HYBRID WATERMARK TECHNIQUES FOR SKIN CANCER IMAGES

OMAR ADIL DHEYAB

05-4506832 pustaka.upsi.edu.my Perpustakaan Tuanku Bainun Kampus Sultan Abdul Jalil Shah PustakaTBainun ptbupsi

THESIS SUBMITTED IN FULFILLMENT OF THE REQUIREMENT FOR DOCTOR OF PHILOSOPHY (ARTIFICIAL INTELLIGENCE)

FACULTY OF ART, COMPUTING & CREATIVE INDUSTRY
SULTAN IDRIS EDUCATION UNIVERSITY

2019

05-4506832 pustaka.upsi.edu.my Perpustakaan Tuanku Bainun Kampus Sultan Abdul Jalil Shah PustakaTBainun ptbupsi

ABSTRACT

The aims of this study are to reveal the potentials of digital watermarking in medical data management issues, and proposes a hybrid watermark technique for skin cancer to enforce integrity, authenticity and confidentiality of the medical information. Dermoscopic image dataset (PH2) was used for testing purpose, which includes 200 different images. The hybrid watermark is proposed based on chaotic embedding. The hybrid watermarking includes robust and fragile watermarks embedded in the region of non interest of the image. The robust watermark utilizes the discrete wavelet transform to hide the patient information in the frequency domain. The fragile watermark utilizes the least significant bit to hide the authentication data in the spatial domain. The findings of this study shows high watermarked image quality and promising robustness under different attacks, and when compared with other techniques including discrete cosine transform and 2LSB. The Peak Signal–to-Noise Ratio (PSNR) of the watermarked image is 37.64 dB and the Mean Square Error (MSE) is 36.7507 dB, which indicate good image equality. In general, the hybrid watermark did not degrade the image quality and enhanced medical data security and authentication. The proposed hybrid watermarking can help health organizations to deal with medical information effectively, especially during storage and transmission.

05-4506832 pustaka.upsi.edu.my Perpustakaan Tuanku Bainun Kampus Sultan Abdul Jalil Shah PustakaTBainun ptbupsi

TEKNIK *WATERMARK* HIBRID BAGI IMEJ KANSER KULIT

ABSTRAK

Kajian ini bertujuan untuk mendedahkan potensi *watermark* digital dalam isu pengurusan data perubatan dan mencadangkan satu teknik *watermarking* hibrid untuk mengukuhkan integriti, ketulenan dan kerahsiaan maklumat perubatan. Set data imej dermoskopik (PH2) digunakan untuk tujuan pengujian yang merangkumi 200 imej yang berbeza. *Watermarking* hibrid dicadangkan berdasarkan pembenaman huru-hara. *Watermarking* hibrid ini merangkumi *robust watermark* dan *fragile watermark* yang dibenam di rantau tanpa kepentingan imej tersebut. *Robust watermarking* menggunakan transformasi wavelet diskrit untuk menyembunyikan maklumat pesakit dalam domain frekuensi. *Fragile watermarking* menggunakan bit yang kurang signifikan untuk menyembunyikan data pengesahan dalam domain spatial. Penemuan kajian ini menunjukkan kualiti imej *watermark* yang tinggi dan menjanjikan kekukuhan di bawah pelbagai serangan, dan apabila dibandingkan dengan teknik lain termasuk transformasi kosinus diskrit dan 2LSB. Nisbah Isyarat Puncak kepada Hingar (PSNR) untuk imej *watermark* adalah 37.64 dB dan Min Kesilapan Persegi (MSE) adalah 36.7507 dB, yang menunjukkan kualiti imej yang baik. Secara umum, *watermark* hibrid tidak merendahkan kualiti imej dan meningkatkan keselamatan dan pengesahan data perubatan. *Watermarking hibrid* yang dicadangkan boleh membantu organisasi kesihatan untuk menangani maklumat perubatan dengan berkesan, terutamanya semasa penyimpanan dan penghantaran.

TABLE OF CONTENTS

CHAPTER 5 RESULTS AND DISCUSSION

CHAPTER 6 CONCLUSIONS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

AES	Advanced Encryption Standard
AI	Artificial Intelligent
ANN	Artificial Neural Network
BCR	Bit Correction Rate
CT	Computed Tomography
DCT	Discrete Cosine Transform
DES	Data Encryption Standard
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
IDEA	International Data Encryption Algorithm
KNN	K-Nearest Neighbors
LSB	Least Significant Bit
MRI	Magnetic Resonance Imaging
MSE	Mean Square Error
NC	Normalized Cross Correlation
PCA	Principal Component Analysis
PSNR	Peak Signal –to-Noise Ratio
SVM	Support Vector Machine
MI	Medical Image
ROI	Region of Interest
RONI	Region of Non-Interest

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Internet facilitates the communication of huge numbers of people and the transmission of enormous data, which poses a challenge to information security, resources and to ensure the network authenticity against various attacks. The security is essential and compulsory due to the digital technologies rapid development including Internet technologies and image processing tools. These developments facilitate easy access to

huge digital data via various transmission channels, and facilitate digital media transmission such as images, audio, video and text more adequately. On the other hand, the powerful image processing tools and advanced software make it easy to manipulate, alter and distribute data (Moniruzzaman et al., 2014; Ghebleh & Kanso, 2014). Therefore, it becomes mandatory to enhance content security during data use and transmission. Cryptography and steganography are significant methods to ensure security. The cryptography scrambles data in a random manner based on encryption key. However, the encrypted text is known, and therefore raises the suspicion of the attackers to exist secret information. Cryptography provides confidentiality, authenticity, non-repudiation, and integrity of data. Steganography is an embedding technique of sensitive information into a cover media in such a way that it cannot be seen. Steganography techniques are combined with encryption to achieve more active security.

The extensive researches on authenticity and integrity of images have led to develop two approaches namely digital signature, and digital watermark. The basic idea of digital signature is to use a hash function that generates the digital signature, which is embedded in the image as redundant data, invisible to the eye. In case of a malicious attack, the digital signature can be identified and the image authenticity cannot be confirmed. A main drawback of such scheme is the inability to localize the tampered area on the image, and the damaged data cannot be recovered (Rawat & Raman, 2011). To overcome this problem, watermarking based scheme has been proposed as an alternative approach, which embeds data called a watermark into a multimedia object (Zhang et al., 2013).

1.1.1 Watermarking

Watermarking is the art of hiding formation (text, images, audios or videos) into cover mediums so that the presence of the secret information cannot be detected (Xu et al., 2010). Watermarking emerged as an effective mean to protect data and prevent unauthorized manipulation of information against illegal use during their transmission and store particularly medical image databases, military image databases, online private images album, etc. The digital watermarking concept emanated while attempting to find solutions to problems related to intellectual property of digital products management. Digital watermarks are widely and successfully used in most media objects across various applications such as copyright protection, data hiding and authentication, fingerprinting, and more (Zhu & Zhao, 2010; Hamouda et al., 2014).

The watermark should be robust against a diversity of potential attacks including compression, scaling, rotation, cropping, altering, cryptographic and statistical attacks, (Pereira et al., 1999). Various watermarking techniques exist, which can be classified into various categories as shown in Figure 1.1.

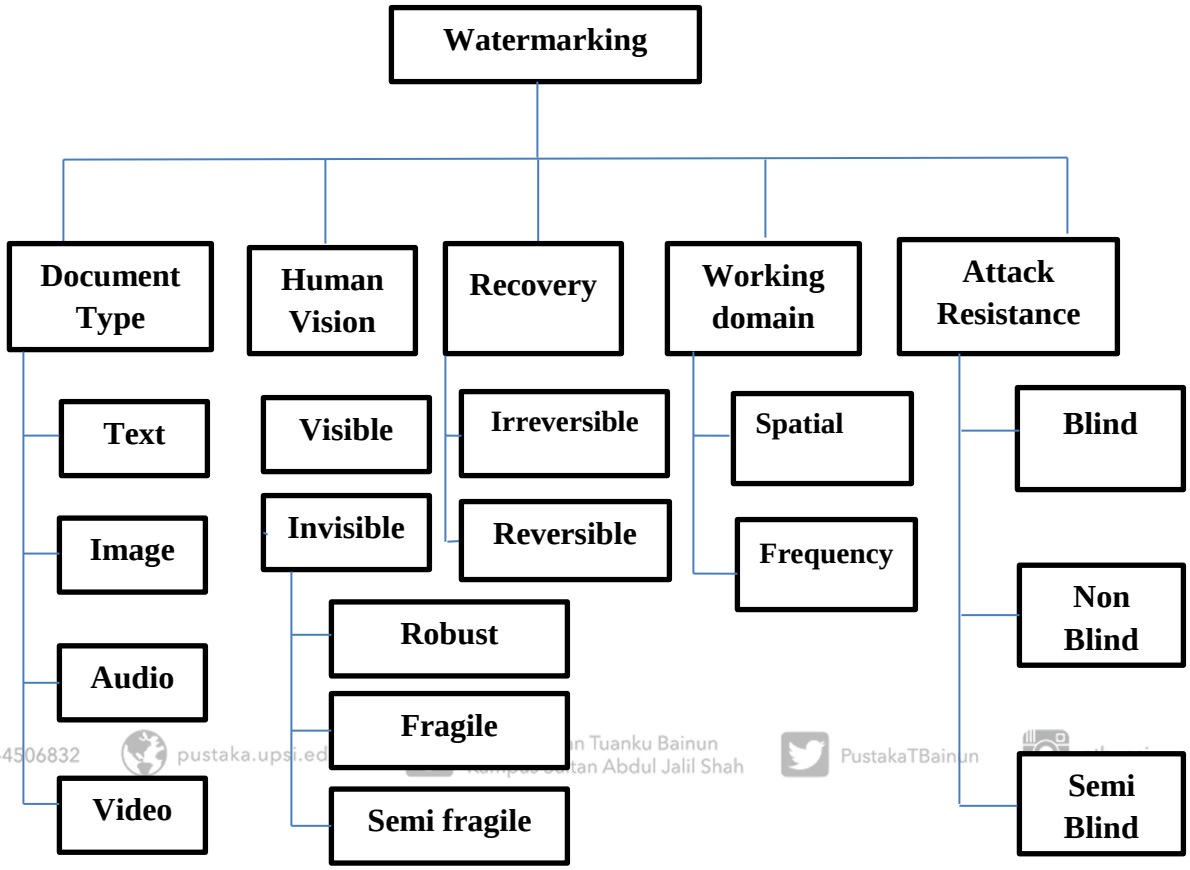

Figure1.1. Watermarking Taxonomy

1.1.2 Medical Images

The health care system exploits the Internet to simplify the digital medical images and information exchange between health institutions to provide e-health services to patients. Complicated data set such as medical notes, clinical examinations, diagnosis

and receipt, scanned images of patient's clinical examinations, etc are the significant information of any medical information system (Chitla & Chandra Mohan, 2014). Digital medical images such as Ultrasound scan (US), Computed Tomography (CT), Electrocardiography (ECG), Magnetic Resonance Imaging (MRI) and X-ray images are essential to diagnosis and treatment of several diseases, and thus, it is quite important to ensure secure storage, transmission, processing and analysis of medical images without breaching the ethics code for health information (Das & Kundu, 2013). To attain these objectives, health authorities and interested entities in information security pay more attention to digital watermarking application in medical images to meet the authentication and security requirement. Embedding watermarking in medical imaging aims to embed large data in images to include more useful information of the patient, and to protect images (Chitla & Chandra Mohan, 2014).

1.2 Problem Background

Digital images usually have very large-sized. Encrypting such huge data with conventional ciphers such as data encryption standard (DES), advanced encryption standard (AES), and international data encryption algorithm (IDEA) needs significant overhead, and is too costly for real-time applications (Tabash et al., 2013). To facilitate digital images sharing and remote handling in a secure manner, watermarking ensures attractive properties. Several watermark-based image authentication schemes have been proposed to check the digital images integrity and authenticity (Xiao & Jin 2012).

Among these medical images are dermoscopy images. The dermoscopy images are taken by an optical system called dermatoscope. The dermatoscope is an optical device coupled with a robust lighting system used to magnify the skin lesions during the examination process (Mendonca et al., 2013; chakravorty et al., 2016).

Medical image watermarking needs more attention than other watermarking types. In natural image watermarking, deformation can be accepted unlike medical images, because even a change in single bit may misguide the diagnosis decision. In other words, embedding additional information into the medical images, should not affect the quality of image. Recently, the medical images amount that transmitted through the internet has increased speedily, thus needs more bandwidth and more memory, as well as speedy and safe transmission medium. Medical images security is a major issue which should be considered remarkably during store or transfer the image for diagnosis purposes (Naseem et al., 2013). Cryptographic methods are not suitable for medical image security due to fundamental issues such as needing more computational resources and depleting more time to recover the original image (Koppu & Viswanatham, 2017).

Protecting medical information risks are augmented, particularly over the Internet. This obliges three compulsory characteristics: confidentiality, integrity, and authenticity. Another main requirement is that any degradation that affects the diagnosis from the medical images is not acceptable. In general, medical images should remain intact with no visible change to their original form. There are many techniques for

medical image watermarking; however, they have many disadvantages: some are task and modality specific, while others suffer from low security, imperceptibility, payload capacity problems and without capability to locate tamper (Das & Kundu, 2013).

Medical image watermarking imperceptibility, robustness and capacity must be attained. However, these issues might contradict with each other. In all previous works, either the watermarking algorithm works for a specific medical image, or there is no good balancing between imperceptibility and embedding capacity, moreover, the watermarking are less secure (Al-Qershi & Khoo, 2011).

1.3 Problem Statement

Medical image watermarking is a proper method to enhance medical data security and authentication, which is crucial and used for further diagnosis and treatment. Most watermarking techniques alter, and may distort the host image in order to insert authentication information (Rawat & Raman, 2011; Xiao & Jin, 2012). In several applications, image fidelity loss is not forbidden as long as original and modified images are perceptually equivalent except in medical, military, and legal applications, where the need for authentication is often essential (Das & Kundu, 2013, Bilal et al., 2014). Many techniques and approaches have been developed for watermarking. Least significant bit (LSB) and spread spectrum are some of the spatial domain techniques. LSB substitution is the most popular one that embeds secret data by replacing some LSBs of a cover image pixel with secret data bits directly. The LSB substitution method is simple and