International Journal of Electronics, Communication & Soft Computing Science and Engineering
ISSN: 2277-9477, Volume 3, Issue 3

Digital Image Watermarking Using a Blind Detection for Copyright Authentication

Anupama Purohit

Abstract - **Today internets play a big role in carrying information from one place to another. And this information may be images, audio, and also video. Attacks on the digital data are very easy and easily monitored in the internet. And watermarking process is used for the purpose of authentication. And the grayscale image watermarking process is used for the process of embedding and detection. Wavelet multi-resolution is used in the watermarking process. Wavelet means the small signal which work simultaneously in time and frequency. During the embedding process spread spectrum technique is used. And the strength of watermark is adjusted according the cover image or the original image. The DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet Transform) method are used. And this method is not more robust against the different types of attacks, different type of noise and JPEG compression because non-blind watermarking algorithm is used. In this paper we purposed a new method which is more robust against the different types of attacks, different types of noise and JPEG compression. We use DWPT (Discrete Wavelet Packet Transform) and we use the blind detection method. Blind detection means that we cannot use the original or the cover image information during the extraction process. And for the purpose of security we also embed the secret key. And this secret is prepared by using the different image or the text image. And this method basically used for the copyright verification purpose.**

Key Words — **DWPT, Grayscale, JPEG compression, Wavelet.**

I. INTRODUCTION

With the advent of internet and the extremely good growth in the field of Digital technology. So, many applications in the area of multimedia communications, multimedia networking have been proliferated over the years. The essential purpose is security and the protection of image from the other people. And these people manipulate our Digital image, audio and video. So to remove the problem of this manipulation the new technology is developing is known as Digital Watermarking. And it is develop for providing security for multimedia data such as images, audio and video. Digital watermarking means that in which we add some information in the Cover image or multimedia data and sometime a secret key is also embedded in the cover image or multimedia data. And the process of watermarking image processing which is basically done for the image. And this image is known as watermarked image. And this watermarking technique attracted lots of attention. Digital watermarking generally falls into the visible watermarking technology and hidden watermarking technology [6]. In addition, according to the watermarking embedding process can be divided into two categories, one kind algorithm directly changes some pixel image grey value to join watermarking spatial domain, such as, Least significant bits and spread spectrum method [7, 8], etc. Another type of method is to make one transform of image and then add to Watermarking transform domain, such as DWT, Radon transform moments [9].

The basic idea is that decompose the image with multi-resolution decomposition technology, and the image will be decomposed into many different space, different frequency sub-images .Watermarking has two most important properties: transparency and robustness. For the image watermarking, the invisibility is defined that carrier image is not significantly degraded after embedding. The robustness refers to the ability that the watermark will not lose after a kind of common signal processing operations.

A watermark can be considered to be some kind of information that is embedded into underlying data for tamper detection, localization, ownership proof, and/or traitor tracing purposes. Watermarking techniques apply to various types of host content. Digital watermarking is changing an image in a way so that you can see some text or background image without actually corrupting the image. Watermarking is used to verify the identity and authenticity of the owner of a digital image. It is a process in which the information which verifies the owner is embedded into the digital image or signal.

The main work is to implement the super-resolution reconstruction of image sparse representation on processing carrier images and choose a kind of super resolution reconstruction method which original image is first reduced and

then enlarged. In the process of amplification, the filling of the pixel information greatly eliminates the correlation among the original image pixel which can enhance the robustness of the watermark. And the mixed error correcting coder can add more redundancy among codes and increase the error correcting capability of decoder. Finally, block the image and the watermarking which is encoded with mixed error-correcting code is embedded in low frequency band of the Discrete Wavelet Transform (DWT) repeatedly. The results show that our image watermarking scheme with SRIR is better than the traditional one.

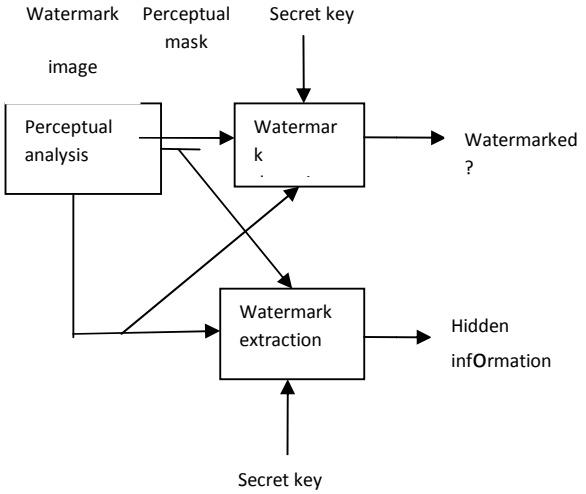

Fig. 1 Watermark embedding Unit

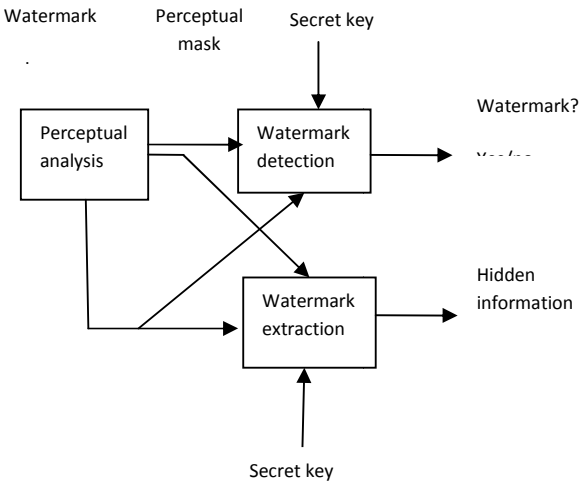

Fig.2 Watermark Detection Unit

II. LITERATURE SURVEY

Qing Liu et al [1] proposed "Grayscale Image Digital Watermarking Technology Based on Wavelet Analysis". Aim at the grayscale image watermarking embedding and detection, on the basis of introduction of digital watermarking principle and wavelet multiresolution analysis, adaptive blind grayscale image watermarking algorithm based on wavelet analysis is put forward. Firstly, the embedded watermarking signal is processed by spread spectrum technology, secondly the location of the embedded watermarking and strength is automatically adjust according to the characteristics of the original image, and watermarking is adaptively added to the grayscale images, finally the watermarking signal is blindly extracted without the information of the original image. Experimental results show that the proposed algorithm enhances the anti- attack capability and the hidden nature of the image, improve the security of the watermarking detection, and has higher robustness to random noise attack, cutting and JPEG compression. An adaptive wavelet grayscale image watermarking algorithm is brought forward. In order to improve the robustness of the watermarking, the spread spectrum principle is introduced in the watermarking embedding and detection. Under the premise of image quality, this algorithm can realize the blind watermarking extraction and detection, and has a good robustness to random noise attack, cutting, noise pollution and JPEG compression.

Anamitra Makur et al [2] proposed "Tamper-Proof Image Watermarking using Self Embedding". A fragile watermarking with self-embedding for recovery of tampered image that does not use authentication bits. They use a robust spread spectrum based watermarking scheme using block based embedding, DCT based compression, and other improvements. Simulation results showing recovery performance are presented and find out the Conclusion we develop a novel algorithm for tamper detection and recovery of images using no authentication bit and robust watermarking. Here, the watermark is not only used for tamper detection, but it also carries enough information regarding the cover image so as to help in recovering the tampered

parts of the received image. They have used a DCT based image compression scheme, spread spectrum image steganography to embed the watermark, several error correction schemes (both at the encoder and decoder) to enhance the watermark extraction, and careful selection of global and local MSE thresholds, to achieve up to 90% restoration of the tampered image.

A. V. Subramanyam et al [3] proposed "Robust Watermarking of Compressed and Encrypted JPEG2000 Images". A compressed-encrypted domain jpeg2000 image watermarking "gives the concept about digital rights management (DRM) systems, digital media is often distributed by multiple levels of distributors in a compressed and encrypted format. The distributors in the chain face the problem of embedding their watermark in compressed, encrypted domain for copyright violation detection purpose. Here they propose a robust watermark embedding technique for JPEG2000 compressed and encrypted images. While the proposed technique embeds watermark in the compressed encrypted domain, the extraction of watermark can be done either in decrypted domain or in encrypted domain and found out the Conclusion a technique to embed a robust watermark in the JPEG2000 compressed encrypted images. The algorithm is simple to implement as it is directly performed on the compressed-encrypted domain i.e it does not require decrypting or partial decompression of the content.

Xiangbin Feng et al [4] proposed "Digital Image Watermarking Based on Super- Resolution Image Reconstruction". This algorithm based on the Super-Resolution Image Reconstruction (SRIR). They use pattern recognition method to optimize the performance of digital watermarking. First, the binary watermarking is scanned to one dimension sequence before embedding, at the same time ,they chose a mixed error-correcting code—(3,1,2) convolutional code and (3,1) repetition code to encode the original watermarking, and the sequence is inputted into the (3,1,2) convolution encoder and (3,1) repetition encoder frame by frame. The output sequence is scanned to some matrixes as the watermarking information. Second, the super-resolution reconstruction of image sparse representation is implemented on carrier image and finally a novel robustness watermarking based on SRIR is proposed. This method is mainly applied the SRIR to pre-process the original image. The correlation among pixels of original will be reduced. Meanwhile, encode the watermark with (3,1,2) convolutional encoder and (3,1) repetition encoder before embedding. It also contains the results of tests performed showing the high robustness of the algorithm against the attacks of JPEG lossy compression and salt-and pepper noise, multiplicative noise, center cutting.

Bin Zhang et al [5] proposed "A Near Reversible Image Watermarking Algorithm". The near reversible watermarking algorithm based on LSB replacement. It can not only recover the original data to a high extent, but also have strong robustness and low calculating complexity. Being a novel category of watermarking schemes, reversible watermarking algorithms were developed in recent years. As it can recover the watermarked data back to the original host signal, reversible watermarking algorithms are suitable for medical, military and other special fields. However, these algorithms have their defects, such as weak robustness, low embedding capacity and high calculating complexity.

III. PROPOSED WORK

A. *Watermark Embedding*

The main concept of embedding the watermark by using the DWPT (Discrete Wavelet Packet Transform) method. Firstly, the watermark selects the random binary no. and this selected no. is embedded into the DWT (Discrete Wavelet Transform) of the cover image by using the DWPT (Discrete Wavelet Packet Transform). And this watermark is only known by the owner. The watermark is placed in the cover image by selecting the co-efficient of the selected block by using the quantization process.

B. *Algorithm: Watermark Embedding*

1. Input HI as Host image. Apply Discrete Wavelet Transform to decompose it into four sub-bands LL, HL, LH and HH.

2. Select HH band and apply discrete cosine transform to it and get discrete cosine transform coefficient matrix H.

3. Map discrete cosine transform coefficient matrix H into four quadrants q1, q2, q3 and q4 by using S-Pattern scanning.

4. Apply Singular Value Decomposition to each quadrant q1, q2, q3 and q4 to get S1, S2, S3 and S4.

5. Input WI as Watermark image. Apply Discrete Wavelet Transform to decompose it into four sub-bands LL, HL, LH and HH.

6. Select HH band and apply discrete cosine transform to it and get discrete cosine transform coefficient matrix W.

7.Apply Singular Value Decomposition on matrix W to get Sw.

8. Modify S1, S2, S3 and S4 by using equation $S_{ii} = S_i + a * S_w$ where, I = 1 to 4.

9. Mapping coefficients from S-Pattern scanning to original position matrix H*.

10. Apply inverse discrete cosine transform to H* to produce HH*.

11. Apply inverse Discrete Wavelet Transform to LL, HL, LH and HH* to get watermarked image WI.

C. Extraction Process

In extraction process, not only the coefficients selection and quantization steps are applied but also watermark extraction method is used.

We use a blind detection technique which is used during the watermark extraction.

D. Algorithm: Watermark Extraction

1. Input WI as Watermarked image. Apply Discrete Wavelet Transform to decompose it into four sub-bands LL, HL, LH and HH.

2. Select HH band and apply discrete cosine transform to it and get discrete cosine transform coefficient matrix W.

3. Map discrete cosine transform coefficient matrix W into four quadrants q1, q2, q3 and q4 by using S-Pattern scanning.

4. Modify S1, S2, S3 and S4 by using equation $S_w = (S_{ii} - S_i) / a$ where, i = 1 to 4

5. Re-construct Singular Value Decomposition matrix for each quadrant q1, q2, q3 and q4.6. Apply inverse *discrete cosine transform* and inverse Discrete Wavelet Transform to each quadrant.

CONCLUSION

A blind digital image watermarking scheme, which embeds watermark in the wavelet domain of an image by using the discrete wavelet packet transform (DWPT) and quantization of the selected dominant coefficients, was proposed in this paper. In addition to this, blind detection of the watermark is applied in this method. It saves the time and space for transferring the original image and saving the original image, respectively. The results of experiments show that the proposed method is very robust against JPEG compression and Gaussian noise, which has different value affects the robustness. The quantization parameter of the watermark, used in the algorithm is user-defined. It needs a large number of experiments to decide a proper value. Moreover, the capacity, which is an important part of digital watermarking, will also be developed in our future work.

REFERENCES

[1]. Qing Liu ,Tianshui Grayscale Image Digital Watermarking Technology Based on Wavelet Analysis 2012 IEEE Symposium on Electrical & Electronics Engineering (EEESYM).
[2]. Anamitra Makur, Nikhil Narayan S."Tamper-Proof Image Watermarking using Self Embedding" Electrical & Electronic Nanyang Technological University, Singapore, acm-2012.
[3]. V. Subramanyam, Sabu Emmanuel and Mohan S. Kankanhalli "Robust Watermarking of Compressed and Encrypted JPEG2000 Images" Member, Ieee Transactions On Multimedia, Vol. 14, No. 3, June 2012.
[4]. Xiangbin Feng , Yonghong Chen. Digital Image Watermarking Based on Super- Resolution Image Reconstruction 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2012),978-1-4673-0024-7/10, IEEE-2012.
[5]. Bin Zhang, Yang Xin, Xin-Xin Niu, Kai-Guo Yuan, Hui-Bai Jiang, "A Near Reversible Image Watermarking Algorithm" Proceedings Of The Ninth International Conference On Machine Learning And Cybernetics, Qingdao, 11-14 July 2010.
[6]. ME Haroutunian, S.A Tonoyan, "Random coding bound of information hiding E-capacity," Proc. IEEE Symp. International Symposium on Information Theory, IEEE Press,Jun. 2008: 536.
[7]. A Menezes, P. Orschot, S. Vanstone. "Handbook of Applied Cryptography," London: CRC Press, pp.454 -4591996.
[8]. D. Johnson, A Menezes, S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," International Journal of Information Security, voL I, pp. 36-63, 200 I.
[9]. B. He, "A Digital Watermarkinging Algorithm Based on Radon Transform Invariant Moments and Wavelet Lifting," Computer & Digital Engineering, vol. 39, pp.124-128, 2011.

AUTHOR'S PROFILE

Anupama Purohit

P.G :- M.TECH(DIGITAL COMM.)
GRADUATION: B.E(ELECTRONIC & COMM.)