**International Academy of Science,
Engineering and Technology**

IASET   Connecting Researchers; Nurturing Innovations

ANALYZE THE DIGITAL IMAGE WATERMARKING

SCHEMES FOR DATA SECURITY

PREETY GUPTA[1], RASHMI JORA[2] & RICHA ARYA[3]

[1]HOD, Department of Computer Science and Engineering, Amity University, Jaipur, Rajasthan, India

[2]Department of Computer Science and Engineering, Amity University, Jaipur, Rajasthan, India

[3]Assistant Professor, Department of CSE & E, Amity University, Jaipur, Rajasthan, India

ABSTRACT

There are so many digital services and applications are available in today's world. As the applications and services are increased day by day, the security is to be needed. In this paper, there are some watermarking techniques are described for example visible or transparent watermarking technique and invisible or non-transparent technique and also some attacks and noises that degrade the value or performance of the extracted watermark image. To implement these procedures, there are some approaches used and they are: Discrete Wavelet Transform and Principle Component Analysis.

KEYWORDS: Visible Watermark, Invisible Watermark, Principle Component Analysis

INTRODUCTION

In this paper, some watermarking schemes are to be described. In few past years, there has been a great increase in data exchanged through internet. As more the data will use, the security is also needed to protect the same data. To protect the data, digital watermarking is the most efficient way. The digital watermarking is a most popular technique of copyright protection. It hides the authorized information of the particular organization. The data can be hided in the form of digital image, video signals, audio signals or text. So, we have described some watermarking schemes in this paper. There may be two types of watermarking schemes: Visible Watermarking and another one is Invisible Watermarking. In both the techniques, there are two approaches are used. The approaches are: Discrete Wavelet Transform and Principle Component Analysis.

Multimedia data transmission over pubic network is gaining importance. To secure the multimedia data transaction over the internet, the data has to protect with any effective technique.

Digital image watermarking can be performed in two domains, one is spatial domain and another is frequency domain. The spatial domain is that when pixel values of any image are altered in order to hide authorized information and when the image is converted into the frequency components and these components are used to hide the authorized information, called frequency domain. In comparison to both the domains, the spatial domain is more effective and easy to perform than a frequency domain.

A good digital image watermarking technique needs some particular characteristics:

- **Robustness:** It is an ability of a system to cope with the errors during execution. The watermark image needs to be robust enough against various attacks like Gaussian noise, salt and pepper noise, JPEG compression, filtering, cropping, scaling and rotation.

- **Un-ambiguity:** It deals with the extracted image whether it is clear enough or not. The extracted image should be clear enough so that it can indicate the ownership of cover image without any ambiguity.

- **Imperceptibility:** It refers to the similarity between the original image and the watermarked image.

- **Capacity:** Capacity is how much amount gets embedded in the cover image as a watermark to protect the copyright information.

- **Blindness:** It is able to recover the copyright information with or without cover image. This copyright protection technique can be classified into two: one is blind and another is non-blind.

- **Security:** It refers to protect the embedded watermark image from the various attacks.

RELATED WORK

In this paper, we introduced a very robust watermarking technique which is based on two approaches. The approaches are: Discrete Wavelet Transform and Principle Component Analysis. We have taken two images one is cover image and another is watermark image. The cover is of 512px*512px and watermark image is of 64px*64px. There are two watermark techniques: Embedding Technique and Extraction Technique.

To embed a watermark in to the host cover image to protect the authorized information, it required a particular way to embed. By, using DWT the cover image is divided into four non-overlapping bands. The bands are: LL, HL, LH and HH. Here, LL band is used to embed the watermark. Before embedding procedure, LL band is being further separated into four non-overlapping bands. Then, embedding procedure followed.

To embed a watermark in to a host image or cover image the following steps have to be followed:

- Take an image of size 512px*512px as a cover image or host image.

- Convert the image from RGB to YUV format.

- Now, DWT is to be applied on a cover image or a host image to separate it into the four non-overlapping bands. The bands are LL, HL, LH and HH.

- Then, take one more image of size 64px *64px as a watermark image.

- To embed the watermark image in to the host image. Firstly, convert watermark image from RGB to YUV format.

- Select LL band to embed the watermark.

- Separate LL band into further four non-overlapping bands.

- Apply PCA to each block.

- Watermark is embedded.

- To set the transparency of the watermark image, the value of α has to be set. To get more transparency of the watermark image, the value of α has to be decreased and vice versa.
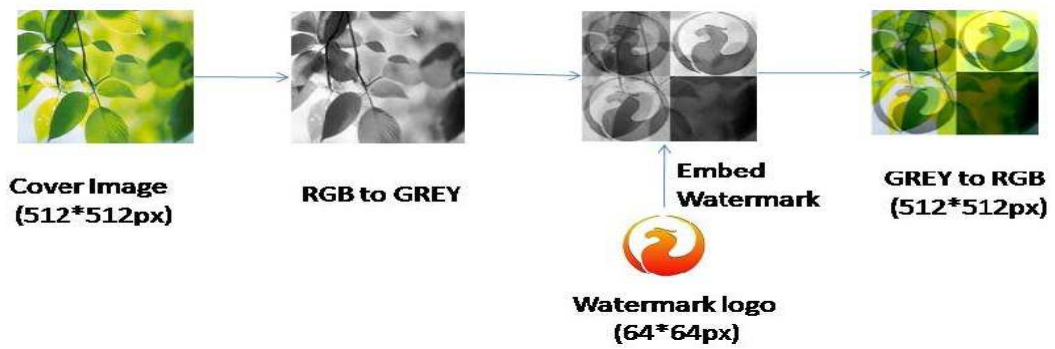
Figure 1: Embedding Scheme

Now, the logo has been embedded in the host image or cover image. And on the other end, the logo has to be extracted.

To extract the logo out from the host image, it has to follow some steps.

- Read watermarked host image to extract the logo out of it.

- Separate RGB bands.

- Decompose each band using 2-DWT.

- Select the sub-band LL to extract the logo.

- Apply PCA to each block in the chosen sub-band LL.

- The watermarking bits of logo are extracted from the principle component of each sub-block of LL band.
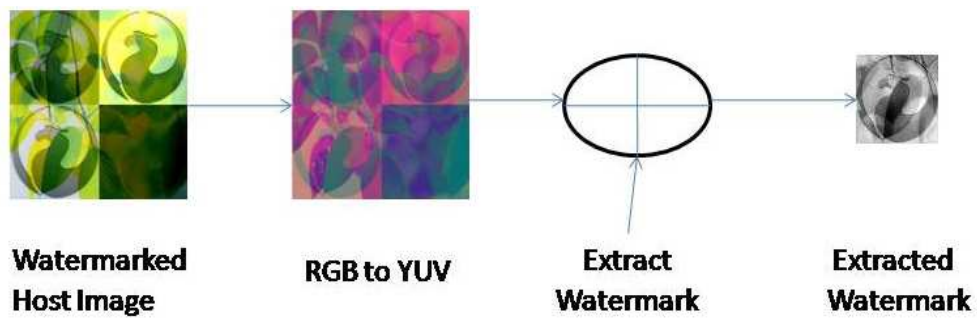

Figure 2: Extraction Scheme

Proposed technique is experimented on some images. Those images are:

- **Host Images (512*512px)**

Figure 3

- **Watermark Images (64*64px)**
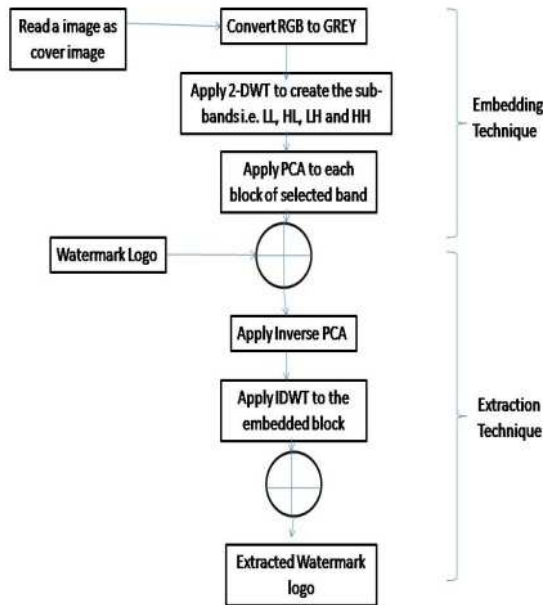

Figure 4

Figure 5: Block Diagram of Watermarking Schemes

CONCLUSIONS

In this paper, some watermarking techniques are described which are used to maintain the quality and imperceptibility of the watermark image. The techniques are embedding technique and extraction technique. All directional sub-bands are to be quantized based on the energy of the particular sub-band. To embed the watermark logo in to the host image, two approaches are used. Those are: DWT and PCA. There are some attacks, which affect the quality of the watermark image. To analysis the performance of the watermark, we are experimented the same techniques on the various images. On some results, we got the degradation of the quality and some are good. In the future work, to improve the robustness and imperceptibility of the watermark image, there can be used some more suitable techniques.

REFERENCES

1. R. B. Wolfgang, C. I. Podilchuk, E. J. Delp, *"*Perceptual watermarks for digital images and video," in *Proc. of theIEEE, Special Issue Identification and Protection of Multimedia Information*, Vol. 87, no. 7, pp. 1108 – 1126, July1999.

2. X. Xiang-Gen, C. G. Boncelet, G. R. Arce, "A multire solution watermark for digital images," in *Int. Conf. on Image Processing (ICIP'97),* vol. 1, pp. 548 – 551, 1997.

3. H. Liu, N. Chen, J. Huang, "A Robust DWT-Based Video Watermarking Algorithm", Proceedings of the International Conference on Signal and Image Processing Applications(ICSIPA), IEEE, pp. 352 – 356,2000.

4. X. Niu, S. Sun, "A New Wavelet-Based Digital Watermarking for Video," Proceedings of the 9th IEEE Digital Signal Processing Workshop, pp. 241 – 245, July 1999.

5. C. X. Wang, X. Nie, X. Wan, W. B. Wan and F. Chao, "A Blind Video Watermarking Scheme Based on DWT", Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE, Vol. 1, pp. 434-437, 2009.

6. N. Ahmidi and R. Safabakhsh, "A novel DCT-based approach for secure cooler image watermarking," in *Proc. Int. Conf. Information Technology: Coding and Computing*, Apr. 2004,vol. 2, pp. 709 – 713.

7. S. Voloshynovskiy, S. Pereira, T. Pun, "Watermark attacks," Erlangen Watermarking Workshop 99, October 1999.

8. G. Langelaar, I. Setyawan, and R. Lagendijk, "Watermarking Digital Image and Video Data: A State of - Art Overview," IEEE Signal Processing Magazine, Vol. pp. 20 – 46, Sep. 2000.