QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

Unbreakable Digital Watermarking Technique

Abdulkareem O. Ibadi
Computer Engineering Department, Baghdad university college for economic sciences, Baghdad - Iraq

ARTICLE INFO

Article History:
Received: 8 March 2017
Accepted: 1 April 2017
Published: 10 April 2017
DOI:
10.25212/lfu.qzj.2.2.45

Keywords:

Digital Watermarking,
Image Watermarking

ABSTRACT

In this research, a new concept of watermarking method is introduced; it is suitable for any type of information file. It doesn't make any change on the watermarked file. The concept is to store secure watermarking file (SWF) in a reliable third party (RTP). SWF is generated by locating the logo file in the watermarked file. SWF is formatted in special compressed form and can be compressed and encrypted using any suitable application.

1. Introduction

The threats of copyright are grown up on the owner's mind, so they always try to secure their data from these threats by merging the owner ID with digital media. This process is called Watermarking; the proof of ownership is done by extracting the owner ID from the digital information file.

The protection of ownership of digital information becomes important concerns with the ease of editing and reproduction. Digital watermarking, a scheme to embed special labels in digital sources, has made considerable progress in recent years. There are several categories of watermarking schemes [1]. Watermarking can be robust or fragile. In robust watermarking technique, the modification to the watermarked content will not affect the watermark. But fragile watermarking is a technique in which watermark gets destroyed when watermarked content is modified or tampered with [2].

Among them, fragile watermarking is a technique to insert a signature for image authentication. The signature will be altered when the host image is manipulated.

An effective authentication scheme should have desirable features that the embedded authentication data is to be invisible under normal viewing conditions; and to allow the watermarked image be stored in lossy compression format.

In other hand, the patent must be registered to save the owner rights. The registration itself means a patent protection. Although patent registration protect the intellectual rights, some patent can't be registered like cars company industrial secrets, military weapon industries, secure communication applications and techniques, ..,etc.

Besides, the ideation in some fields can't be protected from being stolen like literatures and arts. Therefore a new concept or type of watermarking is needed.

In this paper, a new concept is discussed for watermarking any type of information files with the condition that the size of the watermarked file must be greater than the size of the logo file in mostly small ratio.

2. Image Watermarking

Digital image watermarking is derived from steganography where content is hiding with other content for secure considerations. The difference between them is that in steganography the hidden data is in a highest priority while in watermarking the cover and the hidden data are both in highest priority [3].

Watermarking must have four properties to reach its goal they are:

a) **Effectiveness**

b) **Host signal Quality**

c) **Watermark Size**

d) **Robustness**

Effectiveness means the watermarking process must be detective. The second property insures that watermarking process will minimize the host changes. The third property provided that the watermarking should be of minimum size. The robustness property is to be withstanding against threats [4].

3. Applications of watermarking

Some of the watermarking applications are listed hereby [5]:

a. **Copy Protection:** this is done by integrating the copying device with the watermarking detection.

b. **Broadcast Monitoring:** broadcasting and TV channels are monitoring by watermarking.

c. **Medical applications:** using watermarking to protecting patients documents from being altered.

d. **Fingerprinting**: detecting the legal fingerprint using watermarking techniques.

e. **Data Authentication:** watermarking is used with data transmission for hast authenticity.

f. **Owner Identification:** watermarking is used to identify the ownership of a digital media.

4. Watermarking models

Watermarking process can be modeled in two classifications they are [6]:

a. **Communication-based models**: in this type watermarking is a process of communication; a secret message is embedded in a cover in the sender side and extracted in the receiver side as shown in figure 1. Communication-based watermarking models can be divided into two sub-categories also. Using side-information to enhance the process of watermarking and without using side-information at all.

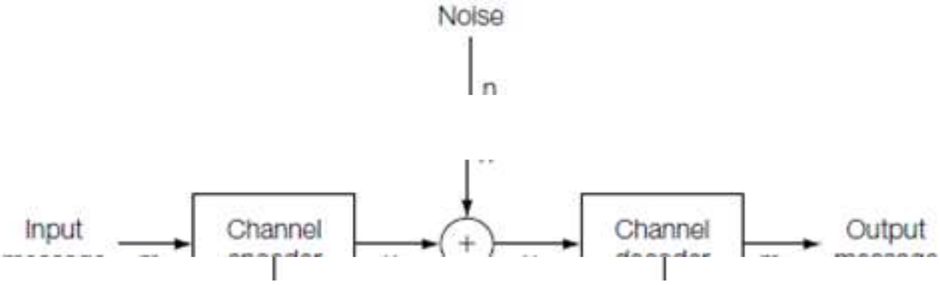


Figure 1. The communication-based model

b.Geometric models: in geometric model, watermarking can be viewed as high-dimensional vectors called the media space and using a number of regions of desirable properties of the image like embedding region and detection region.

5. Types of watermarking

Watermarking can be classified Based on the type of document as [7]:

- Image Watermarking
- Video Watermarking
- Audio Watermarking
- Text Watermarking

Based on processing method used, watermarking can be classified as:

- Spatial-domain techniques
- Transform-domain techniques

On the basis of necessary data for extraction, watermarks can be divided in to two categories:

a. Blind

b. Informed

In blind watermarking original document is not required during watermark detection process. But in informed, original document is required during watermark extraction process.

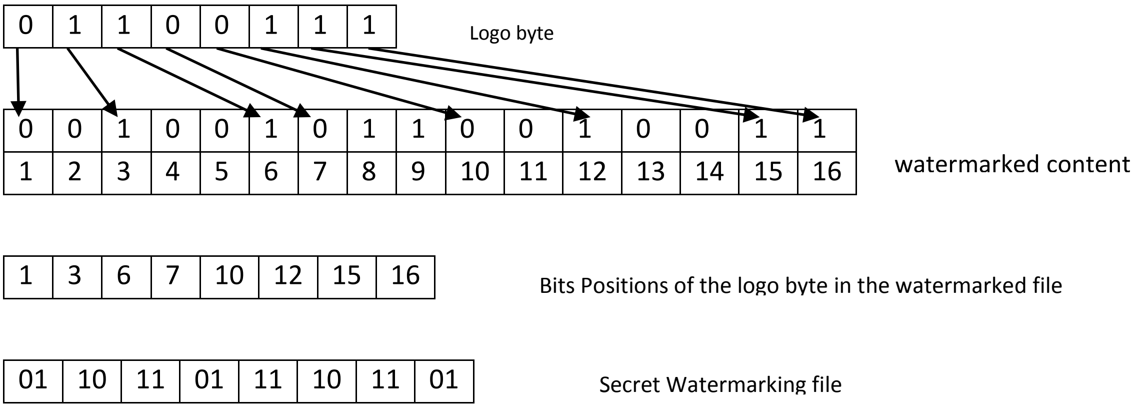
6. The Proposed Authentication Method

The proposed authentication method can be discussed as two phases: the watermarking phase and the extraction phase which are explained in the next sections.

6.1 Watermarking Phase

The idea behind the proposed method is to take the logo file bit by bit and looking for the equivalent bits in the watermarked file and storing the positions in another separate file, so it is not a hiding operation therefore the hidden file will be called logo file and the cover file will be called the watermarked file.

For example the logo byte in figure 2, need to be located in two bytes of the watermarked file.



Logo byte

0	1	1	0	0	1	1	1

watermarked content

0	0	1	0	0	1	0	1	1	0	0	1	0	0	1	1
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Bits Positions of the logo byte in the watermarked file

1	3	6	7	10	12	15	16

Secret Watermarking file

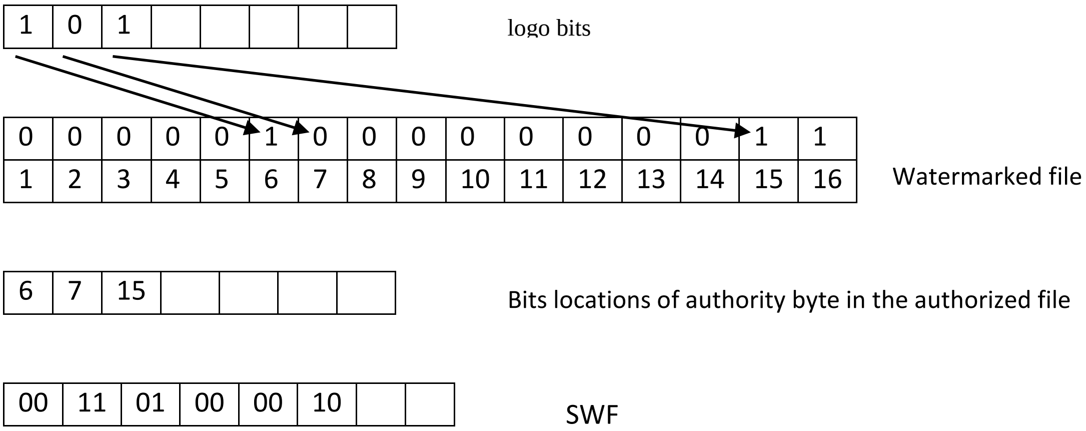
01	10	11	01	11	10	11	01

Figure 2. The proposed authentication

The first bit of the authority byte is located in the first location in the cover file, the second is located in location number 3, the third bit in location six, and, so on the last bit of the hidden byte is located in location number 16. These locations must be stored in a secret file to be retrieved in the extraction operation.

The locations file is written in a special new designed format called the Secret Watermarking File (SWF). Each location in SWF is represented by two bits which explain the difference between each two adjacent locations. The first two bits represent the location of the first bit of the logo file in the watermarked file, the second two bits represent the difference between the second location and the first, the third two bits represent the difference between the third location and the second, and so on the i^{th} two bits is the difference between the i^{th} location and the previous location.

If the difference between locations is greater than three, the 00 state is used to mean that add 3 to the pointer as shown in figure 3.



1	0	1					

logo bits

0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Watermarked file

6	7	15				

Bits locations of authority byte in the authorized file

00	11	01	00	00	10		

SWF

Figure 3. Locations treatment of SWF

The first location is 6, which is represented in SWF as "00","11" and means add 3 to the binary value "11" which is equal to 6, the second location add "01" to the last location which is equal to 7, the difference between 15 and 7 is 8, which is greater than 3, "00" is inserted and subtracting 3 from 8 which equal to 5. 5 is greater than 3, "00" is inserted and subtracting 3 from 5, by subtracting 3 from 5 the value 2 is less than 3 so the binary value "10" is inserted.

6.2 The Extraction Phase

SWF file must be securely stored in the owner database or any reliable application to be used in the extraction process. As in the previously discussed, SWF contains the locations of the logo file contents (bits) in the watermarked file, and once getting SWF the user can retrieve the logo file from the watermarked file.

The extraction method starts by reading SWF which begins by the location of the first logo bit in the watermarked file and storing it in a new file called the extracted file, then reading the location of the second bit and appending it to the extracted file, and so on, until reaching the end of SWF. The last 21 bits in the extracted file are three characters represent the extension of the logo file, so the extracted file will have this extension to be viewed in the viewer application.

7. Secure Authentication Files Management

The output of the proposed authentication method is the secure watermarking file (SWF). SWF size is as the double of the hidden file or greater, when a suitable compression method is used SWF size might be tenth of the logo file size.

SWF is needed to be store in a secure database located in a Reliable Third Party (RTP) which may be a global agency for this specific activity. Once a file ownership prove is needed, SWF will be used to rebuild the logo file from the watermarked file.

If someone needs to save the ownership of digital information, he must generate its SWF and store it in RTP without saving the original information file. RTP will save the name of the owner and send an index number to the owner which must kept for future watermarking proof as shown in figure 4. The index number represents the index of information SWF in the RTP database. The smaller authority number will win the ownership of specific digital information if it has more than one index number.

Anyone has to send the original information file and its authority number to the RTP to prove his ownership of this information. ATP saving other extra information to prove the sender is the owner of the authority number.

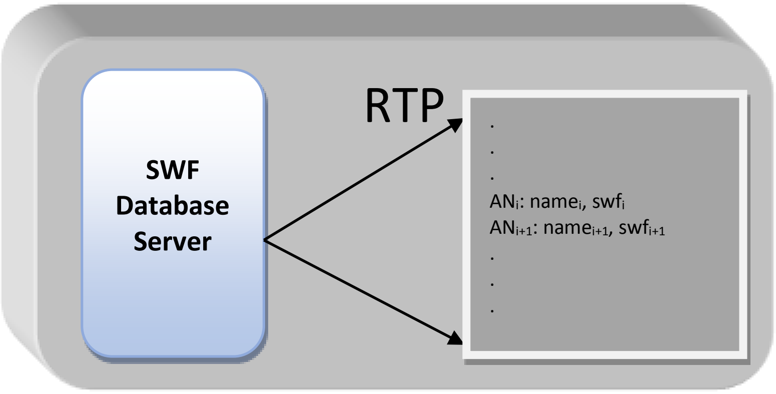

SWF Database Server
RTP
.
.
.
AN_i: $name_i$, swf_i
AN_{i+1}: $name_{i+1}$, swf_{i+1}
.
.
.

Figure 4. Reliable third party

Anyone has to send the original information file and its index number to the RTP to prove his ownership of this information. RTP saving other extra information to prove the sender is the owner of the index number.

8. Evaluations

○ The proposed watermarking method is a new type of authentication concept it is suitable for any type of digital information files. The watermarking process performed without inserting or editing the watermarked file.

○ The logo of the owner will play a great role in this method. The logo file must be unique, reserved and clearly describe the owner. The experiments show that the size of the information file must be greater than the double of the logo file size. This condition can be easily performed by extending the size of the information file by repeating the information or by inserting some remarks.

○ RTP must be one of the greatest companies in the world like Google, Yahoo... etc. because it is reliable, well-known and has infrastructure enough to perform this authentication method.

○ The method is called "Unbreakable" because it looks like a document registration in a secure place (RTP), and breaking the method means attacking RTP.

○ By using this method anyone can authenticate any unnecessarily published or secret information.

9. References

[1] F. Mintzer, G. W. Braudaway, M. M. Yeung: "Effective and Ineffective DigitalWatermarks", ICIP,1997.

[2] Jaseena K.U., Anita John, "Text Watermarking using Combined Image and Text for Authentication and Protection ", *International Journal of Computer Applications (0975 – 8887), Volume 20– No.4, April 2011*

[3] Lalit Kumar Saini, Vishal Shrivastava,"A Survey of Digital Watermarking Techniques and its Applications", (IJCST) – Volume 2 Issue 3, May-Jun 2014

[4] Prabhishek Singh, R S Chadha ,"A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 9, March 2013

[5] Mei Jiansheng, Li Sukang, "A Digital Watermarking Algorithm Based On DCT and DWT", Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China, May 22-24, 2009, pp. 104-107

[6] Melinos Averkiou, " Digital Watermarking", paper, 2015.

[7] M. Chandra, S. Pandey, R. Chaudhary, "Digital Watermarking Techniques for Protecting Digital Images", IEEE, 2010.