International Journal of Information Technology and Knowledge Management
July-December 2008, Volume 1, No. 2, pp. 289-294

AN IMAGE RESTORATION APPLICATION: PIXEL-DIGITAL WATERMARKING OF USER CREATED IMAGES

Milind Kumar V. Sarode, S. A. Ladhake & Prashant R. Deshmukh

Abstract

The most obvious and first question is what is "watermarking"? The process of embedding information into another object or signal can be termed as watermarking. In other words digital watermarking is a technique, which allows an individual to add hidden copyright notices, or other verification messages to digital audio, video, or image signals and documents. Such hidden message is a group of bits describing information pertaining to the signal or to the author of the signal (name, place, etc.). The technique takes its name from watermarking of paper or money as a security measure. Digital watermarking is not a form of steganography, in which data is hidden in the message without the end user's knowledge, although some watermarking techniques have the steganographic feature of not being perceivable by the human eye. Historically, watermarking has been used to send "sensitive" information hidden in another signal. Watermarking has its applications in image or video copyright protection. Basically WATER MARKING has its application for ownership protection.

Keywords: Watermarks, Steganography, Tracking, Embedded watermark, Tracking agent.

1. Introduction

The advent of the Internet has resulted in many new opportunities for creating and delivering content in digital form. Applications include electronic advertising, real time video and audio delivery, digital repositories and libraries, and Web publishing. An important issue that arises in these Applications is protection of the rights of content owners. It has been recognized for quite some time that current copyright laws are inadequate for dealing with digital data. This has led to an interest in developing new copy deterrence and protective mechanisms. One approach that has been attracting increasing interest is based on ***digital watermarking*** techniques.

The main idea behind this work is to prevent the users to change the original image, to check whether the image is the original image or not, to prevent the ownership of the image etc .As we all know, Images are a major part of Digital Media, we use images as wallpapers, digital-art, photos, cover-pages etc. Now-a-days Images/videos are also playing a vital role in judiciary processes to prove crimes and punish the criminals. We have developed software named **PIXEL,** which can be used as digital water marker for JPEG/BMP images for embedding Text/Images as a digital watermark in the JPEG/

BMP images. The watermark is 100% invisible and the embedding process is lossless (i.e. it dose not even disturb/changes the image quality by 0.001%).

2. USE OF DIGITAL WATERMARKING

First applications that came to mind were related to copyright protection of digital media. In the past duplicating artwork was quite complicated and required a great expertise for that the counterfeit looked like the original. However, in the digital world this is not true. For everyone it is extremely easy to duplicate digital data and this even without any loss of quality. Similar to the process in which artist artistically signed their paintings with a brush to claim their copyrights; artists of today can watermark their work and hide for example their name in the image. Hence, the embedded watermark will allow identifying the owner of the work. It is clear that this concept is also applicable to other media such as digital video and audio.

3. WATERMARK MONITORING

A watermark monitor is a device which sits at a place and receives images broadcasted from satellites, or downloaded images via surfing the Internet. With the wide availability of many spiders or robots that are indexing millions of images and documents, it would be easy for the watermark monitor to check the images that have been indexed by these spiders in their databases (such as AltaVista or Yahoo). Since watermark extraction requires the secret key, a monitor can be only dedicated to the detection of the watermarks that were embedded in one secret key or a few secret keys. In the latter case, the monitor must apply each of all secret keys to each image in order to find the watermark. When a watermark monitor is dedicated to detect the owner-watermark, it produces reports to identify who is using the images that are owned by a specific entity. By comparing the reports with licensing records, copyright infringements can be easily found. When a watermark monitor is dedicated to detect the recipient-watermark, it reports who has illegally distributed copyright protected images.

4. WATERMARK TRACKING AGENT

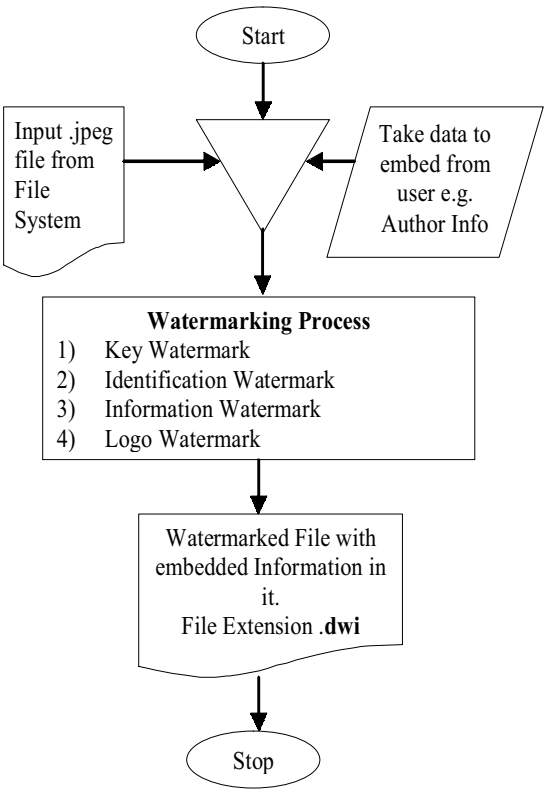
A watermark agent acts like a 'detective' to trace any illicit copies by detecting watermarks and verifying the usage rights of the image. A watermark agent is mobile, for example, traveling from server to server on the Internet to check watermarks of the local images and send reports to the watermark clearinghouse and/or dispatcher. The security of this agent is a major concern. In addition to the security concerns at the language level, i.e. determination of whether the agent will attempt to infect the server, deny service to other agents, an important security and privacy issue which has arisen from the watermark agent is: to prevent anyone on the network from detecting confidential information, such as a watermarking key and detection reports, while the

agent is migrating from host to host. Both watermark monitoring and tracking agent require a knowledge database to guide them in locating and traveling. We propose a centralized knowledge base built incrementally by the feedback and analysis of the watermark monitoring and tracking. For example, a site where illicit copies were detected should be visited frequently by the agent in the future.

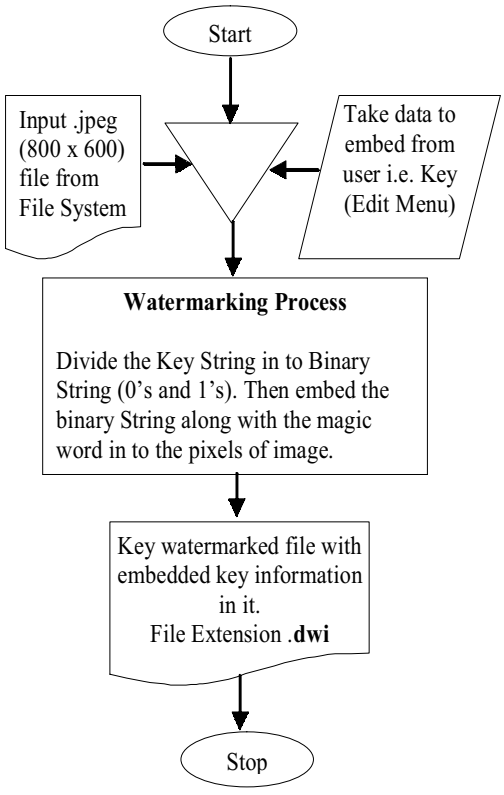
5. ANALYSIS

For the implementation of providing invisible watermark to the user created JPEG images without disturbing the originality of the image. And to allows an individual to add hidden copyright notices or other verification messages into a user created jpeg images and to control the piracy of an images. As we know the analog and visible digital watermark can easily breakable so that it challenge to the security so there is need of providing such type of watermark which cannot be broken or change. In today's era of the digital world digital images play vital role in multimedia sector.

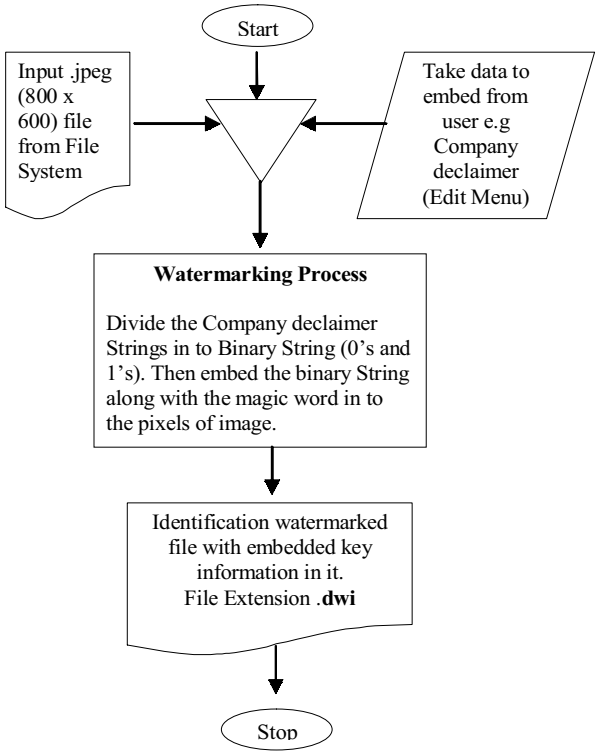
Flow Chart for Pixel-The Digital Water Marker



Flowchart for Key Watermark



Flowchart for Logo Watermark



5.1 Result Analysis

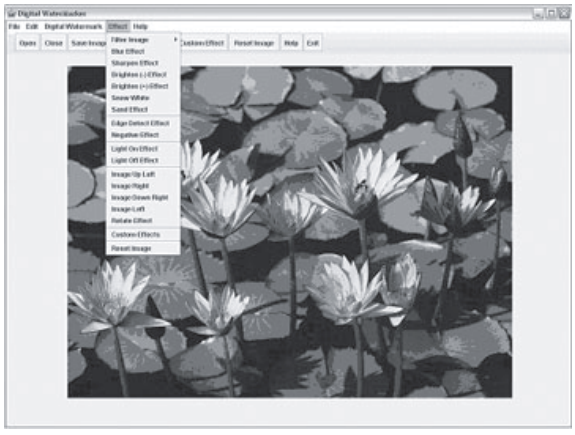


Figure 1: Provided Effects to the Image

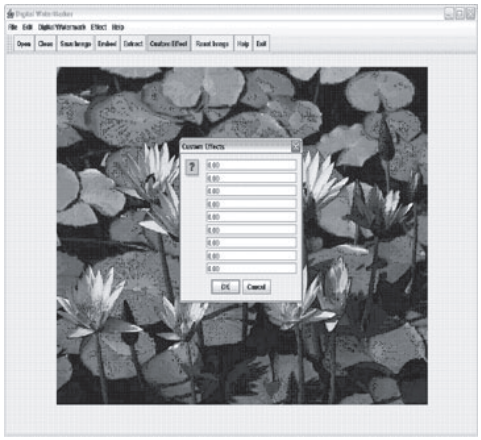


Figure 2: Provided the Custom Effects to the Image

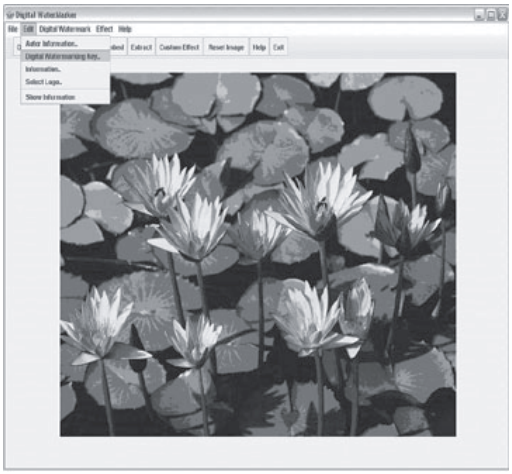


Figure 3: Edit Digital Watermarking Key for Key Watermarking

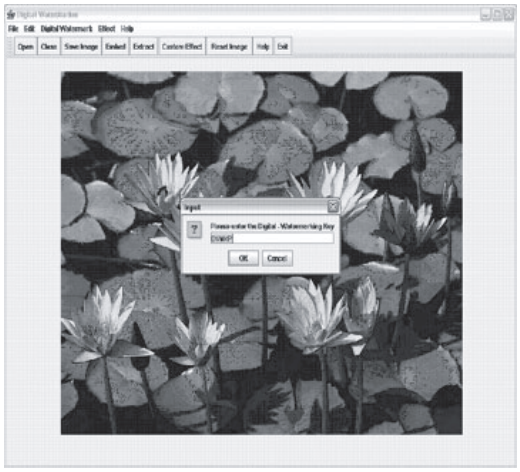


Figure 4: Enter the Five Character Digital Atermarking Key

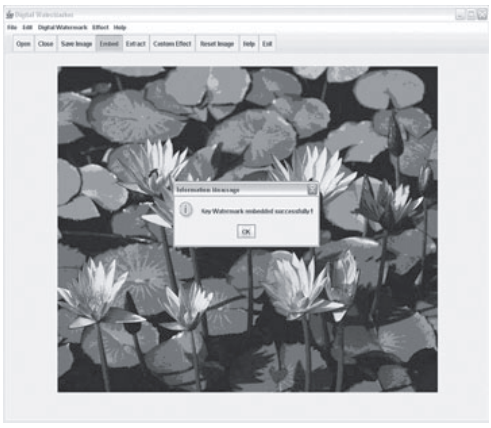


Figure 5: Embed Key Watermark into the Image

Figure 6: Output Dwi Image of Key Watermark

6. CONCLUSION AND FUTURE SCOPE

- **Copy Protection:** The information stored in a watermark can directly control digital recording devices for copy protection purposes. Example: DVD Recorders, Set-top video recorders
- **Broadcast Monitoring:**
  - Embedding watermarks in commercial advertisements.
  - A monitoring system can verify whether advertisements are broadcasted as contracted.

Example: If TV stations follow the contacts

- To apply digital watermarks to all file formats of images.
- To apply invisible digital watermark to audio and video files.
- To use concept of digital watermarking to control audio and video piracy.

REFERENCES

[1] Husrev T. Senscan & Mahalingam Ramkumar "Data Hiding Fundamental and Applications" ELSEVIER *Science & Technology* Books. ISBN-0-12-047144-2

[2] Ingemar Cox, Mathew millar, Jeffrey Bloom "Digital Watermarking", Morghon Kaufman Publisher, (2001), ISBN-55860-714-5.

[3] Mauro Barni & Feranco Bartolini, "Watermarking System Engineeering; Enabling Digital Asssets Security & Other Applications" Marcel Dekker Publication (Feb. 2004).

[4] Sergio D. Servetto, Chisten I. Podichuck & Kannan Ramchandran "Watermarking Digital Images for Copyright Protection".

[5] Nikolaidis, N. and Pitas, I. "Digital Image Watermarking: An Overview", *IEEE Int. Conf. on Multimedia Computing and Systems*, **1**, (June 1999), 1–6.

[6] Perez-Gonzalez, F. and Hernandez, J.R. "A Tutorial on Digital Watermarking", *Proc. IEEE 33rd Annual 1999 Int. Carnahan Conf. on Security Technology*, (Oct. 1999), 286–292.

Milind Kumar v. Sarode
Department of Computer Science and Engineering
Jawaharalal Darda Institute of Engineering & Technology
Yavatmal. MS.
India
E-mail: parthmilindsarode@rediffmail.com

S. A. Ladhake
Sipna Shikshan Prasarak Mandal's College of Engineering
Amravati (MS)
India

Prashant R. Deshmukh
Department of Computer Sci. & Engg. and Information Technology
Sipna Shikshan Prasarak Mandal's College of Engineering
Amravati (MS)
India
E-mail: prdeshmukh@ieee.org