Image Waterkmarking Tool with Self-Deleting Mechanism

An Independent Study

Presented to

The Faculty of the Computer Studies Division

Ateneo de Davao University

In Partial Fulfillment

of the Requirements for the Degree

Bachelor of Science in Computer Science

By

Milcah Penetrante

Gian Kim Jose Isulat

Jaquelyn Lagbas

SCHOOL OF ARTS AND SCIENCES

ATENEO DE DAVAO UNIVERSITY

OCTOBER 2008

Ateneo de Davao University

COMPUTER STUDIES DIVISION

SCHOOL OF ARTS AND SCIENCES

P.O. Box 8016 Davao City

Philippines

Recommendation for Oral Defense

In partial fulfillment of the requirements for the degree of **BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY,** *this SENIOR PROJECT entitled*:

Image Waterkmarking Tool with Self-Deleting Mechanism

has been prepared and submitted by Gian Kim Jose Isulat, Jaquelyn Lagbas, and Milcah Penetrante and is recommended for ORAL PROPOSAL DEFENSE.

Mrs. Michelle Banawan

Adviser

TABLE OF CONTENTS

ABSTRACT

The rampant digital image posting and distribution increases the concern of most of the authors/artists on how to protect their works from modifications of other people. This study discusses a methodology for the development of a self-deleting image with fragile watermark for the security of still images or pictures.

Keywords:

Fragile watermark, self-deleting

CHAPTER 1

INTRODUCTION

1.1 Background of the Study

Many creative artists are blooming everywhere, from pencil and paper to *Photoshop* artists. Most of the time, this digital artwork is posted on the Internet and modified without permission which damages/distorts the original motif or beauty of the art. Also, some culprits take credit for the work of others since no proper detection is being used in proving the originality of the art. This is why digital watermarking is made to protect the authors from crooks who want to benefit from their work and destroy their precious creations.

With the help of digital watermarking, authors can now put a digital signature of their choice in their work for copyright purposes. This watermark will help the author control the modification or detect if a modification has been made in the work. A watermark can also contain information that can aid the author in tracking his/her work. Therefore, with the help of the watermark technology, unauthorized alteration can be minimized, if not prevented, to avoid the distortion of the real essence of the work and ownership theft.

But even with the presence of the existing watermarking technology, image alterations/modifications still abound. Some watermarks were not effective and robust enough in preserving the quality of the images. Recent technology allows the images to be modified even if it is embedded with watermark. Meaning, artists' masterpieces are not safe from thieves and a more effective watermark is needed.

The proponents created a new approach in digital watermarking, which improves identification of a copyrighted image file. In this improved technology, the watermark that will be embedded with hidden codes that will trigger self-deletion of both the watermark and the image once edited or modified.

1.2 Technology Application Context

Existing watermarking technologies have proved to be ineffective in addressing the pervasive problem of image file piracy and/or security. The problem on securing images is that the digital watermark is not that effective in maintaining the integrity of the authors' work due to alterations and/or modifications. Unsecured file will lead to distortion and theft of the authors' work. As the authors make their work available on the internet, their work must be protected from people who will use their masterpiece and change it for their own acknowledgement or any reason that they may have in pirating others' work. This security measure involves digital watermarking, which will keep the authors' identification in their work and protect the same from alterations. This will also include a private key, known only to the author so that he/she can modify his/her work when needed. In addition, a hash function will also be used to authenticate the watermark. Most importantly, the fragile watermark will be embedded within the image and will be used as a detector from any alteration.

1.3 Objectives of the Study

General objective for this research is to develop a digital watermarking tool that will trigger self-deletion of the once alteration/modification on the image is found.

Specific objectives are:

- To identify the use of hash functions on digital watermark.
- To create a structure/framework in self-deleting image embedded with fragile watermark.
- To create a fragile digital watermark tool that allows the image to be easily authenticated.

1.4 Significance of the Study

This study aims to support the Intellectual Property Rights policy by way of preserving the original properties of the image file. Watermarking will be used as a means of conveying ownership and can serve as a tool in impeding piracy that is currently destroying the real essence of digital art. Watermarking can be used as a restriction for other people from modifying a work. Once the image is watermarked, it will be protected from any alteration or modification. It can also serve as an authenticating factor which will serve as the finger print of the author in his/her work.

This study is significant for artist specifically digital image owners/authors. Through a self-deleting image using fragile watermark, authors will be able to

protect their work from any modification and/or alteration by other people. Through this watermarking utility, it will be hard for culprits to modify the work of others.

Digital authors watermark their work to advertise or commercialize their work. Through a visible watermark, the author's signature can easily be seen, thus making him/her famous. Watermarking can also serve as a marketing strategy. An author can make a low-resolution watermarked image for advertising his/her work, and then, he/she can sell a high-resolution image for those who want to have a copy of the said work.

1.5 Scope and Limitations of the Study

The study generally focuses in a technology that will create fragile watermarking tool that triggers image self-deletion once an alteration/modification is detected. The fragile watermark will be embedded with codes, which will authenticate and trigger a deletion script for the altered image.

It shall be implemented on still images or pictures on JPEG format and will run on UNIX based and on WINDOWS operating systems, and the image can be open to any image editor or viewer. The modification will only be apply in image editor or viewer only; using the image in a document (i.e. copying and changing its color or editing it) cannot be said as being modified because once it is save, it is save as a document, and one cannot export back image into a JPEG format. Captioning can be done in two ways: visible watermark and invisible watermark. It is the author's decision what to use in his/her work. If it is visible

watermark then the author's name or signature can be seen as other people copy it. If it is invisible watermark, the author's name or signature cannot be seen since it is hidden, but the watermark is still there. The proponents will use open source software in embedding the fragile watermark in the image. The fragile watermark embedded in the image will be the one that will tell whether the image is modified or not. If it is modified, then the self-deleting mechanism will be triggered. In the self-deleting mechanism, a script is considered as the tool in creating the application and will perform destruction of the image after any modification/alteration.