding process and we can use a secure encryption algorithm, such as RSA, to increase security of the proposed scheme. The watermark extraction also does not require the original image so the application is more practical in real application for ownership verification. The experimental results show that the proposed technique provides good image quality

and robust to various attacks. In summary, the proposed method has the following contributions. Firstly, the watermark extraction process does not require the original image. Thus, it may be applied easily to Internet. Secondly, the proposed scheme overcomes the weak robustness problem of embedding a watermark in the spatial domain. Thirdly, the embedded watermark can survive under various attacks.

REFERENCES

[1] D.-C. Lou, J.-L. Liu, A robust watermarking scheme based on the just-noticeable-distortion, Journal of Chung Cheng Institute of Technology 31 (2) (2003) 11 – 22.

[2] I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image Processing 6 (12) (1997) 1673– 1687.

[3] S. Joo, Y. Suh, J. Shin, H. Kikuchi, S.-J. Cho, A new robust watermark embedding into wavelet DC components, ETRI Journal 24 (5) (2002) 401–404.

[4] C.-T. Hsu, J.-L. Wu, Multi resolution watermarking for Digital image, IEEE Transactions on Circuits and Systems, 2, Analog and Digital Signal Processing 45 (8) (1998) 1097– 1101.

[5] C.-S. Lu, S.-K. Huang, C.-J. Sze, M. Liao, Cocktail watermarking for digital image protection, IEEE Transactions on Multimedia 2 (4) (2000) 209–224.

[6] W. Zeng, B. Liu, A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images, IEEE Transactions on Image Processing 8 (11) (1999) 1534–1548.

[7] S. Stankovic, I. Djurovic, I. Pitas, Watermarking in the space/spatial-frequency domain using two-dimensional Radon–Wigner distribution, IEEE Transactions on Image Processing 10 (4) (2001) 650– 658.

[8] M.-S. Hsieh, D.-C. Tseng, Y.-H. Huang, Hiding digital watermarks using multi resolution wavelet transform, IEEE Transactions on Industrial Electronics 48 (5) (2001) 875–882

[9] S.-C. Chu, J.F. Roddick, Z.-M. Lu, J.-S. Pan, A digital image watermarking method based on labeled bisecting clustering algorithm, IEICE Transactions on Fundamentals E87-A (1) (2004) 282–285.

[10] Peter H.W. Wong, Oscar C. Au, Y.M. Yeung, A novel blind multiple watermarking technique for images, IEEE Transactions on Circuits and Systems for Video Technology 13 (8) (2003) 813– 830.