Watermarking Hiding Techniques

علياء هاشم محمد *

المستخلص

الاعمال الرقمية معرضة للاستنساخ الغير المشروع والتوزيع. العديد من المالكين يتمنون في بعض الوسائل تعريف حق الملكية وحقوق الطبع. العلامة المائية الرقمية تؤدي هذا الدور وتوفر وسائل لتعريف وتعقب الاعمال الرقمية. مع ذلك اخفاء العلامة المائية ربما يفشل نتيجة للهجوم بواسطة الاقتصاص او التشويه مثل التنعيم والتدوير.

اقترحنا طرق جيدة لإخفاء العلامة المائية في الصورة الثابتة وطورنا عدد من التقنيات السابقة لزيادة القوة ضد الهجوم. ذلك يوفر حماية حق الملكية وعندما تتعرض العلامة المائية في الصور للهجوم فأن ممكن ان نضمن بقاء واحدة او اكثر بدون تشويه وذلك بواسطة تكرارها عدة مرات داخل الصورة.

الطرق التالية اقترحت ونفذت لاخفاء العلامة المائية:

- Improved LSB وتتضمن (LSB cloud, Improved Butterfly method)
- JPEG وتتضمن طريقتين (Before Quantization method, After Quantization method)
- GIF Change Local Palette

Abstract

Digital works are subject to illicit copying and distribution. Many owners wish for some means of identifying ownership and copyright. Digital watermarks can fulfill this role and provide a means to identify and track digital works. However, embedded watermarks may fail to be recognized due to attack by cropping or distortions such as smoothing, rotation and scaling. Good techniques were proposed to embedding watermarking in still images and many previously techniques were improved to increasing the robustness against attack, which provide copyright protection.

When watermarking image exposed to attack can guarantee one or more watermark remain without distortion. The following methods of hiding watermark are suggested and implemented: Improved LSB (which consist of two methods " LSB cloud" and "Improved Butterfly method"), GIF Change Local Palette, JPEG method (consist of two methods "Before Quantization method" and "After Quantization method").To ensure watermark is hiding in image, we apply the extraction process to extract the watermark from image.

*مدرس مساعد قسم الحاسبات كلية الادارة والاقتصاد الجامعة المستنصرية

1. Introduction

Today, large amounts of multimedia data are available to every one and can easily be accessed e.g. via the Internet, digital broadcasting of radio and TV programs or satellite communication channels for the home user. Since all these channels provide content in digital format, every one is able to duplicate the received data without provide loss of quality and without asking for permission to do so. This is clearly advantageous, in that it is easier to market and sell one's works. But this brings to front a potential problem, which has resulted in pirating. This is often referred to as the digital world's problem [Neub98].

How do authors claim ownership rights of such digital media if multiple persons have exact copies?

One method is to embed additional information and only the legitimated distributed the media contains this additional information. The embedded information is known as a watermark can provide, for example information about the media, the author copyright or license information [Jone00, John99].

In other words, A digital watermark is digital signal or pattern inserted into digital content. The digital content could be a still image, an audio clip, a video clip, text document, or some form of digital data that creator or owner would like to protect.

Copyright Law is "In essence, copyright is the right of author to control the reproduction of this intellectual creation". When a user reproduces a work that has been copyrighted, without the permission of the owner, a user may be held liable for copyright infringement. To prove copyright infringement, a copyright owner needs to prove two things: -

1. A user owns the copyright in the work, and
2. The other party copied the work (usually determined by establishing that the other party had access to the copyright work, and that the copy is " substantially similar" to the original).

In cases where it cannot be said that the owner's work and the possible illegal copy are identical, the existence of a digital watermark could prove guilt [Jone00].

2: The Purpose of Digital Watermarks

The main purposes of digital watermarks are:-

1. The aim to mark digital data permanently and unalterably, so that the source as well as the intended recipient of digital work is known. Copyright owners can incorporate identifying information into their work. That is, watermarks are used in the protection of ownership. The presence of a watermark in a work suspected of having been copied can prove that it has been copied.
2. By indicating the owner of the work, the demonstrate quality and assure the authenticity of the work.
3. With a tracking service, owners are able to find illegal copies of their work on the Internet. In addition, because each purchaser of the data has a unique watermark embedded in owner copy, any unauthorized copies that user distributed can be traced back to owner.
4. Watermarks can be used to identify any changes that have been made to the watermarked data.
5. Some more recent techniques are able to correct the alteration as well. [Jone00]

3: Digital Watermark Types

There are several approaches in classify watermarking systems. One could categorize them according to the watermarking powerful against types of attack.

1.Fragile Watermark: - is embedded in digital data for the purpose of detecting any changes that have been made to the content of the data and identify where it has taken place and possibly what the signals was before modification. They achieve this because they are distorted, or "broken", easily by data manipulation. A fragile watermarks are publicable in image authentication systems.[Vanw01, Katz00, Kutt01]

2. Semi-Fragile Watermark:- watermarks detect any changes above a user- specified threshold [Jone00]. On the other words, A semi-fragile watermark is mark, which is (highly) sensitive to a modification of the digital data [Kutt01].

3.Robust Watermarks:- are designed to survive " moderate to severe signal processing attacks". In such a way that any signal transform of reasonable strength cannot remove the watermark. Robust watermarks are publicable in image copyright protection and fingerprinting. [Jone00, Kutt01]

4: Design and Implementation of Watermarking System

The proposed system stands for two main processes, these are:-

1. Embedding watermarking in the still image by using one from many proposed techniques of watermarking hiding.

The proposed system takes as an input the watermarking text and the cover-image (which may be one of those image format BMP, GIF, and JPEG image) then embedded watermark text in image to introduce the watermarking image as an output.

2. The proposed system is extracting the watermark from image when image received to the other side without any attack.

4.1: Hiding Watermark:

The proposed system use three main methods for hiding the watermarking in (BMP, GIF, and JPEG) file format image. These methods divided into classical methods and new suggestions methods. The classical hiding methods in (BMP) was improved to prevent some attacks from distorted watermark embedded by its.

The block diagram of hiding watermark system is shown in figure (1)

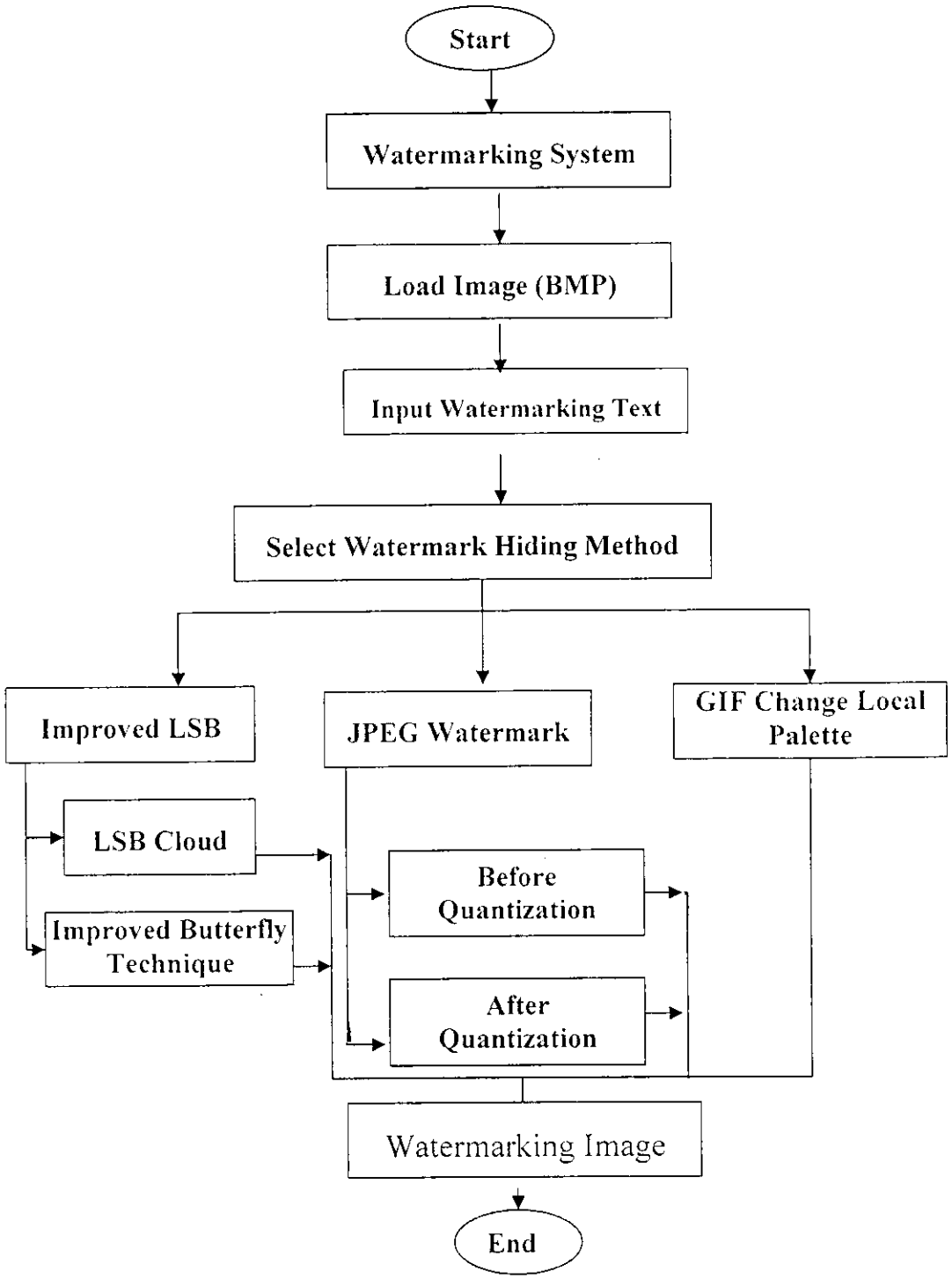


Figure (1) Watermarking System

Bellow explains of these methods:-

4.1.1 Improved LSB:

The original LSB method uses the least significant bit to hide the watermark or information. In this method we suggested to improve the original LSB by embedded the watermark in many locations in image. Before starting the hidden operation, the proposed system will subdivided the image to sub image, and check the sub image by using the statistical averaging to find the good sub image for insertion the watermark data. This operation repeated for many times. This method sub divided into two types dependent on the mechanism of hiding.

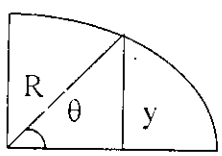
- LSB Cloud Technique:

The first method will hide the watermark similar to cloud and the shape of the cloud drawn by the equations (1) and (2)

$\text{Cos}(\theta)=x/R \Longrightarrow x= R^* \text{Cos}(\theta)$ ...(1)

$\text{Cos}(\theta)=y/R \Longrightarrow y=R^*\text{Sin}(\theta)$ ...(2)

Where R is the radius of the curve and θ is angle (we will be select these parameters to gain the pixels of the cloud shape). As in the following curve:



Improved Butterfly Technique:

The second method used the improved butterfly technique. The original butterfly technique based on partition the cover image into four triangles (left, right, top, and bottom). The left and right triangles

respectively for embedding process. If we use all the pixels that are lie in the left and right triangles and draw the image, it will be like a butterfly. The information will be embedded in the left and right triangles respectively.

In the watermarking system an improvement to the butterfly technique by sub divided the image to (10X10) pixels and applied this technique to all sub images.

4.1.2 JPEG Watermark

JPEG compression considers lossy compression. This can impact on any hidden watermark in the image.

- JPEG Image Format

The main JPEG compression steps are outlined below:

1.Color images are transformed from RGB into a luminance color space. The most common color space is RGB, where the three parameters are the intensities of Red, Green, and Blue in a color.

Luminance is defined as radiant power weighted by a spectral sensitivity function that's characteristic of vision. The eye is very sensitive to small changes in luminance, which is why it is useful to have a color space that use Y as one of their three parameters. A simple way to do this to subtract Y from the Blue and Red parameters of RGB, and use the three parameters Y, B-Y and R-Y as a new color space. The YCbCr ranges are appropriate for component digital video and JPEG. Conversions between RGB and YCbCr are straight forward:

Y=(77/256)R+(150/256)G + (29/256)B, Cb= -(44/256)R- (87/256)G + (131/256)B + 128,

Cr= (131/256)R – (110/256)G- (21/256)B +128;

R=Y+1.371(Cr-128), G=Y- 0.698(Cr-128)- 0.336(Cb-128),B=Y+ 1.732(Cb-128) ... (3)

2.The pixels of each color component are organized in groups of (8*8) pixels called data units. If the number of images rows or columns is not a multiple of 8, the bottom row and the rightmost column are duplicated as many times as necessary. The discrete cosine transform (DCT) is then applied to each data unit to create an 8*8 map of frequency components

$$F(u,v)=\frac{C(u)C(u)}{4}\sum_{j=0}^{7}\sum_{k=0}^{7}F(j,k)Cos\left[\frac{(2j+1)u\pi}{16}\right]\quad Cos\left[\frac{(2k+1)u\pi}{16}\right]\ldots\ldots(4)$$

$$Where\quad C(w)=\begin{cases}\frac{1}{\sqrt{2}} & For w=0\\ 1 & otherwise\end{cases}$$

$$F(j,k)=\frac{1}{4}\sum_{u=0}^{7}\sum_{v=0}^{7}C(h)\,C(v)\,F(u,v)\,Cos\left[\frac{(2j+1)u\pi}{16}\right]\quad Cos\left[\frac{(2k+1)v\pi}{16}\right]\ldots\ldots(5)$$

$$Where\quad C(w)=\begin{cases}\frac{1}{\sqrt{2}} & For\ w=0\\ 1 & otherwise\end{cases}$$

3. Each of the 64 frequency components in a data unit is divided by a separate number called "Quantization Coefficient" (QC), and then rounded to an integer. This is where information is irretrievably lost. Larger QCs. Each of more loss, so the high frequency components

typically have larger QCs. Each of the 64 QCs is a JPEG parameter and can, in principle, be specified by the user. In practice most JPEG implementations use the QC tables recommended by the JPEG standard.

4. The 64 quantified frequency coefficients (which are now integers) of each data unit are encoded using Hufman coding.

5. The last step adds headers and all the JPEG parameters used, and outputs the result. In specialized applications, where the same parameters are always used, the parameters don't have to go on the output stream, which saves a few hundred bytes. The JPEG decoder performs the reverse step.

The watermarking system hide watermark by two methods of JPEG technique. These are watermarking before quantization and watermarking after quantization.

Sample of Standard Quantiztion Table

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

1. Watermarking Before Quantization:- This algorithm of watermarking hide before quantization equation applied for the image.
2. Watermarking After Quantization: This algorithm of watermarking hide after quantization equation applied for the image.

4.1.3 GIF Change Local Palette

In this method, the proposed system will load the GIF file format image then hide the watermark into the local palette of image. After complete hiding process, the system will re-sort the palette of image.

The palette will be sorted, and then change the old palette index of the image-pixels to the new-sorted palette index.

The luminance method, which sort the palette according to its luminance calculated by Equation (6)

$$L = 0.299 \times Red + 0.587 \times Green + 0.114 \times Blue \quad (6)$$

To prevent the effective of re-compression attack, watermark hides in the palette and in the image itself.

4.2: Extraction Watermark Process

To perform the extracting watermark process, we must have the watermarking image. By using the extracting process we will gain the watermark- text.

The extraction processes performing by inverse hiding processes. The block diagram of extraction watermark system is shown in figure (2)

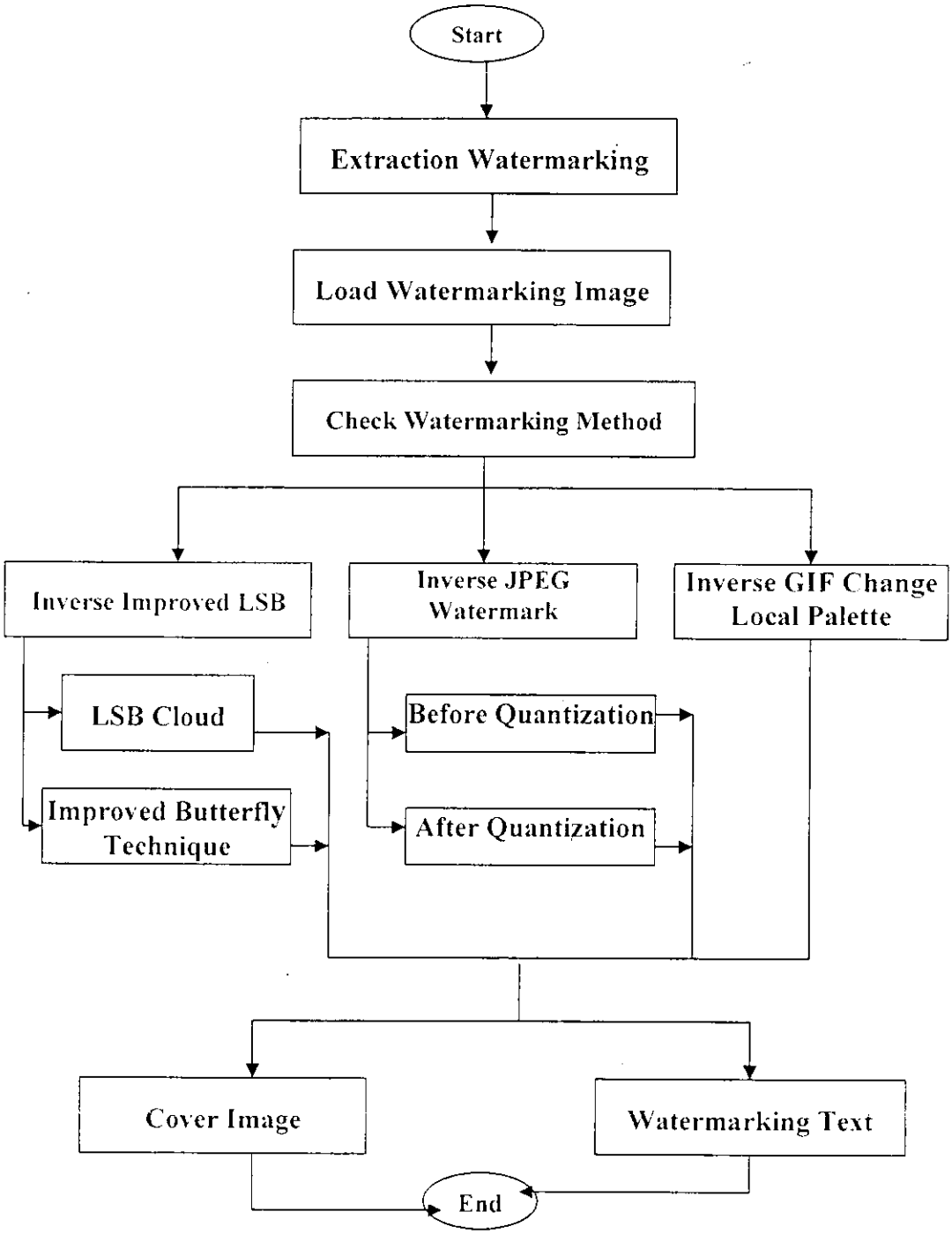


Figure (2) Extraction Watermarking System

5: Conclusions:

We produce the system to hiding watermark in image. In the following are some points concluded from this study.

1. The recovery process is simpler in GIF format from BMP format.
2. Using hiding method in GIF change local palette by re-sort palette prevent the effective of re-compression attack.
3. LSB cloud technique provide unknown shape to hide information which prevent attacker from known or estimate where and how hide information.

9: Refrences:

[Neub98]

C. Neubauer, J. Herre, K. Brandenburg, *"Continuos Steganographic Data Transmission using Uncompressed Audio"*, Information Hiding, Second International workshop, Lecture Notes in computer science, vol. 1525, pp.208-217, Springer , 1998.

[Jone00]

N. Jones, *"Digital Watermarks and Protection of Ownership"*, Computer Science Honours, 2000.

[John99]

N. F. Johnson, *"An introduction to Watermark Recovery from Images"*, George Mason university, 1999, PDF,

[http://issue.gmu.edu/~csis].

[Katz00]

S. Katzenbeisser and F. Petitcolas, *"Information Hiding Techniques for Steganography and Digital Watermarking"*, Artech House pub. 2000,USA,[http://www.ifi.unizh.ch/~oppliger/series editor.html].

[Kutt01]

M. Kutter, *"Digital Watermarking Frequently Asked Questions (FAQ)"*, watermarking world, 2001, [http://www. watermarking world.org]

[Vanw01]

A. K. Vanwasi, *"Digital Watermarking- Steering The Future of Security"*, Home Archives, Securi ty- Network magazine, 2001.

.....

.....

.....