Cryptography based digital image watermarking algorithm to increase security of watermark data

Preeti Gupta

Abstract—Digital watermarking is one of the proposed solutions for copyright protection of multimedia data. This technique is better than Digital Signatures and other methods because it does not increase overhead.

Digital Watermarking describes methods and technologies that hide information, for example a number or text, in digital media, such as images, video or audio. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data.

In this paper cryptography based Blind image watermarking technique presented that can embed more number of watermark bits in the gray scale cover image without affecting the imperceptibility and increase the security of watermarks.

Index Terms—Blind watermark, Cryptography, Decryption, Encryption, Gray scale, Watermarking, Security.

1 INTRODUCTION

It is well known that digital images can be altered or manipulated with ease. Furthermore, it is generally impossible to tell whether a given image is authentic or has been altered subsequent to capture by some readily available digital image processing tools. This is an important issue in, for example, legal applications, news reporting and medical archiving, where the digital image in question truly reflects what the scene looked like at the time of capture.

In the security domain, an integrity service is unambiguously defined as one, which ensures that the sent and received data are identical. This binary definition is also applicable to images. In real life situations, images can be transformed, their pixel values can be modified but not the actual meaning of the image.[1] Security and capacity of watermark data are very important issues to be considered. Watermarking is an emerging research area for copyright protection and authentication of electronic documents and media. Most of the research is going on in this field, spatially in the field of image watermarking. The reason might be that there are so many images available at Internet without any cost, which needs to be protected.

1.1 Information Hiding

Information hiding means communication of information by hiding in and retrieving from any digital media. The digital media can be an image, an audio, a video or simply a plain text file. Information hiding is a general term encompassing many sub disciplines. However, generally it encompasses three disciplines: cryptography, watermarking, and steganography. It is graphically shown in figure 1.1. Watermarking can be robust or fragile depending upon the application domain.

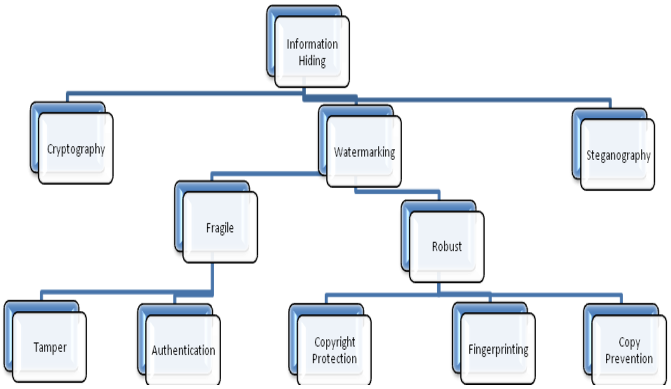

Figure 1.1 A Classification of Information Hiding Techniques

2 DIGITAL WATERMARKING

A digital watermark is a signal permanently embedded into digital data (audio, images, video, and text) that can be detected or extracted later by means of computing operations in order to make assertions about the data. The watermark is hidden in the host data in such a way that it is inseparable from the data and so that it is resistant to many operations not degrading the host document. Thus by means of watermarking, the work is still accessible but permanently marked.

Digital watermarking techniques derive from steganography, which means covered writing (from the Greek words stegano or "covered" and graphos or "to write"). Steganography is the science of communicating information while hiding the existence of the communication.

2.1 Why Digital Watermarking?

Digital watermarking is an enabling technology for e-commerce strategies: conditional and user specific access to

- *Preeti Gupta pursuing masters degree program. in Computer Science from Rajasthan Technical University, Rajasthan, India. PH-+919783811424 E-mail: er.preeti11@gmail.com*

services and resources. Digital watermarking offers several advantages. The details of a good digital watermarking algorithm can be made public knowledge.

Digital watermarking provides the owner of a piece of digital data the means to mark the data invisibly. The mark could be used to serialize a piece of data as it is sold or used as a method to mark a valuable image. For example, this marking allows an owner to safely post an image for viewing but legally provides an embedded copyright to prohibit others from posting the same image.

2.2 General Framework for Watermarking

The digital watermarking system essentially consists of a watermark embedder and a watermark detector (Figure 2.1). The watermark embedder inserts a watermark onto the cover signal and the watermark detector detects the presence of watermark signal. Note that an entity called watermark key is used during the process of embedding and detecting watermarks. The watermark key has a one-to-one correspondence with watermark signal (i.e., a unique watermark key exists for every watermark signal). The watermark key is private and known to only authorized parties and it ensures that only authorized parties can detect the watermark. Further, note that the communication channel can be noisy and hostile (i.e., prone to security attacks) and hence the digital watermarking techniques should be resilient to both noise and security attacks [9].

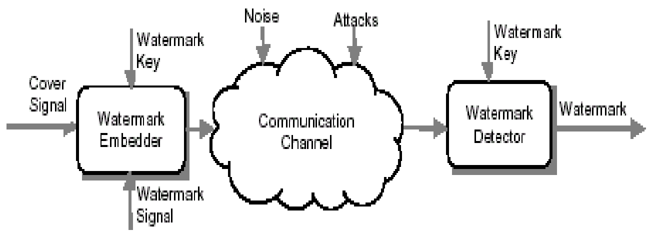

Figure 2.1 General watermarking system

2.3 Types of Digital Watermark

Watermarks and watermarking techniques can be divided into various categories in various ways. Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows: [1]

i. Text Watermarking
ii. Image Watermarking
iii. Audio Watermarking
iv. Video Watermarking

In other way, the digital watermarks can be divided into three different types as follows:

i. Visible watermark
ii. Invisible-Robust watermark
iii. Invisible-Fragile watermark

2.4 Attacks

Watermarking techniques should be tamper resistant to hostile attacks. Depending on the application, the watermarked content encounters certain types of attacks. Some types of attacks are more important than others. Some basic types of attack are:

2.4.1 Active attacks

Here the hacker tries to remove the watermark or make it undetectable. This type of attack is critical for many applications, including owner identification, proof of ownership, fingerprinting, and copy control, in which the purpose of the mark is defeated when it cannot be detected. However, it is not a serious problem for authentication or covert communication.

2.4.2 Passive attacks

In this case, the hacker is not intended to remove the watermark, but to detect its presence or existence of a covert communication. In most of the above mentioned application areas, we are not concerned by this type of attack. In fact, we mostly use visible watermarks making it evident that a watermark exists. But for covert communication, the main concern is to hide the existence of a watermark.

2.4.3 Collusion attacks

These are a special case of active attacks, in which the hacker uses several copies of one piece of media, each with a different watermark, to construct a copy with no watermark. Resistance to collusion attacks can be critical in a fingerprinting application, which entails putting a different mark in each copy of a piece of media. However, the number of copies that we can expect the hacker to obtain varies greatly from application to application. A collusion attack would require that several employees conspire to steal the material, which is an unlikely prospect.

2.4.4 Forgery attacks

Here, the attacker tries to incorporate a valid watermark, rather than removing one. These are our main security concern in authentication applications, because if hackers can embed valid authentication marks, they can cause the watermark detector to accept forged or modified media. This type of attack is a serious concern in proof of ownership.

3 WATERMARK EMBEDDING AND EXTRACTION

A watermark, which is often consists of a binary data sequence, is inserted into a host signal with the use of a key [6]. The information embedding routine imposes small signal changes, determined by the key and the watermark, to generate the watermarked signal. This embedding procedure (Fig. 3.1) involves imperceptibly modifying a hoist signal to reflect the information content in the watermark so that the changes can be later observed with the use of the key to ascertain the embedded bit sequence. The process is called watermark extraction.

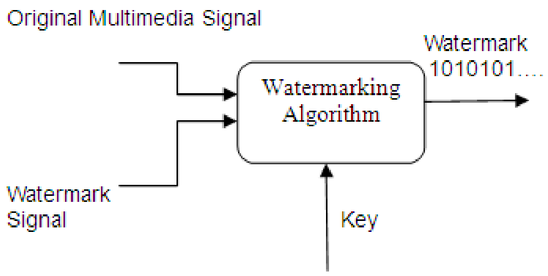

Fig. 3.1 Watermark embedding process

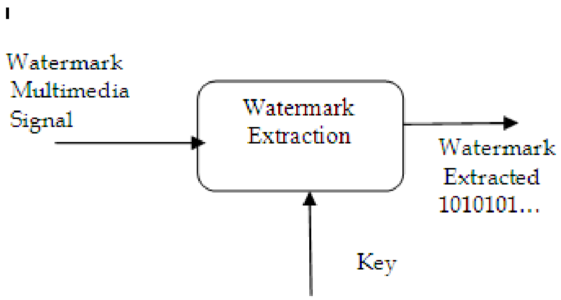

Fig. 3.2 Watermark extraction process

4 Cryptography based Blind Image Watermark Algorithm

4.1 Watermark Embedding Algorithm

Input

Watermark 1 – a binary image act as a watermark that embed in the main watermark.
Watermark 2 – a binary image act as main watermark.
Cover Image – gray scale image to be watermarked.
E1 – key used for encrypting Watermark1
E2 – key used to encrypt watermarked watermark.
W1 – key used to embed encrypted binary watermark into the main watermark.
W2 – key used to embed encrypted watermarked watermark in Cover Image

Algorithm

i. Take Watermark1 and encrypt it by performing XOR operation with the key E1. The output of this step is called Encrypted1.
ii. Apply procedure to embed Encrypted1 in the second binary watermark image (Watermark2) using key W1. Let output image is Watermarked1.
iii. Again encrypt Watermarked1 using XOR with key E2 to give the output image Encrypted2.
iv. Apply procedure embed Encrypted2 in the gray-scale Cover Image using key W2. Output image is final watermarked image (Watermarked2).

Output

Watermarked2 – finally watermarked image

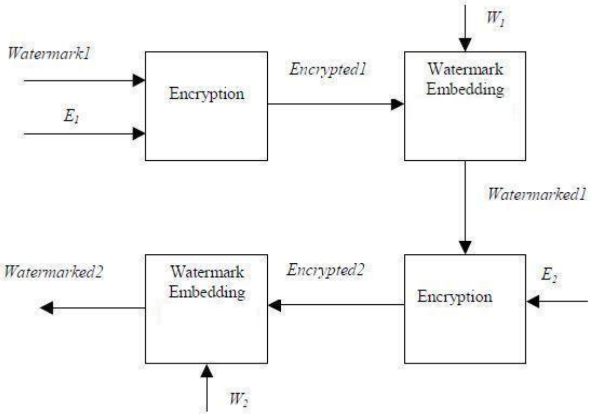

Figure 3.1 Block Diagram of Watermarks Embedding Procedure

4.2 Watermarks Extraction Algorithm

Input

Watermarked2′ – it is the received watermarked image.
S1 – size of watermark1.
S2 – size of watermark2.
E2 – key used to decrypt Recovered watermark from cover Image.
E1 – key used for decrypting Recovered Watermark from main watermark.
W2 – key used to recover encrypted watermarked watermark from Cover Image.
W1 – key used to recover encrypted binary watermark from the main watermark.

Algorithm

i. Apply procedure to extract encrypted watermark2 from Watermarked2 using key W2. say the recovered image is Encrypted2′.
ii. Decrypt Encrypted2′ using XOR with key E2.output of this step is called Recovered2.
iii. Apply procedure to extract encrypted watermark1 from Recovered2 using key W1. Recovered image is called Encrypted1′.
iv. Decrypt Encrypted1′ using XOR with key E1. Output of this step is called Recovered1.

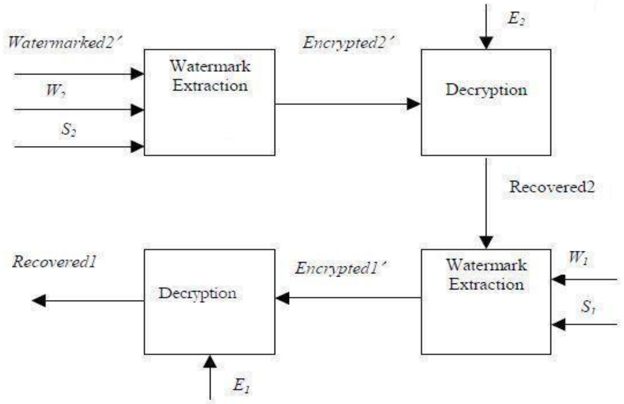

Figure 3.2 Block Diagram of Watermarks Extraction Procedure

Output

Recovered2 – main watermark recovered from the received watermarked image.

Recovered1 – watermark recovered from the main watermark.

5 CONCLUSIONS

The increasing amount of digital exchangeable data generates new information security needs. Multimedia documents and specifically images are also affected. Users expect that robust solutions will ensure copyright protection and also guarantee the authenticity of multimedia documents. In the current state of research, it is difficult to affirm which watermarking approach seems most suitable to ensure an integrity service adapted to images and more general way to multimedia documents.

In this paper, we have a blind watermarking technique that uses watermark nesting and encryption. Nesting means it embeds an extra watermark into the main watermark and then embeds the main watermark into the cover image. For encryption we used XOR operation. For embedding watermarked watermark in Cover Image we used DWT based technique. Proposed watermarking technique has following advantages:

By using watermark nesting we can embed more number of bits in the cover image as compare to without watermark nesting.

Due to nesting feature we can embed some metadata about watermark also. Because our technique uses encryption, so it increases the security of watermarks. For instance if watermarking key is hacked still the attacker will not be able to identify the watermark because it is encrypted.

It is a blind watermarking technique. So, original image is not required at the time of watermark recovery. Because we embed final watermark in DWT domain, so this technique is robust against many attacks.

REFERENCES

[1] Robert, L., and T. Shanmugapriya, "A Study on Digital Watermarking Techniques ", International Journal of Recent Trends in Engineering, vol. 1, no. 2, pp. 223-225, 2009.

[2] F. A. P. Petitcolas, R. Anderson, and M. G. Kuhn, "Information hiding - A survey", Proceedings of the IEEE, vol. 87, no. 7, 1999, pp.1062– 1077.

[3] ZuneraJalil, M. ArfanJaffar, and Anwar M. Mirza, "A Novel Text Watermarking Algorithm Using Image Watermark", International Journal of Innovative Computing, Information and Control (IJICIC) (indexed by ISI with Impact Factor 2.93) (Scheduled to be published in February, 2011)

[4] Alper Koz, "Digital Watermarking Based on Human Visual System", The Graduate School of Natural and Applied Sciences, The Middle East Technical University, pp 2 – 8, Sep 2002.

[5] Nikolaidis, S. Tsekeridou, A. Tefas, V Solachidis, "A Survey on Watermarking Application Scenarios and Related Attacks", IEEE international Conference on Image Processing, Vol. 3, pp. 991 – 993, Oct. 2001.

[6] Dr. Martin Kutter and Dr. Frederic Jordan, "Digital Watermarking Technology", in AlpVision, Switzerland, pp 1 – 4.

[7] Feng-Hsing Wang, Lakhmi C. Jain, Jeng-Shyang Pan, "Hiding Watermark in Watermark", in IEEE International Symposium in Circuits and Systems (ISCAS), Vol. 4, pp. 4018 – 4021, May 2005

[8] Hsiang-Kuang Pan, Yu-Yuan Chen, and Yu-Chee Tseng, "A Secure Data Hiding Scheme for Two-Color Images", in Fifth IEEE Symposium on Computers and Communications, pp. 750 – 755, July 2000.

[9] Lu, C. S., Huang, S.-K., Sze, C.-J., Liao, H.-Y., "A new watermarking technique for multimedia protection'', in Multimedia Image and Video Processing, L. Guan, S.-Y. Kung, and J. Larsen, Eds. Boca cRaton, FL: CRC, pp. 507 –530, 2001.

[10] Voyatzis, G., Pitas, I., "Digital Image Watermarking using Mixing System", in Computer Graphics, Elsevier, vol. 22, no. 4,pp. 405-416, August 1998

[11] Harpuneet Kaur, R. S. Salaria, "Robust Image Watermarking Technique to Increase Security and Capacity of Watermark Data", The IASTED International Conference on Communication, Network, and Information Security (CNIS–2006), MIT, Cambridge, Massachusetts, USA, Oct 9–11, 2006. (Communicated)

[12] Zhao, Y., Campisi, P., Kundur, D., "Dual Domain Watermarking for Authentication and Compression of Cultural Heritage Images", in IEEE Transactions on linage Processing, vol. 13, no. 3, pp. 430-448, March 2004.

[13] Saraju Prasad Mohanty, "Watermarking of Digital Images", Submitted at Indian Institute of Science Bangalore, pp. 1.3 – 1.6, January 1999.

[14] K. Vanwasi, "Digital Watermarking - Steering the future of security" Edition 2001, available at http://www.networkmagazineindia.com/200108/security1.html