WATERMARK TECHNIQUE FOR AUTHENTICATION OF VISIBLY WATERMARK IMAGES

By
Dr. Mohammed K. Hassan, Software Engineering Dept.,
AL-Rafidain Univ. College,Baghdad,Iraq, Sept . 2009.
E.mail : mohamdhassan2004@yahoo.com

ABSTRACT

With the rapid spread of computer networks and the wide use of multimedia technologies, many watermarking techniques are now under development and investigation for protecting owner's intellectual rights. Watermarks can be divided into two types, visible and invisible watermarks, physical visible watermarks have been used for centuries. Now days it is used in digital library, in video broad casting, and other multimedia services. The visible watermark may face several problems. Among these problems, watermark removal and unauthorized insertion are two main concern.

This paper proposes a method of invisible watermark to overcome these problems. The watermarking process based on hiding a selected watermark object, that holds a little a mount of information relative to the source object, inside the cover image which has to be authenticated. The processes are based on using invisible watermarks to protect visibly watermarked images which are done by using different techniques. The experiments have shown that the proposed algorithm can provide a very effective protection for watermarked images.

تقنيات التحقق من العلامة المائية المستخدمة كعلامات ظاهرية في الصور لإثبات الأصل

د. محمد خضير حسن / قسم هندسة البرمجيات / كلية الرافدين الجامعة
بغداد – العراق أيلول - ٢٠٠٩

E.mail : mohamdhassan2004@yahoo.com

ملخص

أن الانتشار السريع والواسع لشبكات الحاسبات واستخدامها تقنيات متعددة الأغراض فان هنالك العديد من تقنيات العلامة المائية التي هي تحت التطوير والتحقق لحماية حق الملكية الفكرية وتقسم العلامة المائية إلى نوعين هما العلامة المرئية والعلامة الغير مرئية وان العلامة المادية المرئية تستخدم منذ قرون وتستخدم في الوقت الحاضر في المكتبات الالكترونية وفي البث الإعلامي وفي الأعلام الفديوي وفي أوساط متعددة إعلامية خدمية أخرى . إن العلامة المائية المرئية ممكن إن تواجه مشاكل عديدة ومن بين هذه المشاكل التي تم الاهتمام بها هي إزالة هذه العلامة أو الإدخال الغير مخول لها.

إن الورقة تتضمن طريقة مقترحة باستخدام العلامة الغير مرئية للتغلب على هذه المشاكل وان العمليات الخاصة بالعلامة المائية تستند في عملها على إخفاء العلامة المختارة والتي تحمل معلومات قليلة تخص المصدر الرئيس في صورة الغطاء المطلوب التحقق من صحتها. إن عمليات العلامة المائية تستند على استخدام علامة مائية غير مرئية لحماية صوره ذات علامة مائية مرئية وبأ استخدام تقنيات مختلفة. حيث أظهرت التجارب التي أجريت فعالية الطريقة المؤثرة في الحماية للصور ذات العلامات المائية .

1. INTRODUCTION

There are many techniques have been used for watermarking process to protect the owner's intellectual property rights. Appropriate protection method relies on the kind of data and environments. Visible watermarks are useful for protecting online images because they discourage unauthorized copying [1].

Visible watermarking requires each watermark should be easily visible , unobtrusive, and hard to remove. From the commercial point of view the last requirement is very important. Although we can use a number of methods to make the visible watermark difficult to remove, but we have to admit that removal is not impossible[٢].

Visible watermark holds a certain logo does not constitute a proof of ownership. That is, some one can insert the logo of others within an image and claim that the resulting image comes from them. Due to the existence of such threats, it is necessary to develop a new mechanism to protect visibly watermarked images[٣].

This paper proposes an invisible watermarking technique in the dual watermarking system to provide additional protection for visibly watermarked images. It first describes the properties and requirements of such an invisible watermark , then the details of the watermarking algorithm are explained.

2. NEW WATERMARKING TECHNIQUE

The following items have to be considered to explain the new watermarking:

2.1 Problem Analysis

Visible watermark has two main problems associated with it :-

1- The watermark must be difficult to remove.

2- The watermark must be able to withstand the impersonator problems.

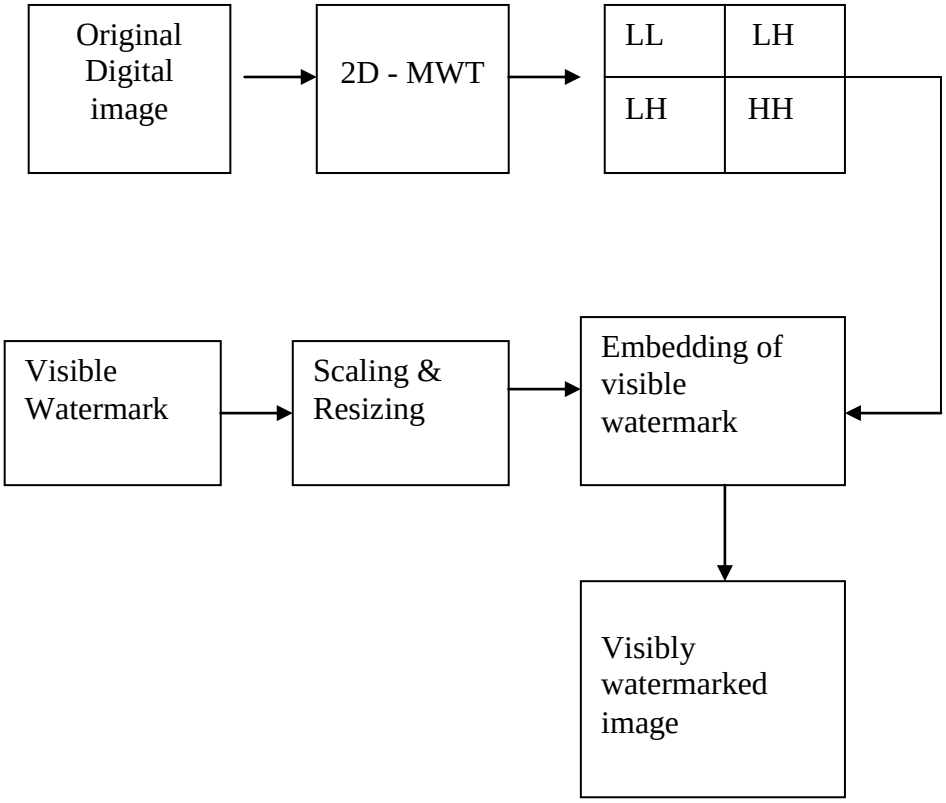
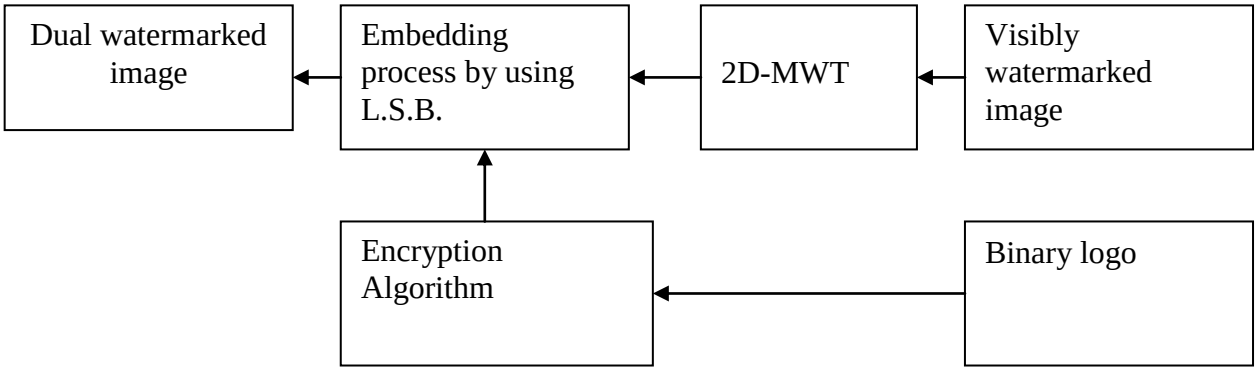


FIG (1) Block Diagram of the Visible Watermark Embedding Process



FIG(2) Block Diagram of the Invisible Watermark Embedding Process

Most of the published papers are concentrated on solving the first problem and few papers published on the second one. The researcher proposed an invisible fragile watermarking scheme to determine whether the watermark is genuine or unauthentic by detecting the alteration to the image[1].

2.2 Some Applied Methods.

In [4] , Mohanty presented a dual watermarking technique to detect the intentional and unintentional tampering of the image, his idea based on visible and invisible watermarking algorithms.

They used DCT based visible watermarking technique algorithm to embed a gray – level watermark image and this image regarded as a new image to carry out the invisible watermark. Invisible watermark is carried in spatial domain[5]. The fragile watermark is consisting of pseudo random number { 0,1} in binary sequence, it EX-ORed with K-th bit of bit plain of

the image. All bit planes (EX-ORed and non EX-ORed) of the image are merged together to obtain the final invisible watermarked image.

With the help of invisible watermark detection algorithm, any tampering in the visible watermark image can be known. However, the invisible watermark can detect any changes, but it is unable to tell whether those changes are targeted at the embedded visible watermark or the visibly watermarked image.

In [6], Wong and Memon used an invisible authentication watermark to ensure the identity of visibly watermarked image. Any modification to the visible watermark would be reflected in a corresponding error in the fragile watermark, However their scheme is too sensitive to be used in most practical applications.

The disadvantages of using fragile watermarks can be described as follows :-

1. Common image processing such as compression, filtering, noise addition or geometric distortion can not hinder the embedded visible watermark from indicting ownership. But they can destroy the fragile watermark easily[7].
2. When the owner's visible watermark is visually removed or tampered, or replaced by another unauthorized visible watermark , one can not identify the right owner to the image with fragile watermarking scheme.

   Based on the above analysis, we can conclude that the fragile watermarking scheme is not the most suitable one for this application. So we need a robust instead of fragile invisible watermarking scheme in the dual watermarking system[8].

2.3 The Properties of Robust Watermark :-

1. The watermark should be invisible and has no apparent interference with the visibly watermark image.
2. The watermark is desirously extracted without resorting to the visibly watermark image.
3. The watermark must be difficult to remove and can resist non malicious changes such as image compression and malicious attacks such as image replacement.

   It is desirable for the invisible watermark to survive most attacks that the visible watermark can survive. Visibly watermarked images are usually compressed for online use[4].

So malicious attacks may be targeted at the compressed/ decompressed version of images. Such challenge to the watermark technique is to make the invisible watermark robust against operations like compression and image in painting (image manipulation)[9].

2.4 Robust Invisible Watermarking Algorithm

The most important challenge to the invisible watermark is the resistance to compression and image inpainting. Compression has low pass nature. The invisible watermark has been chosen to be embedded in the low-pass sub-band of a three –level wavelet decomposition image. The selection of three level decomposition is to make the number of low pass coefficients large enough for watermarking embedding.

The embedding and extraction strategy is based on the used method. The process of watermarking detection is inverse manner of embedding for extracting the watermark.

2.5 Constructing invisible watermarks

Many forms of ***invisible watermark*** can be used. In this paper we choose the watermark in the form of ***binary image*** of the ***embedded visible watermark*** so that the ***extracted logo*** can indicate the ownership without additional computing. To increase the security of the invisible watermark, the invisible watermark is shuffled with some techniques like chaotic mapping before embedding.

3. DETAILS OF COMPUTATION PROCESS

The embedding process block diagram of visible watermark and invisible watermark are shown in Fig(1) and Fig(2) respectively.

3.1 Constructing invisible watermark

The main block diagram of visible watermark image authenticated by invisible watermark is shown in fig(3) .The Algorithm of the processes is consisted of :-

Step 1: Input desired visible watermark : The input colored image is converted to gray scale image and resized by using *imresize* function Math-Lab facility to make its size of (127 *127) pixels then displayed as shown in Fig (9).

Step 2: Watermark is converted to binary form to be used as an invisible watermark for authentication by using Math-Lab function Facility.

Step3 : Rearrangement of the binary form for invisible watermark, regarded as an encryption method to increase security measures, and to make ready for embedding process in the cover image Fig(5).

Step4 : Selection of cover image for input signal and converted to gray scale image and resized it by using *imresize* function, Math –Lab facility to make its size of (512 * 512) pixels as in Fig(8)

Step 5: Transformation processes of cover image : This process includes 2D-MWT (Two Dimensions Multi-wavelet Transforms), which explained in attached appendix -1.The LL band (Lowe-Low band of 2D-MWT) is selected. The result of the 2D-MWT as shown in Fig(6), which can be reconstructed again as shown in Fig(7).

Step 6: Embedding Process for invisible watermark by using the L.S.B. (least significant bit)technique : After converting the values of pixels of the watermark image to a stream of binary form. The pixel values of the

cover image are also converted to binary form to be more convenient for hiding information. Then each 8 bits of the watermarked image is stored in a sequential locations in the covered image. Then hide each bit of the watermark in the position of the least significant bit of each byte of the covered image. After that a sequential processes have done for the other pixel values to be embedded in the cover image as shown in Fig(10).

Step 7: Inverse Process **:** In this stage inverse 2D –MWT is taken to get back the cover image.

Step 8: Display both invisible and visible watermarked image.

3.2 Post processing extracted invisible watermark

Step 1: To recover the invisible watermark ,a reverse sequence of the steps has been followed to get the binary form the invisible watermark. After taking the 2D-MWT of the cover image ,the encrypted binary bits of the invisible watermark is extracted from the LL band of 2D-MWT.

Step 2: Decrypt the invisible watermark **:** This process includes re-arrangement of the unencrypted binary bits of invisible watermark and put them in a good order. As shown in Fig(4).

Step 3: Display the invisible watermark to authenticate the visible watermark

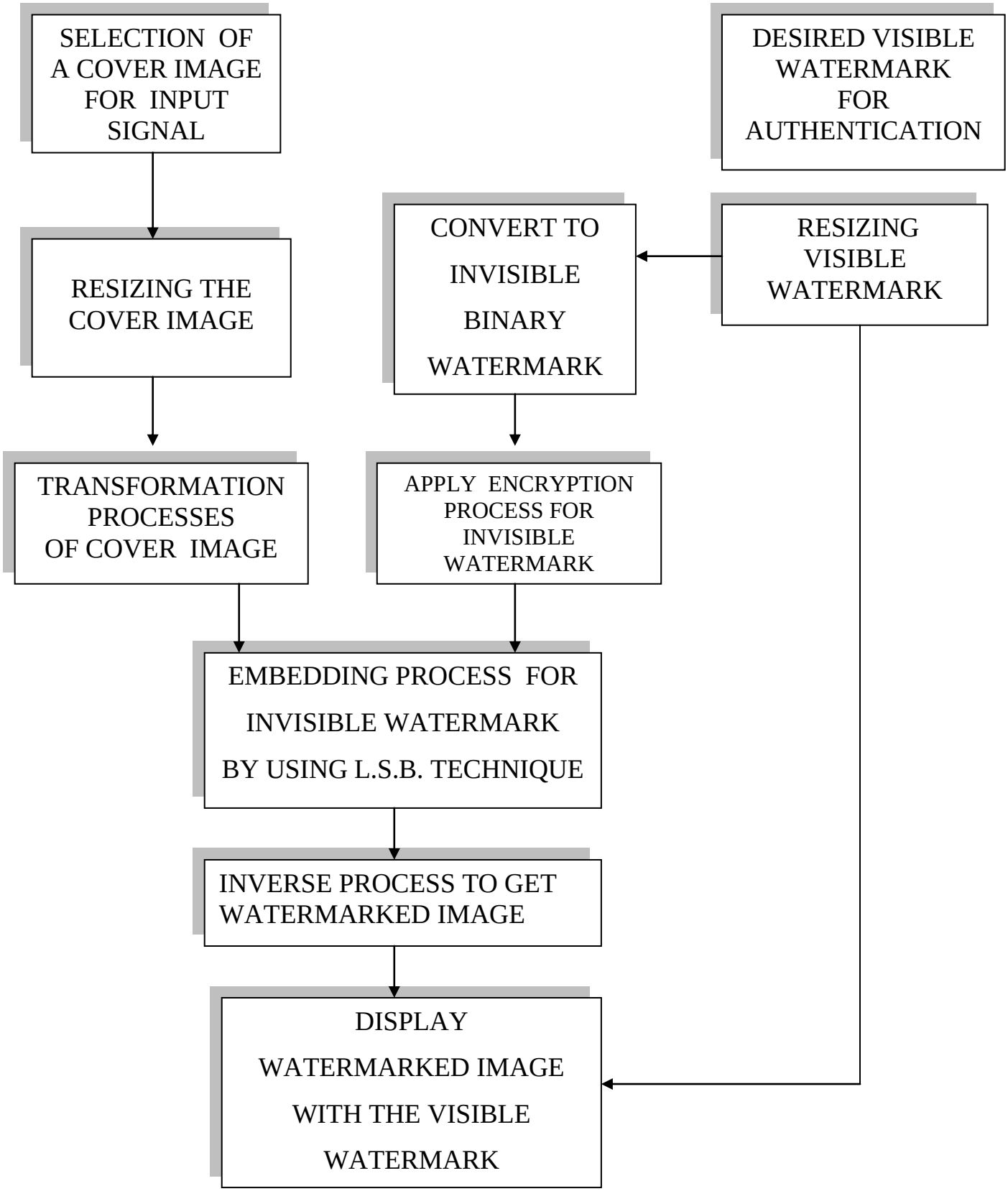
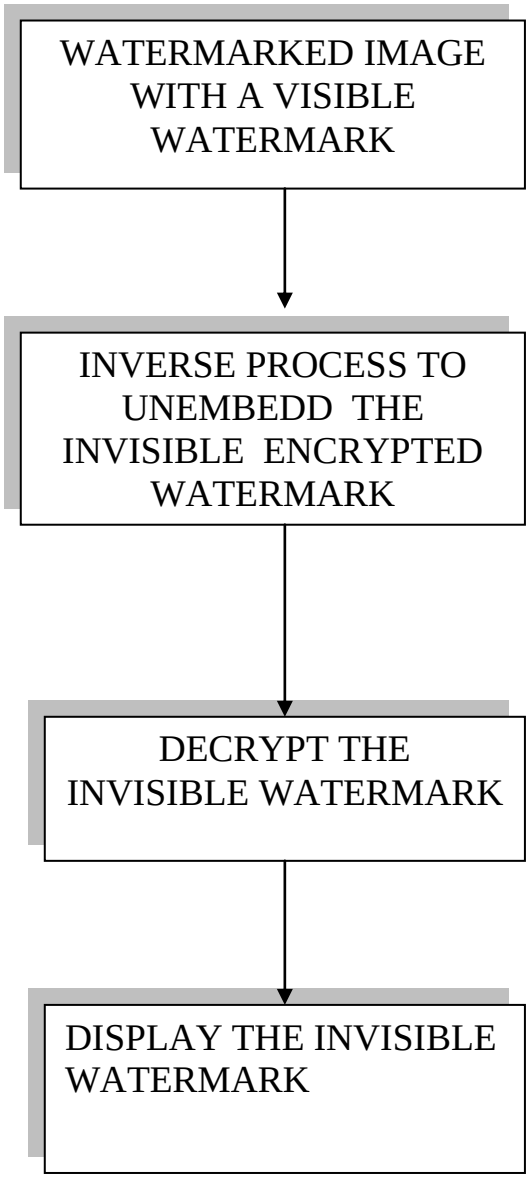


FIG (3) The Main Block Diagram of Visible Watermark Image Authenticated by Invisible Watermark Image



FIG(4) The Main Block Diagram of Un -embedding process to Get the Invisible Watermark

Fig. (5) Input of 2D image

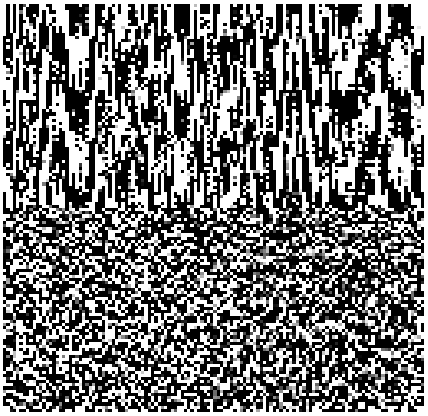


Fig. (6) Output of 2D MWT

Fig(7) Reconstructed 2D image from 2D MWT

Fig. (8) Input of 2D cover image

Fig. (9) 2D watermark image

Fig(10) Output of 2D Watermarked Image

4- RESULTS AND CONCLUSION

Many experiments have been performed to demonstrate the effectiveness of the proposed algorithm. The experimental results on the horse image (512 x 512) pixels as a cover image, and the size of the watermark (small horse image) equal to 64 x 64 pixels. The computer that has been used is pentium 4 with a processor of 1.7GHZ.

After performing visible watermarking , the visibly watermarked image is obtained as shown in the fig (8).This image is then processed with the proposed invisible watermarking scheme to produce to produce the dual watermark image as shown in fig (10).The dual watermark image has a very high PSNR (peak signal to noise ratio) around 40 db. Therefor the insertion of invisible watermark has very small impact on the image quality. If there is no effect or interferences on this dual watermarked image, the invisible watermark ,binary logo, can be easily extracted. But if there is some effect like compression processing , the invisible watermark can be constructed with some watermark bit lost .

The proposed method is a good way for protecting visibly watermarked images. The algorithm of invisible watermark must be robust and also the methods of embedding, extracting and post processing.

Many factors has to be consider in choosing watermark and one of these factor, is the size should be small in order not to cover wide area of the cover image.

The future work has to concentrate on enhancement of robustness of the embedding of the watermark against geometric attack.

The research on dual watermarking system is very significant for practical application of visible watermark. Because of paper length limitation the details is made briefly.

REFERENCES

[1] Mintzer, " Developing digital libraries of cultural content for internet access," IEEE Communications Magazine, Vol.37, jan.1999,pp 72-78

[2] CH. Huang, and J.L. Wu, "Inpainting attacks against visible watermarking schemes", Proc. SPIE Conf. on Security And Watermarking of Multimedia Contents, vol.SPIE 4314,2001,PP.376-384.

[3] P.W. Wong and N. Memon,"Secret and public key image watermarking schemes for image authentication and ownership verification", IEEE Trans. on image processing, vol.10, Oct.2001 pp.126-132

[4] S.P.Mohanty" A dual watermarking technique for images", ACM multimedia(2),1999,pp.49-51

[5] Rafael C. Gonzalez, Paul Wintz " Digital Image Processing", 2004.

[6] P.W. Wong and N.Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification",IEEE on image processing. Vol.10,Oct,2001,pp.1593-1601

[7] Thomas Braunl, Stefan Feyrer "parallel image processing ", 2006.

[8]Y. Hu, and S. Kowng, " Wavlete domain adaptive visible Watermarking " Electronics Letters. Vol.37,Sep. 2001, pp 1219- 1220

[9] Scott E. Umbaugh, "Computer Vision image processing ", 2006