UNIVERSITI PUTRA MALAYSIA

IMPROVED WATERMARKING ALGORITHM BASED ON DISCRETE WAVELET TRANFORM AND FIBONACCI PERMUTATION

SALEH HUSSIN SALEM HUSSIN.

IMPROVED WATERMARKING ALGORITHM BASED ON DISCRETE WAVELET TRANSFORM AND FIBONACCI PERMUTATION

By

SALEH HUSSIN SALEM HUSSIN

Thesis Submitted to the School of Graduate studies, Universiti Putra Malaysia, in Fulfillment of the Requirement for the Degree of Master of Science

October 2005

DEDICATION

TO

MY BELOVED FAMILY

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in Fulfillment of the requirements for the degree of Master of Science

IMPROVED WATERMARKING ALGORITHM BASED ON DISCRETE WAVELET TRANSFORM AND FIBONACCI PERMUTATION

By

SALEH HUSSIN SALEM HUSSIN

October 2005

Chairman : Elsadig Mohamed Ahmed Babiker, PhD

Faculty : Engineering

Digital image watermark is an imperceptible, robust, secure message embedded into the image, which identify one or more owner, distributor, or recipient of the image, origin or status of the data or transaction dates. Watermarking is also used for data hiding, content labeling, broadcast monitoring, and integrity control applications. Digital watermarking resembles communication systems. Watermark is the sent message. Image is the watermark channel or carrier. Image pixels and possible attacks on marked image constitute the noise. Only the authorized parties' extracts the watermark message from the marked image by using detector.

Digital watermarking has three major requirements. Watermark should be robust against noise and attacks, imperceptible and has the required capacity. These three requirements conflict with each other. To illustrate, increasing the watermark strength makes the system more robust but unfortunately decreases the perceptual

quality. As a second example, increasing the capacity of the watermark decreases the robustness.

In this thesis, the goal was to study digital image watermarking and develop watermarking algorithm that can achieve high imperceptibility, maximum capacity, and high robustness against image manipulation at the same time. This algorithm is based on the combination of Fibonacci permutation and discrete wavelet transforms (DWT). A binary image is used as the watermark and inserted into a mid-frequency wavelet subband of the permuted image. The watermarked image is reproduced by taking the inverse DWT and the inverse permutation. In extraction process the watermark is extracted from the watermarked image directly without using the original image.

The experimental results have shown that the proposed watermark is invisible to human eyes and very robust against image manipulation, such as JPEG compression, median filtering, wiener filtering, and noises.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

PEMBAIKAN ALGORITMA TERA AIR BERASASKAN KEPADA PENJELMAAN WAVELET DISKRET DAN PERTUKARAN FIBONACCI

Oleh

SALEH HUSSIN SALEM HUSSIN

October 2005

Pengerusi : Elsadig Mohamed Ahmed Babiker, PhD

Fakulti : Kejuruteraan

Imej digital tera air adalah mesej yang tidak dapat boleh ditanggap, selamat yang di tanam kedalam imej, yang mana boleh mengenali satu atau lebih pemilik, pengedar, atau penerima imej, punca atau status data atau transaksi tarikh. Tera air juga digunakan untuk menyembunyikan data, melabelkan isi kandungan mengawas penyiaran dan aplikasi kawalan integriti. Tera air digital menyerupai sistem komnikasi. Tera air adalah mesej yang dihantar. Imej adalah saluran atau pembawa tera air. Pixel imej dan kemungkinan serangan kepada imej bertanda adalah bisingan. Hanya pihak yang berkuasa dapat menguraikan imej tera air daripada imej bertanda menggunakan suatu pengesan.

Tera air digital mempunyai tiga keperluan utama. Tera air perlu tegap terhadap bisingan dan serangan, tidak dapat ditanggap dan mempunyai kapasiti yang diperlukan. Tiga keperluan ini adalah ber konflik antara satu sama lain. Untuk

mengilustrasi, peningkatan kekuatan tera air menyebabkan sistem lebih tegap tetapi malangnya ia mengurangkan kualiti penglihatan. Sebagai contoh kedua, peningkatan kapasiti tera air mengurangkan ketegapan.

Matlamat tesis ini adalah untuk mengkaji imej digital tera air dan membeutuk algoritma tera air yang boleh mencapai ketidakboleh tegapan yang tinggi, kapasiti maksimum dan ketegapan yang tinggi terbadap manipulasi imej pada masa yang sama. Algoritma ini berasaskan kepada kombinasi Pertukaran Fibonacci dan penjelmaan wavelet diskret. Imej binari digunakan sebagi tera air dan dimasukkan kedalam frekuensi tengah wavelet subjalur imej yang dipertukaran. Imej tera air dihasilkan dengan mengambil diskret penjelmaan gelombang kecil songsang dan Pertukaran songsang. Dalam proses cabutan, tera air dikeluarkan daripada imej tera air secara terus tanpa menggunakan imej asal.

Hasil eksperimen menunjukkan cadangan tera air ini adalah halimunan pada pandangan mata manusia dan mata tegap terhadap manipulasi imej, seperti pemampatan JPEG, penurasan median, penurasan wiener, dan bisingan.

ACKNOWLEGEMENTS

First and foremost, I owe my gratefulness to ALAAH for giving me the strength and willpower to complete this research.

I would like to profusely thank my supervisor Dr. Elsadig Mohamed Ahmed Babakr for his timely advices and encouragement throughout my project work. I would like to acknowledge Assoc. Prof. Dr. Abd Rahman Ramli for reviewing my work from time to time. I am no less grateful to my committee member Tuan Sayed Abd. Rahman Al-Hadad.

Thanks also to Eng. Mohamed Almashrgi for his encouragement and support. He was always available for providing useful direction and advice when I needed. I fell happy to have friend like him.

I would also like to thank all who helped me during my project work.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

2D	2 Dimensional
3D	3 Dimensional
AD	Average Absolute Difference
ASCII	American Standard Code for Information Interchange
AVI	Audio Video Interleaved
BCR	Bit Correct Ratio
dB	Decibel
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DVD	Digital Versatile Disk
DWT	Discrete Wavelet Transform
HS	Histogram Similarity
HVS	Human Visual System
IDWT	Inverse Discrete Wavelet Transform
IEEE	Institute of Electrical & Electronic Engineers
JPEG	Joint Photographic Experts Group
LSB	Least Significant Bit
LZW	Lempel-Ziv-Welch
MPEG	Moving Pictures Experts Group
MSB	Most Significant Byte
MSE	Mean Square Error

PSNR	Peak Signal-to-Noise Ratio
RGB	Red, Green, and Blue
ROI	Region-Of-Interest
SNR	Signal-to-Noise Ratio
SSKF	Symmetric Short Kernel Filters
TV	Television
WWW	World Wide Web

CHAPTER 1

INTRODUCTION

1.1 Digital Media and Copyright Protection Problem

Digital storage and transmission is the major trend of handling information. The image, audio and video industries are distributing their products in digital form. Broadcast television, big corporations and photo archives are converting their content from analog formats to digital. With the increasing availability of a lot of advanced multimedia broadcasting services such as pay-per-view, video-on-demand, tele-marketing, tele-teaching, electronic newspapers, tele-gaming, electronic commerce, advertising, interactive TV, digital libraries, and web magazines, this trend will further increases (Cox *et al* 2002).

Digital technology has many superior as compared to the analog technology. First of all, the quality of digital image, audio and video is superior to that of analog form due to noise free transmission. Secondly, it is easier to process and distribute digital media. Therefore, most of the multimedia applications exploit digital technology. On the other hand, digital media has the disadvantages of lack good copyright protection mechanism. Since the unauthorized reproduction, distribution and manipulation of digital media is very easy, the authorized service providers are reluctant to offer commercial services in digital form (Piva *et al* 1998).

1.2 Digital Watermarking as a solution for Copyright Protection

In order to provide copyright protection for digital media, two complementary techniques are used: encryption and watermarking.

Encryption is applied as a security measure. In this technique, the data is scrambled at the transmitter using a secrete key. The authorized receiver is only the other party, which is intended to know this secret key in order to descramble the received data. Since, on the average it takes years for a hacker to fined out the key, encryption looks like a safe technique. However, since computers are getting more and more speedy and it is possible to use multi-processor, multi-computers, and multi-human systems, it is getting easier to break the encryption protection and do illegal reproduction and distribution of valuable media. Moreover, once the receiver has received and decrypts the data, it is no longer protected. For these reasons, encryption is not a perfect solution for copyright protection. In fact, it is mainly concerned with secure communications but not copyright protection.

Watermarking cannot by itself prevent copying, modification and redistribution of digital media, but if encryption fails to do so during transmission, watermarking allows document to be traced back to its rightful owner and to the point of unauthorized user after the delivery of the data (Janathan *et al* 2000).

Digital watermarking starts by embedding a signature, or watermark (often imperceptible, robust, secure) into the digital content before its release. Upon receiving the watermarked asset, the embedded watermark is then extracted for comparison against the original watermark. The embedded watermark, once extracted and successfully verified, can provide information such as the source of distribution, identification of owner and recipients, time and date of creation, and so on.

Watermarks can be placed within content having a wide variety of digital representation. Within the realm of digital watermarking, the definition of content can generally include text, audio (music and speech), images (graphics and high-quality photographs), video (movies or digital TV), 3-D graphics models, and even computer software codes (Ohbuchi 1998).

1.3 Watermarking applications

Watermarking is not limited to copyright protection. It is also used in the following fields (Cox *et al* 2002):

1.3.1 Authentication

In some applications such as news pictures, it is important to be sure that the content of the media has not changed since its distribution. As a verification mechanism, the detector compares the extracted watermark with the embedded one. If they do not match, it means that the content has been modified. In this application the watermarking system should be non-robust. Such a watermark is called fragile watermark and it should disappear if the media experience any intentional attack.

1.3.2 Secret and invisible communication

Watermarks can be also used to hide secret and private messages. In this type of application, robustness is not of much concern. Because, the assumption is, third parties are not aware of existence of the watermark in the media. Therefore capacity of this application can be up to the limit of creating awareness of its existence.

1.3.3 Content labeling and hidden annotation

Watermarking can be used in content labeling, multimedia indexing and transaction tracking, usage control, access level control and medical applications. For example, a digital camera can hide the date and place of the taken photo which is in the category of content labeling. As another example, in medical applications, the watermarking system can embed patient record directly into radiography images in such away to

speed up the access to records and to prevent errors of mismatching between patient records and images.

1.4 Watermarking requirements

Each watermarking application has its own special requirements with regard to robustness, security, imperceptibility, and the amount of data that needs to be embedded. For example, when digital watermarks are used for copyright protection, the need for robustness and imperceptibility is obvious, while the amount of data to be embedded is of only marginal interest. The technical requirements vectors for the other applications are all different as shown in Figure 1.1 (Zhao *et al* 1998).

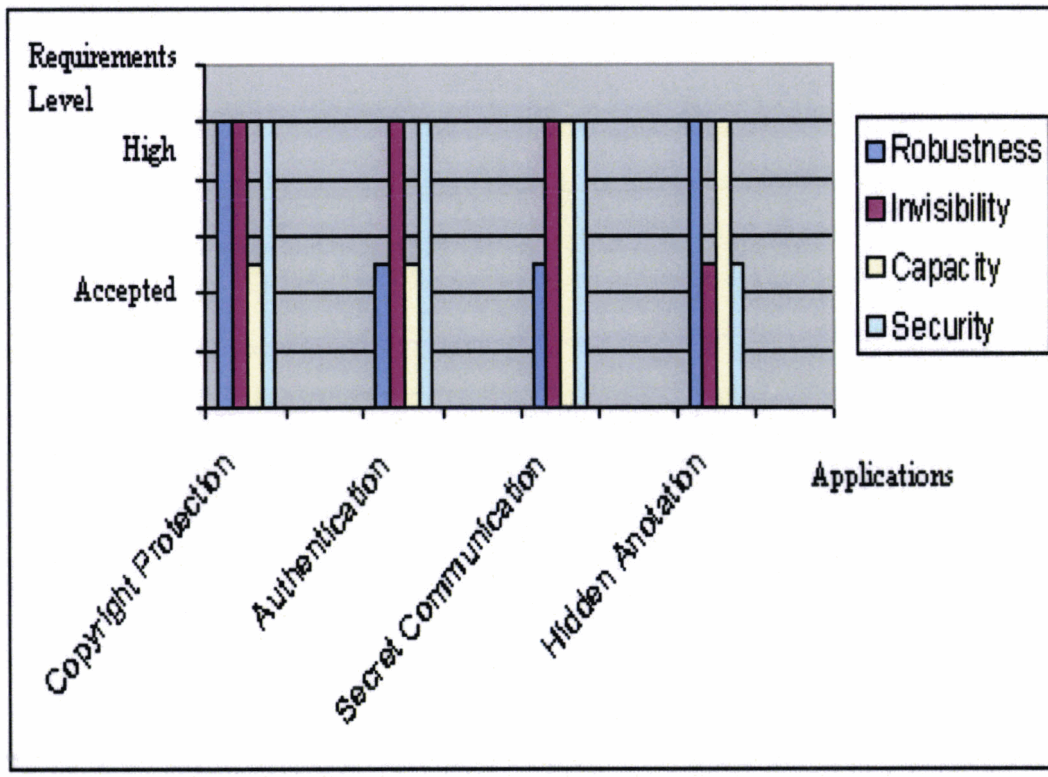

Figure 1.1: Applications and technical requirements.

The specific requirements for each watermarking technique vary with the application. There is no universal watermarking technique that satisfies all requirements of all applications! Consequently, each watermarking technique has to be designed within the context of the entire system in which it is to be used (Craver *et al* 1998).

1.5 Watermarking requirements for copyright protection

As mentioned in the previous section, digital watermarking has many applications. Different applications refer to different requirements. There are no general requirements for all watermarking problems. In this work, the concern is about copyright protection application of image data, where as the concept discussed here can be applied to other media such as video as well. The requirements of copyright protection watermark include (Swanson's 1998):

1. Public watermark: The watermark extraction process should be public, in which no original image is needed, to reduce the transmission number and improve the security. On the other hand, the private scheme needs the original image in the watermark extraction process.
2. Imperceptibility: The watermark should be imperceptible to avoid interrupting the viewing experience.