SECURE IMAGE WATERMARKING SCHEMES BASED ON DIGITAL HOLOGRAPHIC INTERFEROMETRY TECHNIQUE

By

TAN HAO QIANG

A dissertation submitted to the Department of Electrical and Electronic Engineering,
Lee Kong Chian Faculty of Engineering and Science,
Universiti Tunku Abdul Rahman,
in partial fulfillment of the requirements for the degree of
Master of Engineering Science (A).
July 2017

ABSTRACT

SECURE IMAGE WATERMARKING SCHEMES BASED ON DIGITAL HOLOGRAPHIC INTERFEROMETRY TECHNIQUE

TAN HAO QIANG

As demand for digital work copyright protection and security keep increasing, researchers have been intergrading optical system especially digital holography into digital watermarking. Digital holography watermarking embeds hologram as watermark into digital work to improve its performances and security. However, present digital holographic watermarking scheme are mainly focused on improving the watermarking embedding algorithmic to improve the watermarking scheme overall performances. On the other hand, secure digital holographic watermarking usually employed large amount of key to encrypt the watermark information. Therefore, it is inconvenient to send these large amounts of keys to the authorized user through the Internet.

In this project, a digital watermarking scheme based on digital holographic interferometry is presented to address the large key file sizes. The main contributions of this project can be separated into two chapter, where firstly, is to reduce the hologram information by using a portion of the total hologram size as watermark. The unique properties of the hologram allow the object information to be reconstructed by using a portion (60% to 100%) of the total hologram size. Experiment results showed that this method able to improve the watermarking perceptual quality by +0.64% when using 60% of the hologram size. The second contribution is to develop a secure watermarking scheme based on Digital Holographic Interferometry (DHI), where two holograms have been used, one as the watermark and the other as the key. The proposed scheme offers an additional layer of security, as the recovery of watermark information requires the knowledge of key. Experimental results demonstrated that the perceptually quality of watermarked image of the proposed scheme based on DHI increased by 27.6% and 19.7% when compared with the Double Random Phase Encoding (DRPE) and Double Random Phase Encoding-Fractional Fourier Transform (DRPE-FRT). Besides

that, the proposed watermarking scheme is able to withstand against most image processing attacks especially against Gaussian noise, Gaussian filter, JPEG compression and Image cropping.

ACKNOWLEDGEMENTS

First and foremost, I would like to express my outmost gratitude to my project supervisors, Dr. Yong Thian Khok and Prof. Ir. Dr. Goi Bok Min, for their valuable advices and guidance throughout my research project. Their patience, encouragement and assistance have been the keys for me to complete this project. I would like to convey my thanks to my beloved parents and my family for their encouragement and full support during my studies. They have given me the strength and determination in completing this work. Last but not least, I would also like to express my greatest appreciation to all my friends who have been helping me to overcome various obstacles and problems.

APPROVAL SHEET

This dissertation entitled “**SECURE IMAGE WATERMARKING SCHEMES BASED ON DIGITAL HOLOGRAPHIC INTERFEROMETRY TECHNIQUE”** was prepared by TAN HAO QIANG and submitted as partial fulfillment of the requirements for the degree of Master of Engineering Science at Universiti Tunku Abdul Rahman.

Approved by:

____
(Dr. YONG THIAN KHOK)
Date:…………………..
Supervisor
Department of Electrical and Electronic Engineering
Lee Kong Chian Faculty of Engineering and Science
Universiti Tunku Abdul Rahman

____
(Prof. Ir. Dr. GOI BOK MIN)
Date:…………………..
Co-supervisor
Department of Mechatronics and BioMedical Engineering
Lee Kong Chian Faculty of Engineering and Science
Universiti Tunku Abdul Rahman

LEE KONG CHIAN FACULTY OF ENGINEERING AND SCIENCE

UNIVERSITI TUNKU ABDUL RAHMAN

Date: ___31 DEC 2015_______

SUBMISSION OF FINAL YEAR PROJECT /DISSERTATION/THESIS

It is hereby certified that ***TAN HAO QIANG*** (ID No: ***11UEM06714***) has completed this ~~final year project~~/ dissertation/ ~~thesis~~* entitled "**SECURE IMAGE WATERMARKING SCHEMES BASED ON DIGITAL HOLOGRAPHIC INTERFEROMETRY TECHNIQUE**" under the supervision of Dr Yong Thian Khok (Supervisor) from the Department of Electrical and Electronic Engineering, Lee Kong Chian Faculty of Engineering and Science, and Prof. Ir. Dr. Goi Bok Min (Co-Supervisor) from the Department of Mechatronics and BioMedical Engineering, Lee Kong Chian Faculty of Engineering and Science.

I understand that University will upload softcopy of my ~~final year project~~ / dissertation/ ~~thesis~~* in pdf format into UTAR Institutional Repository, which may be made accessible to UTAR community and public.

Yours truly,

____

(*TAN HAO QIANG*)

*Delete whichever not applicable

DECLARATION

I hereby declare that the dissertation is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UTAR or other institutions.

Name: TAN HAO QIANG

Date: 31 DEC 2015

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

A watermark is a recognizable pattern that appears in different shades of darkness/lightness when observed under transmitted light. According to Shih (2008), for nearly a thousand years, watermarking has been used on paper and currency to discourage counterfeiting. Nowadays, most data and information are stored in digital format and transmit through the Internet. Digital watermarking techniques embed a digital message as watermark into digital work (e.g. image, music and video).

On the contrary, another technology known as encryption made the information of the content unreadable to observer without knowledge or specific keys. Hence improves its overall security. Chang and Hang (2004) works have shown that digital watermarking when combine with encryption can serve a vast application including copyright protection, broadcast monitoring and data authentication.

Imperceptibility, robustness, capacity and security are some of the aspects of watermark design. An ideal watermarking system should embed large amount of hidden information securely with no visible degradation to the host image.

On the other hand, holography is an optical method to record and reconstruct optical wavefield. The term holography comes from Greek meaning whole writing. Holography is a two-step process: firstly a coherent light illuminated an object of interest to produce interference fringes in a photosensitive medium. Secondly, the developed interference pattern is re-illuminated by the same coherent light to produces a three-dimensional image of the object.

The past twenty years have seen a rise in demand for better digital work copyright protection and security. The emerging of computer technology of the last decade- increasing processing speed and memory capacity, as well as the CCD or CMOS cameras having more and smaller pixels allowed researcher like Takai and Mifune (2002) to proposed the first Digital Holographic Watermarking. In this method a digital-watermark image is first converted to Computer Generated Hologram (CGH) using Fourier transform. The digital hologram – unlike the traditional digital message – contains the amplitude and the phase of an object. The unique properties of the hologram made it resilient to cropping effect and its information can be reconstructed using only partial of its data. Research on digital holographic watermarking can be divided into two groups: one is based on improving the holographic watermarking performances in terms of perceptual quality and robustness, while the other is based on improving the security of holographic watermarking by image and optical encryption (Kishk and Javidi (2003)).

1.2 Problem Statement

In holographic watermarking, many researchers have been focusing either on the watermark embedding algorithmic or the security part but very few on both to improve the holographic watermarking performances (Li, 2014). Undeniably, one would expect the embedded watermark to be robust and imperceptible. However the existing holographic watermarking is less secure as experimental parameters (for example: wavelength of the laser & recoding distance) can be easily deducted.

The watermark information is encrypted with large amount of keys data before embed into the host image to improve the holographic watermarking security (Kishk and Javidi (2003)). However, it is inconvenient to send these large amounts of keys data across the limited bandwidth over to the authorized user. Robustness is another concern by secure holographic watermarking as the encrypted watermark information must survive against possible attacks. In an event, if the watermark information is destroyed by a possible attack, then the security has lost its purpose in watermarking.

1.3 Aims and Objectives of Project

This project work is an attempt to reduce the key data needed for secure holographic watermarking by using the holographic interferometry. The project aim and objective project can be divided into three tasks:

1. To investigate the digital watermark embedding algorithmic that offers best perceptual quality for the project
2. To show that the hologram key data can be reduce by using a portion of the total hologram file sizes.
3. Developing a digital watermarking scheme based on digital holographic interferometry. One criterion for secure watermarking schemes is robustness. Thus the experiments are mainly focused on the robustness of the proposed schemes. The proposed watermarking scheme~~s~~ performance is compared with existing secure holographic watermarking schemes such as Double Random Phase Encoding (DRPE) and Double Random Phase Encoding-Fractional Fourier Transform (DRPE-FRT).

1.4 Dissertation Outline

The dissertation is divided into six chapters. Chapter 1 introduces the watermarking and holographic watermarking followed by objectives and aims of project. Chapter 2 summarizes the watermark history followed by explaining the basic principle of watermarking and the basic formulation of holography and wavefront reconstruction. The final chapter summarized the development of holographic watermarking technologies

In Chapter 3, the unique properties of the holograms are investigated. The detailed discussion includes digital holography and digital holographic interferometry in term of recording and numerical reconstruction is presented.

The watermark scheme performance using different hologram file sizes are tested against some image processing attacks is presented in Chapter 4

The application of digital holographic interferometry into digital watermarking is presented in Chapter 5. The robustness of the proposed watermarking scheme is tested and the results are compared to the existing method.

Chapter 6 concludes the work done within this project. It also addresses future improvement in the proposed watermarking system.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction to Information Hiding

Information hiding, Steganography and Watermarking are three fields that share many technical approaches. Yet there are fundamental differences between them that effect the requirements and design of the technical solution.

Information hiding is a method of making the existence of the information secret or invisible (as in Steganography and Watermarking). The information hiding techniques can be divided into two categories: Cryptography and Steganography. Cryptography is an art of protecting the information during the transmission. The message is encrypted prior to transmission. A key is send to the user to decrypt the encrypted message. However, the message after the decryption is no longer protected. Steganography is the art of hiding or conceal a hidden message into another message. In other word, steganography conceal a message to hide its existence to avoid drawing suspicion. As opposed to steganography, watermarking has the additional robustness against intended attacks to destroy and remove the watermark.

2.2 Historical Development of Watermark

Hunter (1967) reported the first known watermarks appeared in 1282, Italy. The watermark is made by adding thin wire patterns to the paper molds. At that time, the watermark purpose is used as an indicator for paper quality. In Eighteen century, the watermark is generally used as an anti-counterfeiting measure in paper money. However counterfeiters managed to duplicate the watermark forging technique that protects the paper money. An Englishman, William Congreve invented the world first colored watermark method by adding dyed solution into papermaking process. However the Bank of England declined his method as the resulting marks are extremely difficult to forge. A more practical approach was created by William Henry Smith. This method is done by pressing shallow relief sculpture into the paper mold. The resulting mold surface consists of beautiful watermarks with varying shades of gray.

Szepanski, (1979) proposed a machine detectable pattern that placed watermark on the documents for anti-counterfeiting. Nine years later, Holt, et al. (1988) proposed a watermarking technique for adding an identification code into an audio signal. However, digital watermarking did not receive substantial interest as a research topic until the 90's. Advances in computer and network technology allow most work to be stored digitally and communicated through Internet. There is a significant demand to protect published copyright as well as information security. Digital watermarking techniques embed a digital message as watermark into the digital work, i.e. Images. Music and Movies, in such a way it appeared imperceptible and should be robust against intentional (e.g., Noise) and unintentional (e.g., cropping, resizing, or compression).

2.3 Classification of Digital Watermarking

As digital work is widely accessible on the Internet, there is an increase in demand to protect its copyright. Digital watermarking is one of the technologies used to identifying the authorized user. Since there are great numbers of watermarking scheme, it is important to classify them in order to understand how different watermarking schemes are applied. In this chapter the digital watermarking technologies is categorized into four groups.

1. Perceptible versus Imperceptible
2. Robust versus Fragile
3. Blind versus Non-Blind
4. Private versus Public

2.3.1 Perceptible versus Imperceptible

A watermark is known as perceptible watermark (visible watermark) if the embedded watermark information is visible to naked eyes. Logos are commonly used as a visible watermark to indicate the ownership of the content. These visible watermarks can be normally found on the television channel such as CNN, where the logo is visible at the corner of the picture. The disadvantage of visible watermark is that they can be removed easily by cropping off the logo. In contrast, an imperceptible watermark (invisible watermark) is embedded into the host image in such a way that they are imperceptible to human eyes. It could however be detected by a decoder.

Watermark information which embedded into the host image may distort the perceptual quality of the watermarked data. This will reduce the commercial value of the watermarked data. Therefore it is important the watermarking scheme design does not exceed the perceptible threshold. The most common way to measure the watermarked image imperceptible is by comparing the unmarked image and the watermarked image perceptual quality using the peak signal to noise ratio:

$$\mathrm{PSNR(dB)} = 20\log\left(\frac{255MN}{\sum_{i=1}^{M}\sum_{j=1}^{N}\left[x(i,j) - x^{1}(i,j)\right]}\right) \qquad (2.1)$$

where $x(i, j)$ and $x^1(i ,j)$ are the original and watermarked image, respectively The higher the PSNR values the better the watermarked image perceptual quality. In general, a watermarked image PSNR greater than 30 dB, it is acceptable to human perception.

2.3.2 Robustness versus Fragile

Watermark Robustness is another important requirement for the watermarking scheme. It refers to ability to detect the watermark after image processing attack, such as intentional or unintentional attack. The watermarking robustness can be categorized into three types: robust, semi fragile and fragile. Robust watermarks are made to survive against image processing attacks. However the watermarking scheme is not required to be robust against all kind of signal processing operation. Depending on its application, there is always a tradeoff between the watermark properties. For instance, the watermark image quality is reduced to improve its robustness. The design of an optimal watermarking scheme always involves a tradeoff between these requirements. Robust watermark are usually used for copyright protection.

Semi-fragile watermarks are made to detect unauthorized modification, at the same time offer some resistance to image processing attacks. In other words, the semi-fragile watermark able to survive attacks up to a certain threshold before the message is destroyed.

A fragile watermark is designed to be destroyed whenever a slight modification is applied onto the watermarked image. To evaluate the different between the recovered watermarks with the original watermark, a 2-D correlation coefficient is used:

$$cc = \frac{\sum_{m}\sum_{n}\left(A_{m,n} - \bar{A}\right)\left(B_{m,n} - \bar{B}\right)}{\sqrt{\left(\sum_{m}\sum_{n}(A_{m,n} - \bar{A})^2\right)\left(\sum_{m}\sum_{n}(B_{m,n} - \bar{B})^2\right)}} \tag{2.2}$$

where $\bar{A}$ and $\bar{B}$ are the mean values of A and B images. The 2-D correlation has a range values between 0 and 1. If cc = 1 then the recovered watermark and original watermark are same. The acceptable value of correlation may different from person to person. Hammed, et al. (2006), Okman, et al. (2007) and Mahasweta, et al. (2011) have fixed 0.75 as acceptable quality. Therefore, in this project, the acceptable value will fixed from 0.75 to 1.

2.3.3 Blind versus Non-Blind

A watermarking scheme is blind if it able to extract the watermark without access to the original host image. A watermarking scheme is known as Non-blind if the original host image is needed. For instance, the algorithms of Barni, et al. (1998) and Nikolaidis, et al. (1998) belong to the blind category. While those of Cox (1997) and Swanson, et al. (1996) belong to Non-blind. In general, non-blind scheme is more robust than the blind one because the watermark can be recovered easily using the unmarked host. However, in most applications the unmarked host is not available for detection. Therefore the blind watermarking is much more useful as it does not need the original data.

2.3.4 Private versus Public

A watermark is known as private watermarking if only authorized owner can extract and read the watermark. Private watermarking put in efforts to made sure it is impossible for the unauthorized user to read its watermark information, for instance, using a private pseudo random key. This watermarking scheme often combined with encryption techniques to make its watermark unreadable. Encryption is a process of obscuring information to made it unreadable to observer without specific keys or knowledge. The private key indicates the watermark's location in the host image. If the secret location is known, the watermark information can be recovered. One of the most popular watermarking-encryption methods is the Rivest-Shamir-Adleman (RSA) (Rivest, et al. 1978). RSA is known as an asymmetric cystography algorithm because it processed two different keys namely the Public key and Secret Key. The RSA algorithm is briefly explained below:

1. Two prime numbers p and q must be chosen at similar bit length. The key length of the public key is compute by

$$n = p \times q$$

2. The Euler totient ψ is given as

$$\psi(n) = (p-1)(q-1)$$

3. An integer e is choose to satisfy $1 < e < \psi(n)$ and $\gcd\left(e, \psi(n)\right) = 1$. Integer e is known as the public key.

4. The private key *d* is compute as given by $d = e^{-1} \bmod \left(\mathrm{y}(n)\right)$

5. Encryption is done use the below equation

$$K(m,e) = m^{e} \bmod n = c$$

   where *m* is the message, *e* is the public key and *c* is the cipher.

6. The message *m* is recovered using the private key *d*.

$$K(c,d) = c^{d} \bmod n = m$$

This method requires both the public and private keys for encryption/decryption. The private key is used to decrypt message that has been encrypted with public key. Thus, if the public key is exposed, they could not decrypt the message. However, an authorized user able to recovered the message using the private key. A public watermarking embeds its watermark into a known location of the host. Watermark software can extract the watermark information by scanning the host.

For optimal watermarking application, a trade-off cannot be avoided between the above mentioned criteria. For instance, if the watermarking scheme must be robust, then its image quality will be sacrificed, vice versa if the watermarking scheme must have high quality watermarked image, then its robustness will be scarified. Therefore, the right decision must be made for the type of application

2.4 Application of Digital Watermarking

Digital watermarking has been used in many applications and has been successfully protecting the digital work. Together with cryptography, watermarking represent an efficient method to ensure data integrity and authentication. This chapter categorizes the digital watermarking technologies into five groups according to their application:

1. Copyright Protection
2. Broadcast Monitoring
3. Fingerprinting Watermarks
4. Content Authentication
5. Healthcare Sector

2.4.1 Copyright Protection

Copyright protection is the most well-known watermarking application. The main concern for this type of application is where the owner wanted to protect their digital work that are widely distributing on the web. This watermarking scheme is designed to identify its authorized users as well as the source of the image. The watermarking schemes works by embedding an invisible watermark into the digital work. For a successfully copyright protection, this watermarking scheme requires very high level of robustness. A famous copyright protection algorithmic for digital image watermarking is proposed by Cox, et al. (1997). In this work the author embeds an invisible watermark image into the host image using the transform domain algorithmic.

The watermarking scheme has high robust against most attacks as it watermark information is spread evenly on the host image.

2.4.2 Broadcast Monitoring

The cost of producing news, movies and television shows series could cause more than $100,000 per hour (Juergen, 2005). Therefore, it is important that production companies to secure their intellectual properties and stop permitting illegal broadcasting actives. On the other hand, there are also several organizations and individuals who spend millions of dollar for advertising, wanted to ensure that they getting the royalties they purchased from advertising firms. To archive this, digital watermarking can be used monitor and track unwanted illegal broadcasting. The European ESPRIT project VIVA has offered solution for professional television broadcast monitoring system using digital watermarking (Termont, et al. 1999). This watermarking scheme works by embedding a unique watermark in each video or music clip before broadcasting. An automated system consists of a computer will then monitors the broadcasting and look for these watermarks in the video or music, and identifying when and where each clip appears.

2.4.3 Fingerprinting Watermarks

The design, purpose and the application of fingerprinting is different from the watermarking. Watermarking scheme relies on embedded watermark information in the digital work for verification. While fingerprinting does not embed any information; it analyzes the unique characteristics in the digital work. The identified pattern is then compared and match with the pattern stored. This allows the authorized owner to trace if their work is illegally distributed. Fingerprints takes in the digital work piece of content and store it in database to compare with new piece of content it encountered. However if an attacker able to identify the piece of content and altered them, then the digital work cannot be traced. Steinebach, et al. (2002) embeds unique watermark information into copies of client's digital work, i.e. music clip. The clients can play and redistribute the clip without any restriction. To trace piracy, the owners will do a content screening on these illegally copied clips. Each identified pirated clip is then analyzed for the existence of the watermark and compare with its information in the database.

Low, et al. (2007), on the other hand, proposed a fingerprint watermarking scheme based on human biometric features such as face, human fingerprint and iris recognition. The uniqueness, invariance, and the living characteristics of the human biological features are apposite for watermarking. By embeds these biometric features as watermark, it would help to resolve any ownership dispute.

2.4.4 Content Authentication

As technologies improve, it becomes easier to tamper digital work in such a ways that is difficult to detect. Cox, et al. (2008) reported that the Adobe Photoshop is the most commonly used computer software to modify the original image. If this image is an important piece of evidence in police investigation; any modification might pose a serious problem. The problem of authentication has been well studied (Stingson, 1995). A digital Signature technique is commonly used to address this problem. An asymmetric key is required to generate the digital signature and the key is governed by the authorized owner. When someone tried to changes the image content, they cannot create a new signature without knowing key. If someone compares the original digital signature with the modified image content, they will find the signatures does not match. However, these signature is metabase that must be transmit together with work. It is easy to lose the signature and it requires extra bandwidth to transmit it. A more preferable solution is to embed the signature directly into the work using watermarking. Chen, et al. (2001) offers such a watermarking systems by embeds the digital signature as authentication mark into the host image. The authentication marks design to be fragile watermark; as its content becomes invalid after a slight modification of work.

2.4.5 Healthcare Sector

In the last 10 years, advances in medical digital imaging equipment allows physician in health care sector to diagnose their patients using digital image from digital equipment such as Ultrasonic, Magnetic Resonance Imaging (MRI) and X-ray images However this generates large amount of digital data such as medical images at heath care center around the world.

Authenticity, integrity and confidentiality of the medical images are required as its information leads to life-threatening decision to make the right treatment. Therefore the medical image information must not be changed in any other way, or else it will leads to wrong decision being made. Moreover, the medical images are exchanged between healthcare centers thru unsecured networks which potentially lead to the tampering on its information. Therefore it is important to protect the authentication for these digital medical images. Although the main solicitation of digital watermarking is to protect the user intellectual properties, watermarking can offers tampering protection by embedding some secret mark in to the medical images. The watermarked image will be send over to the authorized user to extract the secret mark. If the recovered secret mark does not match with the original secret mark, the physician would discover some abnormalities in that received medical images and he/she would not proceed to make treatment based on that medical image. Zain, et al. (2004) proposed a watermarking scheme where a mark image is embedded into the ultrasound (US) images RONI (Region of Non-Interest).using least significant bits (LSB) algorithm. This is because the ROI is an area that contains patient diagnostically information. Any changes to this area will cause distortion, leads to wrong decision in giving treatment. Zain, et al. (2006) improved the security of the medical images watermarking scheme by adding the ability to detect tampering. Giakoumaki, et al. (2003) improved the watermark performances by embedded the mark image into RONI frequency region using discrete wavelet transformation (DWT).

2.5 Digital Image Watermarking Framework

2.5.1 Embedding the Watermark

Digital image watermarking is defined as an insertion of hidden information into a host image in such a way it appear imperceptible to naked eyes. A digital watermarking can be divided into of two categories: embedding and recover. Figure 2.1 shows embedding process.

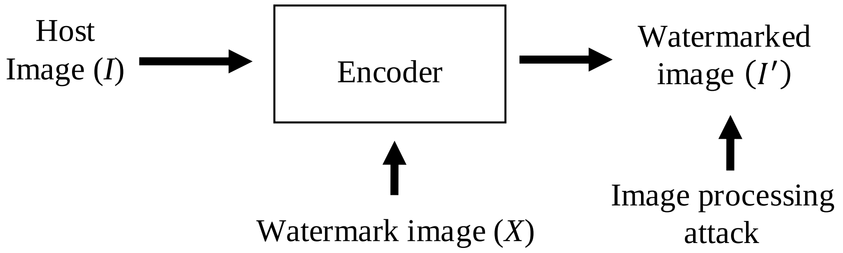


Figure 2.1: Embedding process

The encoder takes in the host image (*I*) and watermark image (*X*) to produce a new image called watermarked image I'. One can choose to embed the watermark image into the host image in spatial-domain or transform-domain of the host image. Spatial-domain watermarking involves modifying the host image pixel values. This method is simple and easy to implement. The most common spatial domain-watermarking algorithm is the Least Significant Bit (LSB). However the algorithm is not robustness against image cropping (Aggarwal, et al. 2011). On the other hand, transform domain watermarking schemes inserts a watermark into the host image frequency domain. The transformations algorithmic include discrete cosine transform (DCT), discrete wavelet transform (DWT) and singular value decomposition (SVD). These algorithmic will first transforms the host image into the frequency domain which consist of low, medium and high frequency. In general, most image information's is concentrated at low frequency and human eyes are sensitive to any changes in high frequency. Therefore the watermark image is usually embedded into medium frequency domain to obtain high quality and imperceptible watermarked image. The advantage of transform domain watermarking schemes is that the embedded watermark information is distributed evenly throughout the entire image.

The digital watermarking can be categorized into two stages: perceptible (visible) and imperceptible (invisible). The perceptible watermark can be found if the embedded watermark is intended to be visible. A watermark is said to be imperceptible if it is intended to be invisible to naked eye. The purpose of watermarking can be robust or fragile. A robust watermark intention is able to withstand the attacks from common image processing attack. Whereas a fragile watermark aims to sense whether the watermark has been altered.

The attacker can be classified as unintentional or intentional. The attacker intention is to disable and destroy the embedded watermark, making its watermark information unrecognized. Unintentional attack are those who are unaware of their action which may affect the watermark image, for instance, one chooses to reduce an image's size by using JPEG compression. The intentional attacker malignantly disable the watermark function for specific reason, for instance, to destroy the watermark image for an illegal purpose such as image forgery. In order to identify the robustness in watermarking techniques, some popular attack schemes are discussed in Chapter 2.6. The image processing attacks includes the noise, filter, image cropping, occlusion, JPEG compression and rotation.

2.5.2 Extracting the Watermark

Figure 2.2 shows the decoder takes in a watermarked image (I') to extract the watermarked image (X'). The watermark image may or may not be the same as the original watermark image X. There are two ways to find out whether the watermark image is the right one. Either the recovered watermark is compared with the original watermark by pixel to pixel or measures the watermark strength using correlation method. If the watermark recover process can be done without the original unmark host image, such watermarking techniques are known as blind watermark. In contrast, non-blind techniques required the original unmark host image to extract the watermark by comparison and correlation procedures. Note that watermark recover can only prove ownership whereas watermark detection can only verify ownership.

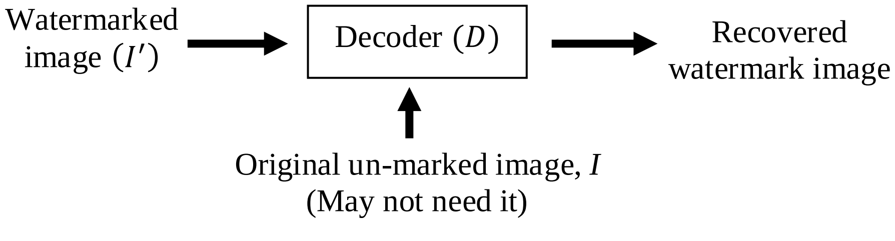


Figure 2.2: Recover process

2.6 Review of Watermarking Techniques

As previously mentioned, digital image watermarking techniques can be categorized into two embedding domain namely the spatial domain and frequency domain. In this chapter, the embedding domain algorithmic will be explained here.

2.6.1 Spatial Domain Techniques

Least Significant Bits (LSB) is the most simple and straight forward method introduced by Celik, et al. (2002) for spatial domain watermarking. During the embedding procedure, the watermark is first transformed into bit streams. Each bit streams is embedded into the specific bit for the host image. For instance the pixel value for grayscale image 254 in binary form is 11111110. If a modification is done on the 8th bit plane, it will change the pixel value by ±1. The image quality is kept best as human eyes cannot perceive these slight changes. In general, the modification on lower bit plane (i.e. 1st) offers higher robustness but this would significantly degrade the image quality.

In general, the LSB watermarking is easy to implement and offer high capacity than any other watermarking approaches. Despite its simplicity, LSB watermarking is at risk against attack such as noise addition. Furthermore the watermark robustness is limited, as changing far left bit plane will degrade image quality.

2.6.2 Transform Domain Techniques

Watermark technique in transform domain is more robust than spatial domain as the watermark information is spread entirely on the host image. To embed a watermark, a transform transformation is applied to the host image to covert its information to frequency domain. Then modifications are made to the image transformed coefficients. The most commonly used transform techniques are the Discrete Cosine Transforms (DCT), Discrete Wavelet Transforms (DWT) and Singular Value Decomposition (SVD).

Barnis (1998) proposed a watermarking scheme based on discrete cosine transform (DCT) to transform the host image into bands of frequencies coefficients (low, median and high). The watermark image is embedded into the medium frequency coefficient as they avoid effecting the image information (low frequency) and avoid being removed by noise and compression (high frequency). The host image and the watermark information are combined by the following Equation.

$$C'_{ij} = C_{ij} + \alpha W_{ij} \tag{2.3}$$

where C_{ij} is the frequency component of a host image, α is a weighting constant, and W_{ij} is the watermark image. The choice of α value affect the watermark robustness and imperceptible. One advantage of DCT includes its high energy compaction properties and fast computation algorithmic.

Barni, et al. (2001) introduces another watermarking schemes based on Discrete Wavelet Transformation (DWT) into digital watermarking. The DWT offers multi-resolution representation of an image and gives a perfect reconstruction of decomposed image. In other words, the DWT convert the image into sub-bands of different resolution namely the four frequency district (low-frequency district (LL), low-high frequency district (LH), high-low frequency (HL) district and high-high (HH) frequency districts. Since the image information gather at LL sub bands, any modification on these coefficients will significantly degrade the image quality. Therefore, the areas to embed the watermark are the high frequency sub-band HL, LH and HH. The watermark is embedded onto the selected coefficients in HL, LH and HH district:

$$x'i = xi + \alpha w_i \tag{2.4}$$

where w_i , and α are the selected coefficient and weighting constant, respectively.

On the other hand, Singular Value Decomposition (SVD) is one of the powerful linear algebra techniques and has been used in digital watermarking (Chung, et al., 2001 and Sun, et al., 2002). SVD offers some advantage over DCT and DWT, for instance, higher watermarked image quality can be expected as the SVD allows the maximum signal energy to be packed into a few coefficients as possible.

Sun, et al. (2002) proposed a SVD and quantization-based watermarking scheme. The first steps of embedding procedure is to decompose the image matrix (*I*) into three parts USV^T as given by

$$I = USV^T \tag{2.5}$$

where, matrix *S* is the diagonal matrix:

$$S = \begin{bmatrix} S_1 & 0 & 0 \\ 0 & S_{n-1} & 0 \\ 0 & 0 & S_n \end{bmatrix}$$

and the *U* and *V* are the orthonormal matrix:

$$U^T U = V^T V = I$$

The watermark image is embedded into the largest coefficients in diagonal matrix *S*:

$$S_w = S + \alpha W$$

where S_w is watermarked *S* matrix and α is the is weighting constant. After that, an inverse of the SVD transformation is performed to obtain the watermarked image:

$$I = US_w V^T$$

Since the largest coefficients in diagonal matrix resist to general image processing attack, SVD watermarking offers high robustness and image quality.

On the other hand, a FRT based technique is the combination of the spatial and frequency domain techniques. The FRT performs a rotation of signal in the time (spatial)-frequency plane to any order α between 0 and 1. Since the order σ of transform can be chosen between 0 and 1 freely, it can be considered as an extra key to protect the safety of the embedded watermark information. This intrinsic characteristic made FRT as a popular choice in improving the security of the watermark (Djurovic, et al., 2001 and Lang, et al., 2014). The FRT can be defined as:

$$P(\xi,\eta) = K\iint f(x,y)\,exp\left(\frac{j\pi(x^2 + y^2 + \xi^2 + \eta^2)}{tan\ \sigma_1} - \frac{j2\pi(xy\xi\eta)}{sin\ \sigma_1}\right)dxdy$$

where $f(x,y)$is the input image. $(x,y)$and (ξ,η) represent the space and fractional domain coordinates, respectively. The parameter K is given as:

$$K = \frac{exp\left[- j\,\tfrac{1}{4}\,\pi\mathrm{sgn}(sin\ \sigma) - \tfrac{1}{2}\,\sigma_1\right]}{\left|sin\ \sigma_1\right|^{1/2}}$$

where $$sgn = \begin{cases} -1 & \text{if } x < 0 \\ 0 & \text{if } x = 0 \\ 1 & \text{if } x > 0 \end{cases}$$

$$Q(p,q) = K\iint P(\mathrm{x},\mathrm{h})\exp\left(\frac{j\mathrm{p}(\mathrm{x}^2 + \mathrm{h}^2 + p^2 + q^2)}{\tan \mathrm{s}_2} - \frac{j2\mathrm{p}(pq\mathrm{xh})}{\sin \mathrm{s}_2}\right)d\mathrm{x}\,d\mathrm{h}$$

The $Q(p,q)$ is the encrypted image of the watermark $f(x,y)$.The encrypted watermark is embedded into the host image given by:

$$H_w(\rho,\sigma) = H_c(\rho,\sigma) + \alpha q(\rho,\sigma)$$

Furthermore, the FRT technique possesses dual characteristics of time-frequency domain and its robustness can be adjusted by changing the order σ. As the order α is close to 0, the FRFT as the transformation being dominantly in the time domain, while α is close to 1, the FRF is dominantly in the frequency domain.

2.7 Digital Image Processing Attacks

A watermark attack can be labeled as an intentional/unintentional process to remove or to simple destroying it watermark. Image processing attacks are used to test the watermark robustness. Thus, if an attack is said to be successfully if it able to remove or destroy the watermark, while retaining the quality of the digital image. On the other hand, different types of attacks are possible depending on the information and the tools the attackers processed. Digital image processing can be classified into two categories namely: Removal attack and Geometrical attack.

Removal attacks are designed to remove the watermark signal from digital image without trying to break the algorithm security. The attacker has little interest in finding out the encryption algorithmic as long as the watermark is removed. Noise attack, linear filtering and JPEG compression are common removal attacks used to remove the watermark image. On the other hand, Geometrical attacks come with intention to distort the watermark signals. The most common geometrical attacks are the Image cropping, Rotation and Occlusion. In the following chapter, each attack will be discussed in details.

2.7.1 Attack by Linear Filtering

Since most of the watermarking approaches tend to preserve the host image low frequency parts by embedded the watermark into mid or high frequency components. The Gaussian filtering, mean filtering and median filtering are used to attack such watermarking approach. The differences between these filters are the filtering ways is carried out. The Gaussian filter is a low pass frequency filter, which will filter out the high frequency components of the image while preserving the low frequency part of the image. In the spatial domain, the image pixel values are replaced by a window matrix whose component values are defined by the Gaussian function and its width σ. A sampled 3x3 Gaussian filter window matrix is given as

Figure 2.3: The watermarked image after the 3x3 Gaussian filter attacks.

Mean filtering and Median filtering are used to reduce the noise in images. The mean filtering works by replacing an image pixel values with the average (mean) value of its neighborhood and itself. The differences between mean filtering and median filtering are the way it's carried out. Instead of replacing the mean values, a median filtering will first sort all the pixel values from its surrounding neighborhood and then replacing the pixel being considered as middle pixel values. Figure 2.4 shows an example of the watermarked image after 3x3 mean filter and 3x3 median filter.

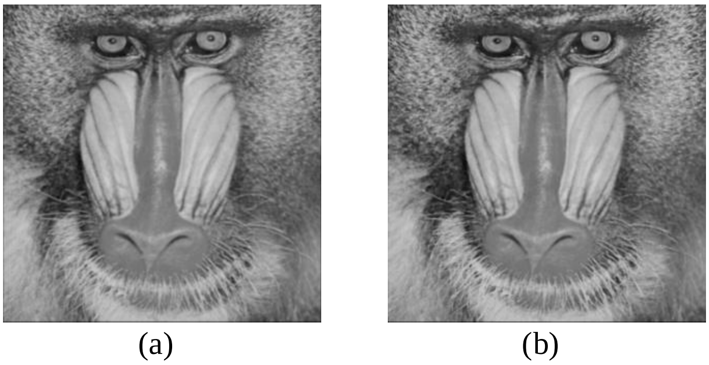

(a) (b)

Figure 2.4: The watermarked image after the 3x3 (a) Mean filter attack (b) Median filter attack.

2.7.2 Attack by Noise Addition

Gaussian noise is commonly used noise attack in image watermarking to reduce its visual quality. Gaussian probability distribution function PDF is the most commonly used probability distribution function to generate random numbers as shown in Equation 2.6:

$$p(z) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(\frac{z^2}{2\sigma^2}\right)$$

$$p(z) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{Z^2}{2\sigma^2}}$$

where σ is the width of the Gaussian probability density function. Figure 2.5 shows an example of the watermarked image after Gaussian noise at σ = 30.

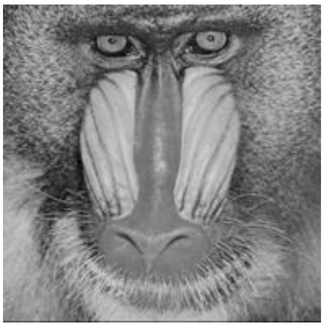


Figure 2.5: The watermarked image after the Gaussian white noise at σ = 30

2.7.3 Attack by JPEG Compression

JPEG compression is commonly use to resized and compressed image to meet the layout and bandwidth requirements. The lossy compression tends to remove image high-frequency components while preserve the lower ones. The JPEG compression values used in this project ranges from 100 (no compression) to 5 (highest compression). The smaller the quality factor, the more the watermark image quality degrades. Figure 2.6 shows an example of the JPEG compression attack at quality factor of 50.

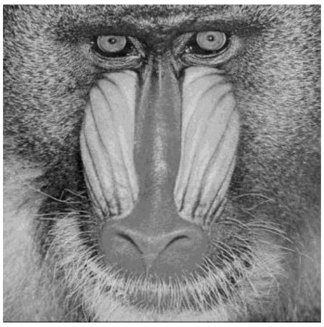


Figure 2.6: The watermarked image after the JPEG compression.

2.7.4 Attack by Image Cropping

Image cropping is a simple yet effective attacking operation to disable the watermark image. This is done by chopping off parts of the watermarked image. Visible watermarks are very vulnerable to this kind of attack, as the watermark image can be easily removed by cropping it off. Invisible watermark has the upper hand as the attacker unable to pin point the exact locations where the watermark image embedded. Figure 2.7 shows an example of the 50% cropped watermarked image. To test the proposed watermarking scheme against the cropping effect, the watermarked image is cropped from 90% until 60% of the original size.

F**igure 2.7: The watermarked image after 50% cropped of its original size.**

2.7.5 Attack by Occlusion

Occlusion is an unintentional attack caused by transmission error or inadequate bandwidth of the network. The watermarked image with 60% of its image occluded is shown in Figure 2.8.

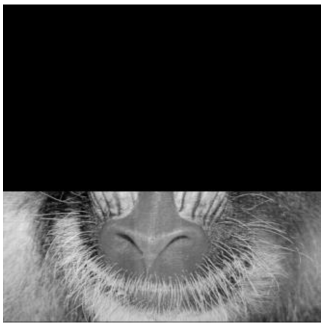


Figure 2.8: 60% occluded watermarked image.

2.7.6 Attack by Rotation

To apply rotational angle θ on to the watermarked image $f(x, y)$, let ϕ be the positive angle and the rotated watermarked image be $f*(x*, y*)$. Figure 2.9 illustrates the rotation from a point P to P^*. If r denotes the distance from P to the origin, the following formula can be derived as

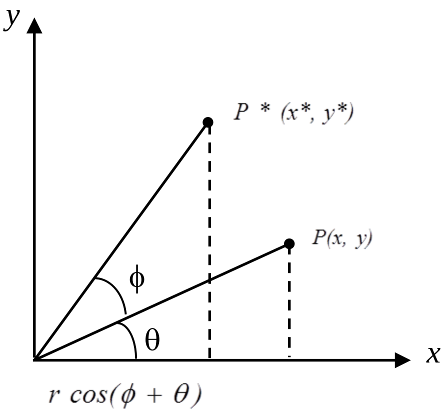


Figure 2.9: An illustration of rotation.

$$x = r \cos \phi \quad y = r \sin \phi$$

$$x^{*} = r \cos(\phi + \theta) = r \cos \phi \cos \theta - r \sin \phi \sin \theta = x \cos \theta - y \sin \theta$$

$$y^{*} = r \sin(\phi + \theta) = r \cos \phi \sin \theta + r \sin \phi \cos \theta = x \sin \theta + y \cos \theta$$

$$\begin{bmatrix} x^{*} & y^{*} \end{bmatrix} = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} \cos \theta & \sin \theta \\ - \sin \theta & \cos \theta \end{bmatrix}$$

Angle rotation does not usually affect the image commercial value but they can make the watermark untraceable. Figure 2.10 shows an example of watermarked image rotated by 5^{o} angle.

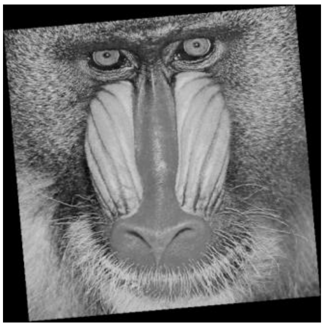


Figure 2.10 watermarked image rotated by 5^{o}.

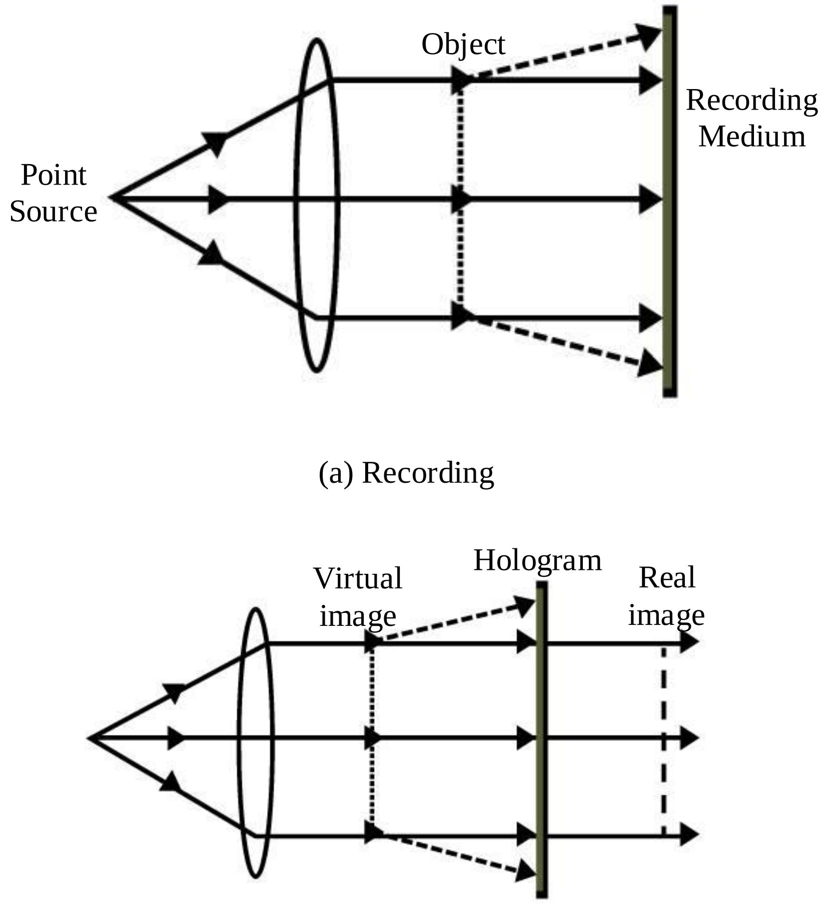
2.8 Digital Holography

2.8.1 Introduction

Holography coined from two Greek words ‘holos’ and ‘graphein’ which mean ‘entire write’. In other words, it involves recording and reconstructing the whole information of the optical wavefront, namely amplitude and phase. Holography involves a two-step process: firstly a coherent light illuminated an object of interest to produce interference fringes in a photosensitive medium. Secondly, the developed interference pattern is re-illuminated by the same coherent light to produces a three-dimensional image of the object.

Holography is a method of recording and reconstructing wavefronts that is based on recording the distribution of the intensity of an interference pattern formed by an object wave and a reference wave coherent with it. A recorded interference pattern is called hologram. D. Gabor (1948) discovered the principles of the holography during an attempt to improve the resolving power of the electron microscope. Gabor proposed to record interference pattern of electron waves by the superimposition of a coherent reference wave. Although unable to demonstrate the validity of his principle with electron waves, he was able to do so with visible light. This was the beginning of holography. Figure 2.11 shows the original holography setup developed by D. Gabor in 1948. Firstly a monochromatic light illuminates the transparency object. Secondly the directly transmitted light (reference wave) together with the light scattered by transparency (object wave) are recorded on a photographic plate. To reconstructs the object hologram, the developed photographic plate is re-illuminated with the same monochromatic light. Two images are reconstructed, where the virtual image appeared at the object original location, and the other, appeared at opposite location, forming the real image.

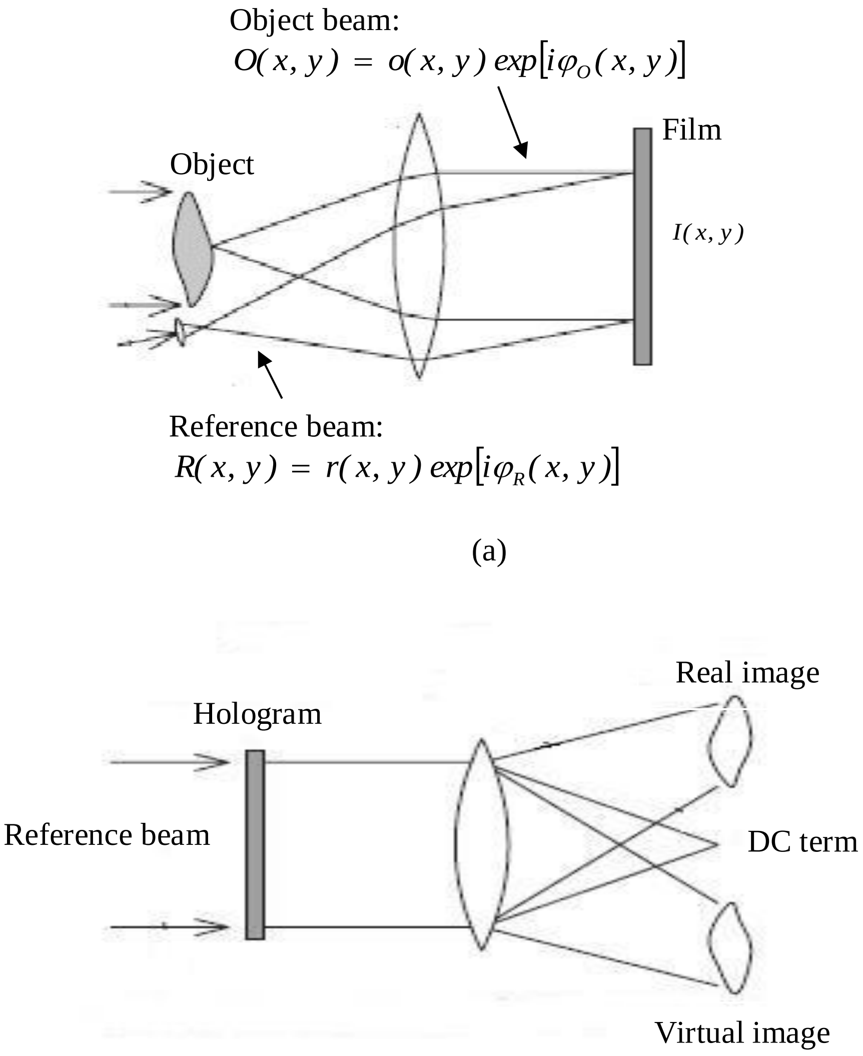
The main disadvantages of in-line hologram are the disturbed reconstruction due to bright reference beam and the twin images virtual and real image along the same line of sight. So while viewing one of them, an observer sees it superposed by an out of focus image of the other one. The presence of this unwanted image constitutes the most serious limitation of the in-line hologram, as well as the light source at that time is not truly "coherent" .These drawbacks are avoided when Leith and Upatnieks (1946) introduced the off-axis arrangement and the discovery of laser by Theodore Maiman at Hughes Research Labs. Figure 2.12 (a) shows the systematic diagram of the off-axis arrangement for hologram formation. In this method, a reference waves come in at an angle to form the interference pattern. As a result, the real image and the virtual image are separated from each other.



(a) Recording

(b) Reconstruction

Figure 2.11: Gabor In-line holography setup for (a) recording (b) reconstruction (Kries, 2005).



(a)

(b)

Figure 2.12: Off axis holography setup for (a) recording and (b) reconstruction of hologram (Kries, 2005).

The complex amplitude of the object and reference waves at plane $z = 0$ is given as:

Object wave: $$O(x, y) = o(x, y)\, exp[i\varphi_0(x, y)] \tag{2.6}$$

Reference wave: $$R(x, y) = r(x, y)\, exp(i2\pi fx) \tag{2.7}$$

where $f = sin\,\theta/\,\lambda$ is the spatial frequency of the reference wave, $o(x, y)$ and $r(x, y)$ are the real amplitude of the object and reference beam; and $\varphi_o(x, y)$ the phase of the object wave.

The resultant interference pattern can be calculated by determine Its intensity $I(x, y)$:

$$I(x, y) = |O(x, y) + R(x, y)|^2$$

$$I(x, y) = o^2(x, y) + r^2 + 2r^* o(x, y) \cos\left[2\pi fz + \varphi_o(x, y)\right] \quad (2.8)$$

For simplicity, the photograph plate is assumed to be process so that its amplitude transmittance is proportional to the intensity $I(x, y)$:

$$h(x, y) = t_o + \beta\tau I(x, y)$$

$$h(x, y) = t_o + \beta\tau\left[\left[o^2(x, y) + r^2\right] + 2ro(x, y) \cos\left[2\pi fz + \varphi_0(x, y)\right]\right]$$

where τ is the exposure time and β is a parameter constant dertermined by the photosensitive material. When the hologram is illuminated with same reference beam $R(x, y)$, as shown in Figure 2.12(b), the complex amplitude U(x, y) of the wave is given by:

$$\mathrm{U}(x, y) = R(x, y)h(x, y)$$

$$\mathrm{U}(x, y) = t_0 re^{i2\pi fx} + \beta\tau r|o(x, y)|^2 e^{-i2\pi fx} + \beta\tau r^2 o(x, y) + \beta\tau r^2 o^*(x, y)e^{i4\pi fx}$$

Four terms are obtained,

1.	$t_0 r e^{i2\pi fx}$	bright diffracted beam or also known as DC term
2.	$\beta\tau r\lvert o(x,y)\rvert^2 e^{-i2\pi fx}$	halo surrounding the transmitted beam
3.	$\beta\tau r^2 o(x,y)$	direct image (virtual)
4.	$\beta\tau r^2 o^*(x,y)e^{i4\pi fx}$	conjugate image (real)

In this arrangement, the virtual and real images are form and located opposite to each other. Thus this method eliminates the major drawbacks of Gabor in-line arrangement. The publication of Leith and Upatniek's work in 1962, 1963 and 1964 created an explosive interest in the field and the development of holography after that was very intensive. By 1965 to 1966, its theoretical and experimental foundations were laid and in the following years, holography developed mainly along the patch of improving its application. Progress continues to be made in the development of new materials and techniques sustaining a high level of interest in holography and its technical, commercial and its applications. In the present day holography is widely known as a practical means for storing wavefronts in a record from which the wavefronts may later be reconstructed.

Nowadays the hologram technologies can be found in various applications in the form of integral hologram, animated holograms and embossed holograms (Kreis, 2005), Integral hologram is a type of transmission hologram which is made from a series of photographs of an object which comes in various sizes and shapes. Integral hologram is widely used as advertising and art showcase. On the other hand, animated hologram has a similar concept to integral hologram. Except the differences is that the series of photograph is made from time-lapse photos. From the observer point of view, the subject appears to move as their viewpoint changes. While embossed hologram in a low cost/effective method against counterfeiter and it was widely found on credit cards and passport.

2.8.2 Holographic Interferometry

Holographic recording and reconstruction of a wave field is sufficient enough so that it can be compared interferometrically, either with a reflected by the object, or with another holographically reconstructed wave field. Holography interferometry allows the measurement of displacement and deformation without any physical contact (Jones and Wykes, 1989, Collier, et al., 1971) and Vest, 1976). In conventional holographic interferometry, two coherent wave fields, which are reflected by two different states scattered by the same object, are made to interfere. This interference is achieved in double-exposure holography by recording of the two wave fields on a single holographic plate. If the developed holographic plate is illuminated with a wave similar to the reference wave used in the process of recording, a holographic interferogram is formed. The fringe pattern represents the phase different between the interfering waves. In double exposure holographic interferometry two wavefronts scattered by the same object are recorded consecutively onto the same holographic film. The two wave fronts correspond to the different states of the object, one in an initial condition (undisturbed), and one (disturbed) after the change of physical parameter, figure by changing the object loading.

Let the complex amplitude of the object wave in initial state be

$$O_1(x,y) = o(x,y)\,exp\left[i\varphi_0(x,y)\right] \tag{2.9}$$

where $o(x,y)$ is the real amplitude and $\varphi_0(x,y)$is the phase distribution. The phase distribution $\varphi_0(x,y)$varies spatially in a random manner due to the microstructure of the diffusely reflecting or refracting object. The variation of a physical parameter to be measured, i.e. the object shaped due to the deformation of an opaque change in the phase distribution at point (x,y) by $\Delta\varphi_0(x,y)$. So the complex amplitude of the second wavefront to be recoded holograpahically onto the file is given as:

$$O_2(x,y) = o(x,y)\,exp\left[i\left(\varphi + \Delta\varphi_o(x,y)\right)\right] \tag{2.10}$$

where$\Delta\varphi_0(x,y)$is the change in the phase distribution at a point (x,y)After development of the holographic fil both wavefronts are reconstructed simultaneously, figure. Both wavefronts interfere and its intensity distribution $I(x,y)$is given as:

$$I(x,y) = \left|O_1 + O_2\right|^2 = (O_1 + O_2)(O_1 + O_2)^* \tag{2.11}$$

$$I(x,y) = 2o^2\left[1 + cos(\Delta\varphi(x,y)\right] \tag{2.12}$$

Equation 2.12 represents the intensity of the of the object, o^2, modulated by a cosine-shaped fringes pattern, $2[1 + cos(\Delta\varphi(x, y)]$. $\Delta\varphi_0(x, y)$ is the change of the interference pattern. Bright fringes are the contours, where the interference pattern is an even integer multiple of π. Dark fringes are the contours corresponding to odd integer multiple of π. In various applications, the interference pattern $\Delta\varphi(x, y)$ may be related to physical quantities such as displacement, rotation, strain, bending moment, vibration amplitude, temperature, pressure, mass concentration, and stress.

2.8.3 Digital Holography

In the early days of holography, the holograms were recorded on photographic films. These films have a very high resolution (e.g., 5000 lines/mm), but this process is time consuming as wet chemical treatment is needed. Researchers have investigated the possible use of fast electronic recording with sufficient resolution to record and evaluate holograms and holographic interferograms in nearly real-time. The first digital reconstruction of a holographic image was accomplished by Kronrod, et al., 1972. Unfortunately, at that time the laboratory equipment did not allow digital recording of holograms and the computer calculation power was insufficient to introduce the new idea into practice. Schnars and Juptner, (2002) proposed the setup for digital holography. The holographic process was divided into two steps: the 1st step is to capture the hologram of an object with the aid of CCD camera and the 2nd step is to reconstruct the hologram by computer calculations. The most important advantage of such a process is absence wet processing connected with the photographic material development.

The tremendous development in optoelectronics and computer technology of the last two decade - increasing data processing speed and memory capacity, as well as the CCD cameras having more and smaller pixels made holographic recoding better suited to an industrial environment. Therefore a digital recording of the primary holograms and a numerical reconstruction of the complex beam fields from the recorded intensity fields would offer real advantages to holographic interferometry metrology. Digital holography is applied with success in optical deformation and strain analysis, shape measurement, microscopy and for investigations of flows in liquids and gases.

One of the disadvantages of digital holographic is that the resolution of the CCD camera resolution used for recording is lower than the resolution of the photographic films used for conventional holography recording. Another issue facing by digital holography is suppression of the bright undiffracted wave or DC term and the separation of conjugate image. Although the off-axis recording setup able to segregate the DC term and conjugate image, the setup also increases the system spatial resolution requirements and produced a low resolution in the resultant holograms. Yamaguchi (1997) solved these drawbacks by altering the phase of the reference waves by ($0, \pi/2, \pi, 3\pi/2$) using a Quarter-wave plate and a half-wave plate. For each of the shifted reference wave, one interferograms is recoded by the CCD camera

$$I(x,y,\theta) = \left|U_R(x,y) + U(x,y)\right|^2$$

$$I(x,y,\theta) = \left[U_R(x,y)\right]^2 + \left[U(x,y)\right]^2 + 2\,Re\left\{\, U_R(x,y)U^*(x,y)e^{j\theta} \,\right\}$$

where $U_R(x,y)$ and $U(x,y)$ are the complex amplitude of the reference wave and object wave. $I(x,y,\theta)$ represent the recorded interference pattern (interferograms) of θ radians of the phase shift. To obtain the resultant hologram, the four interferograms intensity is combined using

$$I_1 = I(x,y,0 - I(x,y,\pi) \qquad (2.13)$$

$$I_2 = I(x,y,\pi / 2) - I(x,\; y,\; 3\pi / 2) \qquad (2.14)$$

Combining Equations 2.13 and 2.14 yield

$$I_1 + jI_2 = 4A_R^{\,*}U$$

The recorded 3D object complex amplitude $U(x,y)$ is calculated by taking four different phase shifts of the reference wave as given by

$$U(x,y) = \frac{I_1 + jI_2}{4A_R} \qquad (2.15)$$

where A_R is the constant amplitude of the reference wave. Phase shifting digital holography offers higher image quality and a wider viewing angle than off-axis digital holography. One disadvantage of phase shifting interferometry is recording process is time consuming as four interferograms are needed to retrieve the 3-D object hologram information. Improvements have been makes to reduce the steps taken to record phase shifting hologram. Awatsuji, et al. (2005) proposed a three-steps phase shifting interferometry to improve Yamaguchi work. The object complex amplitude $U(x, y)$ is determined by combined the intensity three hologram interferograms and calculated using Equation 2.16 yields:

$$U(x, y) = \frac{I_1 - I_3 + j(2I_2 - I_1 - I_3)}{4A_R} \quad (2.16)$$

With these reduced steps taken, the process of recording hologram, using phase shifting digital holography, is significantly speed up.

The holographic technology offers unparalleled high-quality images and displays a three-dimensional image of the object without the need of any special optical tools. But, the process of recording 3D object holograms requires the interference between the object wave and reference wave. The optical component must be setup in a very stable environment with low vibration. This is because very slight vibration can easily destroy the interference fringes. The optical holographic must be setup in a dark room environment as any external light source will disturb the formation of the hologram. These requirements, together with the expensive optical component have prevented optical hologram recorders from outdoor recording usage. One the other hand, a more practical for these limitations would be the use of computer-generated hologram (CGH) (Abookasis and Rosan, 2003). Instead of replying to optical setup, the three-dimensional objects can be constructed using and represented in the computer using mathematical model. The interference between the light waves is substituted by mathematical computation. The process of GHC takes in a two dimensional image as the object and multiplied by a random phase obtain the object wave. The resulted object wave is Fourier Transformed and multiplied by a spherical phase factor to form the computer generated hologram.

2.8.4 Wavefront Reconstruction

Consider a transmittance plane $t(x, y)$placed at z = 0 and an image plane $\Gamma(\zeta, \eta)$ place at distance d away from the transmittance plane, as shown in Figure 2.13. The transmittance is illuminated by a plane wave $R(x, y) = a\, e^{ikp}$ propagating parallel to *z*-axis.

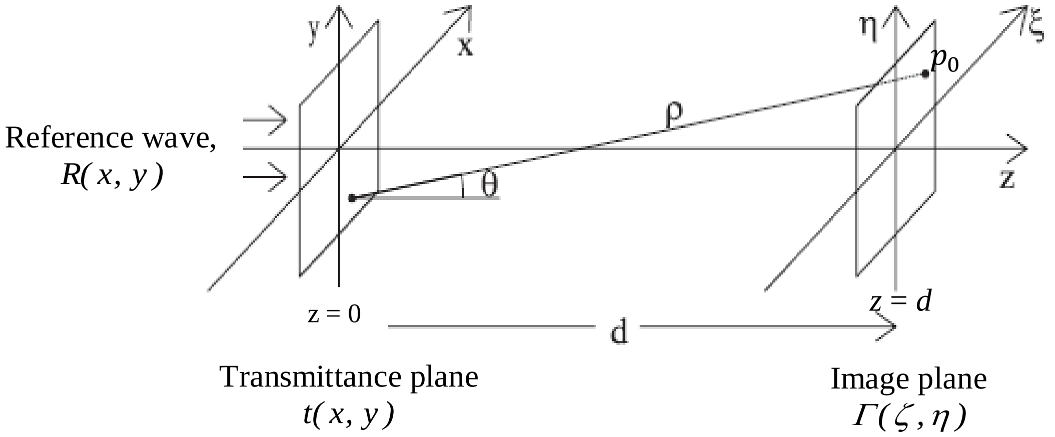


Figure 2.13: Coordinate system for transmittance plane and image plane.

The wave field at the point p_0 that is the distance d away from the transmittance plane, is given by integration over all spherical waves emitted from the *(x, y, 0)* plane, and can be described by the Fresnel Kirchhoff integral

$$\Gamma(\xi,\eta) = \frac{i}{\lambda}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} t(x,y)R(x,y)\,\frac{exp\left(-\,i\,\frac{2\pi}{\lambda}\,\rho\right)}{\rho}\left(\frac{1}{2}+\frac{1}{2}\cos\theta\right)dxdy \quad (2.17)$$

where ρ is the distance between a point in hologram plane and a point in image plane given as:

$$\rho = \sqrt{d^2 + (x-\xi)^2 + (y-\eta)^2} \quad (2.18)$$

where (x, y) and (ξ,η) are the coordinates in the hologram plane and in the plane of the real image respectively as illustrated in Figure 2.13. $t(x, y)$ is the transmittance plane of the hologram, *k* is the propagation constant $(=(2\pi/\lambda))$. The θ is the angle between the distance of transmitting plane and image plane

In order to simplify the integral evaluation, a few assumptions have to be made. This approximation will be discussed in the next chapter.

2.8.5 Classification of Holograms

Holograms can be classified according to the way of forming the object and the reference waves and also according to the way of recording the interference pattern (Kreis, 2005). Depending on the arrangement of the object and the hologram, and also on the presence of optical elements between them, the relationship between the amplitude distribution in the phase of the hologram and the corresponding distribution directly after the object can be described by the Fresnel-Kirchhoff diffraction integral (Equation 2.16).

2.8.6 Fresnel Hologram Reconstruction

The most general kind of hologram is the Fresnel hologram as shown in Figure 2.14. It is formed when a hologram is in the near field diffraction region.

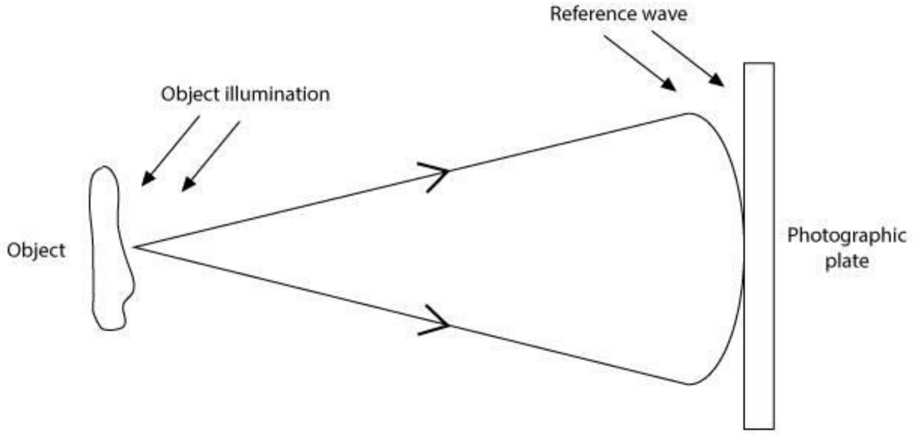


Figure 2.14: Recording of Fresnel hologram.

In order to simplify the evaluation of this integral, a few assumptions have to be made. First assumption is that the values in *x, y* and ξ, η should be smaller than the distance (*d*) separating the two planes, so that the Equation 2.18 can be expressed by Taylor series expansion.

Let u^2 be:

$$u^2 = (x - \xi)^2 + (y - \eta)^2 \qquad (2.19)$$

Substitute u^2 into Equation 2.18:

$$\mathsf{r} = d\sqrt{1 + \frac{u^2}{d^2}}$$

$$\mathsf{r} = d\left[1 + \frac{u^2}{2d^2} - \frac{\frac{1}{2}\left(\frac{1}{2} - 1\right)\left(\frac{u^2}{d^2}\right)^2}{2!} + \cdots\right]$$

$$\rho = d + \frac{(\xi - x)^2}{2d} + \frac{(\eta - x)^2}{2d} - \frac{(x - \xi)^2 + (y - \eta)^2}{8d^3} + \cdot\cdot\cdot$$

The first two terms are considered:

$$\rho \approx d + \frac{(\xi - x)^2}{2d} + \frac{(\eta - x)^2}{2d} \qquad (2.20)$$

By substituting the Equation 2.20 into Equation 2.17 with $\cos\theta \approx 1$. Equation 2.17 can be further simplified since the distance d is larger than x, y and ξ, η values, the dominator part can be replaced with d. The resulting expression for the Fresnel-Kirchhoff integral now becomes:

$$\begin{aligned}\Gamma(\xi,\eta) = \frac{i}{\lambda d} exp\left(i\frac{2\pi}{\lambda}d\right) exp\left(-i\frac{\pi}{\lambda d}(\xi^2 + \eta^2)\right) \\ \times\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} t(x,y)R(x,y)\, exp\left(-i\frac{\pi}{\lambda d}(x^2 + y^2)\right) \\ \times exp\left(i\frac{2\pi}{\lambda d}(\xi x + \eta y)\right)dxdy\end{aligned}$$

(2.21)

Equation 2.21 is known as the Fresnel transformation

2.8.7 Numerical Reconstruction of Fresnel Holograms

Fresnel holography is the most general kind of holography methods. Therefore in this dissertation, a Fresnel hologram is generated on CCD-sensor, which acts as the recording medium allowing digitization and storage in digital image processing system memory. In reconstruction of the real image, the digitized holograms are processed numerically. This process involved numerical realization of the Fresnel-Kirchhoff diffraction integral. In this chapter a detailed description on the numerical reconstruction based on Fresnel-Kirchhoff diffraction integral is discussed. After the description of the digitization of the Fresnel-Kirchhoff diffraction integral, the numerical algorithm of reconstruction based on this discrete representation equation is discussed.

In numerical evaluation of the Fresnel-Kirchhoff integral, Eq. (2.21), for the discrete finite, the terms $\left(-i\frac{2\pi}{\lambda}d\right)$ is omitted, as it has no effect on the intensity and interference pattern of the holograms. The digitization on the Fresnel approximation is done by substitute the following equation:

$$\begin{aligned}\Gamma(\xi,\eta) = {} & exp\left(-i\frac{\pi}{\lambda d}(\xi^2+\eta^2)\right) \\ & \times\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} t(x,y)R(x,y)\, exp\left(-i\frac{\pi}{\lambda d}(x^2+y^2)\right) \\ & \times exp\left(i\frac{2\pi}{\lambda d}(\xi x+\eta y)\right)dxdy\end{aligned} \tag{2.22}$$

The computational method used for this discrete synthesis depends on the form of the digitization of the amplitude transmission of the hologram, $t(x,y)$. The simplest way to digitize $t(x,y)$is to specify it as a matrix of numbers $t(x,y)$taken on a rectangular raster with certain steps Δx and Δy along coordinates (*k*, *l*). This description is based on the sampling theorem by Stern and Javidi (2006). To transform from this discrete description to a continuous description of $t(x,y)$ a linear interpolation of the readings is used. Mathematically, the interpolation can be described as the transformation of the series (Kreis, 2005).

$$t(x,y) = \sum_{k=0}^{N_x-1}\sum_{l=0}^{N_y-1} t(k,l)\delta(x-k\Delta x, y-l\Delta y) \tag{2.23}$$

where δ is the delta function. The ranges of *k, l,* N_x, N_y are governed by the dimensions of the hologram and the digitization step. Practically, $t(x,y)$is non-vanishing in the rectangular [-X_{MAX}, X_{MAX}, -Y_{MAX}, Y_{MAX}], then

$$N_x = \frac{2X_{MAX}}{\Delta x} \quad \text{and} \quad N_y = \frac{2Y_{MAX}}{\Delta y} \tag{2.24}$$

An accurate interpolation of $t(x, y)$ from $t(k, l)$ is possible if

$$\Delta x = \frac{\lambda d}{2\xi_{max}} \qquad \text{and} \qquad \Delta y = \frac{\lambda d}{2\eta_{max}} \tag{2.25}$$

Substitution of Equations (2.23), (2.24) and (2.25) into Equation (2.22) show that the Fresnel hologram of the discrete object $t(x, y)$can be calculated as finite sum

$$\begin{aligned} \Gamma(\xi,\eta) &= exp\left(-i\frac{\pi}{\lambda d}(\xi^2+\eta^2)\right) \\ &\times\sum_{k=0}^{N_x-1}\sum_{l=0}^{N_y-1} t(k,l)R(x,y)\,exp\left(-i\frac{\pi}{\lambda d}(k^2\Delta x^2+l^2\Delta y^2)\right) \\ &\times exp\left(i\frac{2\pi}{\lambda d}(k\Delta\xi x+l\Delta\eta y)\right)dxdy \end{aligned} \tag{2.26}$$

The digitization in Equation 2.26 is now extended to ξ and η. This procedure is similar to that digitize $t(x, y)$, the function $\Gamma(\xi,\eta)$ can be reconstructed by a linear interpolation of the discrete function:

$$\Gamma(\xi,\eta) = \sum_{m=0}^{N_X-1}\sum_{n=0}^{N_Y-1}\Gamma(m\Delta\xi,n\Delta\eta)\delta(\xi-m\Delta\xi,\eta-n\Delta\eta) \tag{2.27}$$

where $\Gamma(m\Delta\xi, n\Delta\eta)$ is the reading of $\Gamma(\xi,\eta)$ taken on rectangular raster with step $\Delta\xi$ and $\Delta\eta$ along the coordinates (ξ,η). Thus, the digitization of Equation 2.27 becomes:

$$
\begin{aligned}
\Gamma(\xi,\eta) &= \exp\left(-i\frac{\pi}{\lambda d}(m^2\xi^2+n^2\eta^2)\right)\\
&\times\sum_{k=0}^{N_X-1}\sum_{l=0}^{N_Y-1}t(k,l)R(k,l)\exp\left(-i\frac{\pi}{\lambda d}(k^2\Delta x^2+l^2\Delta y^2)\right)\\
&\times\exp\left(i\frac{2\pi}{\lambda d}(k\Delta xm\Delta\xi+l\Delta\xi n\Delta y)\right)dxdy
\end{aligned}
\tag{2.28}
$$

The maximum values of N_X and N_Y for which the sum in Equation 2.28 must be calculated are determined by:

$$
N_X = \frac{\lambda d}{\Delta\xi\Delta x} \qquad \text{and} \qquad N_Y = \frac{\lambda d}{\Delta\eta\Delta y}
$$

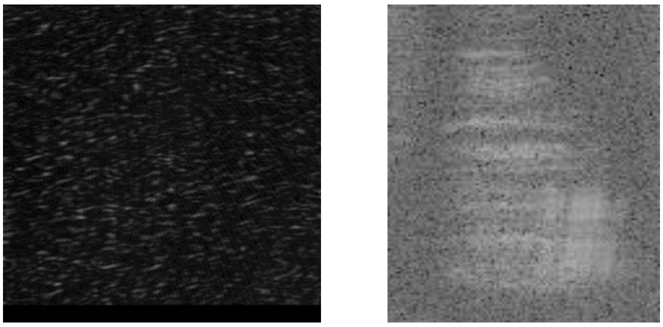
For the case $N_X = N_Y = N$, the Equation 2.28 can be rewritten as:

$$
\begin{aligned}
\Gamma(m,n) &= \frac{i}{\lambda d}\exp\left[-i\pi\left(\frac{m^2}{N^2\Delta x^2}+\frac{n^2}{N^2\Delta y^2}\right)\right]\\
&\times\sum_{k=0}^{N_X-1}\sum_{l=0}^{N_Y-1}t(k,l)R(k,l)\exp\left(-i\frac{\pi}{\lambda d}(k^2\Delta x^2+l^2\Delta y^2)\right)\\
&\times\exp i2\pi\left(\frac{km}{N}+\frac{ln}{N}\right)
\end{aligned}
\tag{2.29}
$$

In most applications, only the intensity and the phase different of the reconstructed hologram are of interest, thus the phase factor $\exp\left(-i\frac{\pi}{\lambda d}(k^2\Delta x^2+l^2\Delta y^2)\right)$ in Equation 2.29 can be neglected. This phase factor is independent of the evaluated hologram, thus at each point it gives the same phase shift in all reconstruction of different object states and cancels out in the phase-subtraction process of holographic interferometry. For this reason, Equation 2.29 can be rewritten as follow:

$$\begin{aligned}\Gamma(m,n) = \sum_{k=0}^{N_X-1} \sum_{l=0}^{N_Y-1} t(k,l)R(k,l) \\ \times exp\left(-\, i\,\frac{\pi}{\lambda d}(k^2\Delta x^2 + l^2\Delta y^2)\right)\ exp\ i2\pi\left(\frac{km}{N} + \frac{ln}{N}\right)\end{aligned} \tag{2.30}$$

Equation (2.30) is known as the Discrete Fresnel Transform (DFT). The recorded intensity pattern $t(k,l)R(k,l)$ is determined by reading the hologram's image, as shown in Figure 2.15. The complex amplitude $\Gamma(m,n)$ is determined by multiply $t(k,l)R(k,l)$with $\exp\left(-i\frac{\pi}{\lambda d}(k^2\Delta x^2 + l^2\Delta y^2)\right)$. In calculation of the transformation, the standard Fast Fourier Transform (FFT) can be applied (Kreis, 2005), which will provide an effective calculation.



(a) (b)

Figure 2.15: (a) Digital hologram of a pyramid-shaped object and (b) numerical reconstructed real image of the digital hologram.

The reconstructed real image $\Gamma(m,n)$ is a complex function, so both intensity and the phase can be calculated. This is in contrast to the optical reconstruction making only the intensity visible. Then intensity can be determined by

$$I(\xi,\eta) = \left|\Gamma(\xi,\eta)\right|^2 = Re\left|\Gamma(\xi,\eta)\right|^2 + Im\left|\Gamma(\xi,\eta)\right|^2 \qquad (2.31)$$

and the phase distribution is calculated by

$$\delta(\xi,\eta) = \frac{Im\left|\Gamma(\xi,\eta)\right|}{Re\left|\Gamma(\xi,\eta)\right|} \qquad (2.32)$$

where *Re* denotes the real part and *Im* is the imaginary part. If the sign of $Im\left|\Gamma(\xi,\eta)\right|$ and $Re\left|\Gamma(\xi,\eta)\right|$ is taken into account separately, $\delta(\xi,\eta)$ takes the values in [–π, +π] the principal values of the arctan function. As a consequence of the surface roughness of the object, the phase varies randomly.

2.9 Digital Holographic Interferometry

In this chapter a method of digital of digital holographic interferometry by Schnars and Juptner (2002) is described here. Two holograms, which represent the undistorted and the distorted state of the object, are recorded on a CCD- target and digitally stored in the computer memory. Then they are added points-wisely, and the numerical reconstruction of this sum wave fields leads to a holographic interferogram. In the numerical reconstruction process not only the intensity, but also the phase of a holographically stored wavefront can be calculated. This mean that the interference pattern, which represent the deformation field quantitatively, can be calculated directly by subtracting the reconstructed phases of the undistorted and the distorted object wave.

2.9.1 Digital Interference pattern

If the two holograms $h_1(k,l)$ and $h_2(k,l)$ are reconstructed separately, their phase distribution $\varphi_1(\xi,\eta)$ and $\varphi_2(\xi,\eta)$ can be calculated separately with Equation 2.32. The interference pattern, which is the phase difference between the wave field of the object before and after a change of the loading, is then calculated by using Schnars's (1994) method

$$\Delta\varphi(\xi,\eta) = \begin{cases} \varphi_1(\xi,\eta) - \varphi_2(\xi,\eta) & \text{if} \quad \varphi_1 \geq \varphi_2 \\ \varphi_1(\xi,\eta) - \varphi_2(\xi,\eta) + 2\pi & \text{if} \quad \varphi_1 \leq \varphi_2 \end{cases} \tag{2.33}$$

where $\varphi_1(\xi,\eta)$ and $\varphi_2(\xi,\eta)$ are the individual phases, respectively

Although the individual $\varphi_1(\xi,\eta)$ and $\varphi_2(\xi,\eta)$ are randomly fluctuating from point to point, the difference modulo 2π is deterministic. This difference is the interference pattern distribution governed by the deformation of the object surface. Equation (2.33) permits the calculation of the interference pattern directly from the digitally sampled holograms. The evaluation of a fringe pattern, as in conventional hologram interferometry, is not necessary. The two possible approaches to achieve the interference pattern distribution in the digital interferometry are summarized in Figure 2.15.

2.10 Digital Watermarking using Digital Holographic Techniques

2.10.1 Introduction

As demand for watermark security and performances keep increasing, researchers begin to look into the possibility applying optical technology into digital watermarking. This is because optical technology especially digital holography technique processed certain unique characteristics which normal traditional watermark does not provide. These characteristics are further explained and experiment in Chapter 3 and Chapter 4.

Digital holographic watermarking techniques can be divided into two groups in terms of application. The two categories are digital holographic watermarking and secure holographic watermarking. Researchers in holographic watermarking are interested in searching for optimum embedding conditions to obtain the best watermark performances. Transform domain techniques are usually used in embedding the watermark as these algorithmic delivers the much needed perceptual quality and robustness.

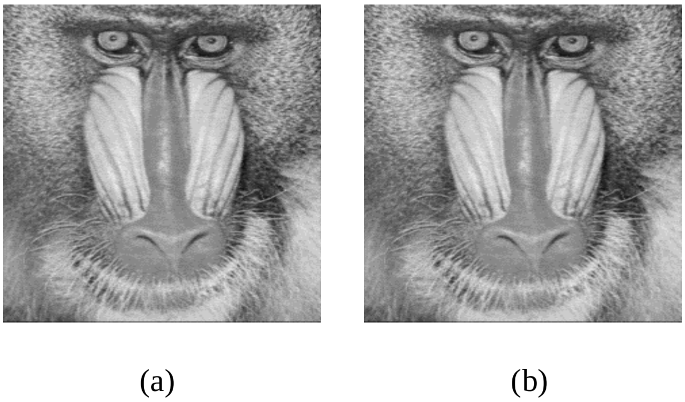
However the security holographic watermarking is not safe as the optical parameters such as the (laser of wavelength & recording distance) can be easily deducted. Therefore in secure holographic watermarking, researcher usually employed image encryption methods including Double Random Phase Encoding (DRPE), three step phase shifting interferometry (PSI) and Fractional Fourier Transform (FRT) to make its watermark information unreadable to the unauthorized user. These methods use large quantity of keys data to encrypt the watermark information before embedded into the host image. To recover the watermark information, the watermarked host image and the keys are transmitted to the authorized user via Internet.

2.10.2 Holographic Watermarking

Takai and Mifune (2002) are the first to propose Holographic watermarking, where a watermark image is first transformed into Fourier hologram by numerical simulating the physical phenomena of light diffraction and interference. The watermark is then embedded into the image in spatial domain as given by:

$$P_m(\xi,\eta) = P(\xi,\eta) + \alpha(\xi,\eta)H(\xi,\eta) \tag{2.34}$$

where $P_m(\xi,\eta)$ is the watermarked image and $\alpha(\xi,\eta)$ is the weighting constants. In Figure 2.16 shows an example of the original and watermarked baboon images using Takai and Mifune's with Fresnel hologram (pyramid-shaped object). Figure 2.17 shows the numerical reconstructed pyramid-shaped object Fresnel hologram from watermarked baboon image.



(a) (b)

Figure 2.16: (a) Original Baboon image. (b) Watermarked Baboon image digital holographic watermarking method proposed by Takai and Mifune (2002)

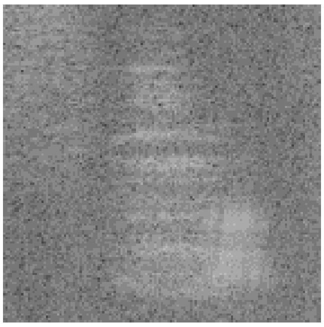


Figure 2.17: The watermark (pyramid shaped object hologram) recovered from the watermarked Baboon image using digital holographic watermarking method proposed by Takai and Mifune (2002) method.

Takai and Mifune’s experiment results show that the scheme is robust against cropping and occlusion. However, the downside of this proposed method is that the host image has to be low pass filter to remove the high-frequency components of the host image before the embedding stage. Hence the watermarked image quality is degraded.

To solve this, the Fourier hologram is embedded into the host image discrete cosine transform (DCT) domain (Chang and Tsan ,2005). Figure 2.18 shows the location of median frequency coefficients of the DCT transformed host image.

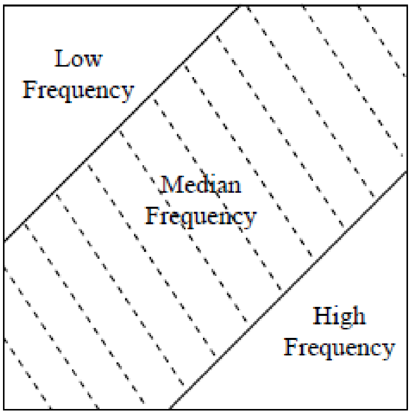
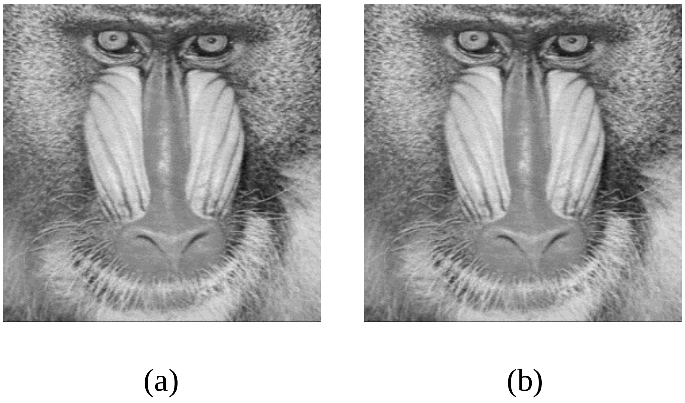


Figure 2.18: Median frequency DCT coefficients for embedding the watermark proposed by Chang and Tsan (2005)

To obtain higher quality image, the size of the hologram is chosen half of the original image but can be choose smaller if one desired to obtain to higher image quality. The half size hologram $H(\xi,\eta)$ is embedded onto the median frequency coefficients given by the Equation below:

$$Q'_{med}(\xi,\eta) = Q_{med}(\xi,\eta) + \alpha H(\xi,\eta)$$

where $Q'_{med}(\xi,\eta)$ and $Q_{med}(\xi,\eta)$ is the low and high frequency coefficients respectively. The watermarked image is obtained by taking inverse DCT of the modified DCT coefficients. Figure 2.19 shows the watermarked baboon image with the half of the pyramid-shaped object hologram as watermark using weighing factor $\alpha = 0.5$.



(a) (b)

Figure 2.19: (a) Original Baboon image. (b) Watermarked Baboon image using digital holographic watermarking method proposed by Chang and Tsan (2005)

In general, the image information's are concentrated at the low frequency coefficient. Modifying these coefficients will degrade the image quality, though the image quality can be preserved by embeds the watermark into either the median frequencies of the transformed host. The high frequency is not suitable as it valuable to attacks. Furthermore, this method provides robustness against common image processing attacks besides image compression.

Holographic watermarking using DCT domain offers high perceptual quality and robustness, but there is a flaw in these methods which causes the image edge to be fuzzy for line singularity. Huang (2010) presented a digital holographic watermarking based on Ridgelet transform. In this method, the host image is decomposed into each blocks which is followed by calculate its Ridgelet coefficient. Once the Ridgelet coefficients matrix is determined, the watermark is embeds into the matrix using Equation 2.3. Similar to DCT watermarking, Ridgelet transform watermarking is weak against image compression attack.

In an attempt increase the watermark resistant to image compression, a watermarking scheme based on Quantization Index Modulation (QIM) is proposed (Osman, et al., 2007). In this method, the watermark is embedded into the host image transformed using three level discrete wavelet transform domain (DWT). The idea behind this DWT transform is to divide the host image into parts and arrange it according to the signal frequency spectrum. For example a 1-level DWT split the host image signal into two parts as low frequency and high frequency components. The low frequency part is then split into two parts until 3-level desired level of decomposition is obtained as shown in Figure 2.20. In general most of the image information is concentrated at the lower frequency sub-bands I^0 and watermarks embedded in these sub-bands will degrade the image quality. However embedding lower frequency sub-bands I^0 could increase robustness significantly especially against the image compression. On the other hand, the high frequency sub-bands I^3 which include the edges and textures of the image, the human eye is sensitive enough to see these changes in high frequency sub-bands. This allows one to embed the watermark into the host image without being obvious to the naked eyes. However embedding in these sub-bands reduce the robustness against most image processing attacks The original host image signal can be obtained by taking an inverse DWT (IDWT) on the decomposed image signal.

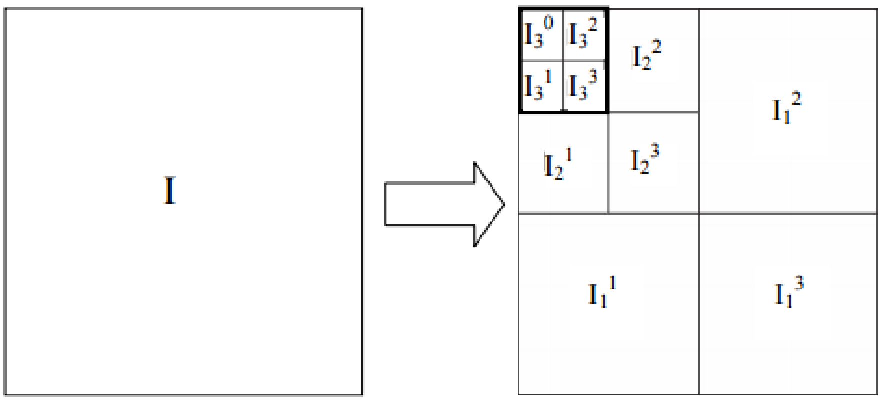
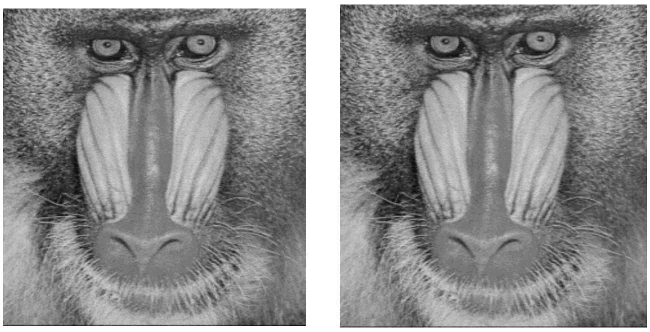


Figure 2.20: Three-level Discrete Wavelet Transform (DWT) of host image as proposed by Osman, et al. (2007).

On the other hand, the general purposed of Quantization Index Modulation (QIM) is to embed one signal into another host signal to create another composite signal. In other words, when the watermark (signal) is embedded into the host signal (host image), the resultant watermarked image quality and robustness can be adjusted by altering the step size of the quantizer. Figure 2.21 shows the watermarked baboon image using Osman et al. method's using 256 Bin quantizer.



(a) (b)

Figure 2.21: (a) Original Baboon image. (b) Watermarked Baboon image digital holographic watermarking method proposed by Osman, et al. (2007).

Moreover, watermarking in the DWT domain has higher resistant towards image compression than watermarking in DCT domain. The weakness of this research is that the watermarking quantizer is determined experimentally. Furthermore there is a trade-off between watermarked image robustness and its perceptual quality.

Li and Kim (2009) combined both DWT-SVD domains to improve the watermark capacity. In this method, the original host image is transformed into DWT domain using the 2-level DWT algorithmic. The information located in the low-high frequency sub-band is used to generate the SVD coefficient. The uses of SVD algorithmic further compress the image energy into as few coefficients as possible, which allow the DWT-SVD combination to insert of watermark up to 384bit size, but beyond that, the results may deteriorate. Li and Kim methods embed computer generated hologram and not optically captured hologram, which obviously has larger file sizes.

Barni, et al. (2001) and Sun, et al. (2002) proposed a watermarking scheme which can resist against various image processing attacks, however geometric attacks such as print scan still pose a major problem. The watermarked image when it is printed as a hard copy, the embedded watermark is likely to be destroyed and make it undetectable from scans. Levy and Shaked (2001) while working for Hewlett-Packard (HP), they proposed a hardcopy watermarking where a discrete Fourier transform (DFT) coefficient is first modified based on print-scan noise characteristics. This is because the Discrete Fourier transform domain embedding is resist to misalignment and distortion and it is invisible in the printed watermarked image hardcopy. They argued that misalignment and distortion is perceivable only when the image hardcopy is scan using a scanner. Vikas and Barman (2005) did a recent study that quantization index modulation (QIM) is capable to survive print-scan attacks more efficiently. But Vikas and Barman methods have limited embedding capacity which is about 100bits. Furthermore the quality of watermarked image is poor from point of view, and furthermore they are not robust to image cropping. After the introduction of digital holographic watermarking (Takai and Mifune, 2002), these weakness appeared in present print-scan watermarking can be solved. Wang, et al. (2010) developed a digital holograph watermarking scheme where the watermark is a hologram generated using a computer-generated holography (CGH). The discrete cosine transformed (DCT) is chosen as the embedding algorithmic. The watermark is then embeds into DCT transform domain of the host image. Test results have shown that even up to 48.9% image hardcopy is cropped. The watermark is able to detect by the scanner with acceptable quality. Furthermore, the presented work is able to adapt to different type of printers and does not need strict alignment when scanning the watermarked image hardcopy, However, DCT based watermarking is not robustness to image compression,

In contrast, print scanning based color image watermarking usually embed watermark into the chosen (Red, Green, Blue) RGB channel. But the color image is print using the CMYK format. P.Ce (2004) converted the color space of the watermarked images into the CMYK. However this process causes the watermarked image quality to distort as there is color space conversion from RGB to CMYK. Whereas research for digital holographic watermarking have been more focus on improving the watermarking algorithm to improve image quality and robustness. Yet the color space conversion influences is completely neglected. Yong, et al. (2013) proposed a print scan color digital holographic watermarking scheme. The author compared the watermarking performances of embedding the watermark into the RGB and CMYK channel using the (Peak Signal Noise Ratio) PSNR and 2D Normalized Correlated Coefficient. Test results show that watermarking in R, B, C and Y color channel offer the best watermarking performances.

In contrast, holographic watermarking has shown high robustness especially to image cropping and occlusion due to its unique characteristic it processed. Nonetheless, the question remain, what is digital holographic watermarking performances compared against traditional digital image watermarking? Yong, et al. (2012) answered this question by compared digital holographic watermarking with traditional digital image watermarking. A 2D image is used as watermark for traditional image watermarking, whereas for digital holographic watermarking, the same 2D image is converted to digital hologram using computer generated hologram technique. Test results show that the holographic watermarking survives geometric distortion than the traditional one, especially cropping, Gaussian filter, and the Gaussian noise.

The above mentioned holographic watermarking technologies are mainly for the space domain. In the holographic domain, a 2D digital image watermark is added into the holographic content. This is because the recording and experiment setup to capture the optical hologram can be very expensive. Hyun, et al. (2008) wanted to protect the hologram valuable information content by embeds a normal 2D image as watermark hologram. Moreover they have compared the performance of the watermarking scheme by embedded the 2D watermark into the hologram domain and the DCT transformed hologram domain. Both results offer high perceptual quality, however it was the DCT domain scheme that offer higher resistant against image processing attacks. Cheng, et al. (2014) presented a fragile holographic watermarking system for hologram authentication. When the authorized user received the hologram, they are the one responsible to recover its information, which involves numerical reconstruction such as Discrete Fresnel transform. This ensures that the authorized user is the one who performs numerical reconstruction on the holograms with proven integrity. Furthermore, experiment data have shown that this method can detected tampering attempts up to 1/16 pixels. Since off-axis Fresnel hologram is used in this experiment, the security of the system is not safe as key such as the wavelength of the laser and the recording distance can be easily guessed. When someone tried to changes the image content, they can create a new hologram through optical setup after knowing the key parameter.

The mentioned holographic watermarking technologies require the embedding stage and construction/ reconstruction of hologram to be done separately. This process is slow, time consuming and not suitable for real life application that requires high speed transmission. Chen, et al. (2005) proposed a fully optical implement of digital holographic watermarks using modified Mach–Zehnder interferometer. The setup uses two liquid crystal spatial light modulator (SLM), where each of the SLM displayed the watermark pattern and cover image respectively. The watermark detection is done by digitally analyze the correlation signal between the watermark pattern and the watermarked image using a Charge Coupled Device (CCD). However the watermarking performance is heavily dependent on the weighting factor. This property leads to trade-off between watermark perceptual quality and robustness. Lin and Chen (2008) proposed a theoretical model based on statistical approach to design an efficient detector structures which able to determine the optimal condition for watermark performances. The weakness in this scheme is that the watermark robustness not fully tested against attacks.

Li and Kim (2013) proposed another type of watermarking by using optical setup using a modified Mach–Zehnder interferometer architecture. Firstly, the laser is split into two paths, one as reference beam and the other illumined the spatial light modulator (SLM) (contains the watermark image to be hidden) and transmitted as object beam. The reference beam passed two wave plates to provide the phase shifting before directed to the host image. The two beams then meet and interference at the CCD camera. Unlike Chen, et al. (2005) methods where the construction and detection of the watermark is done optically, Li and Kim (2013) experimental setup only deals with image embedding. The watermark recover is done digitally. Nonetheless the use of pure optical system not only increases the security of the watermarking scheme and made use of the advantages of high optical information processing. The significant contribution of the work is that the watermarking and encryption is done optically.

With the widespread application of digital audio, audio watermarking technologies is becoming an important research area (Li and Xue, 2003 and Daqing, et al., 2011). Unlike the human vision system (HVS), the human sense of hearing is very sensitive to slight changes in audio, hence it post a major challenge to audio watermarking technologies. Above all that, digital audio signal transmission suffers all kinds of attacks such as the signal lost during transmission and IP network packet loss. Therefore the audio watermarking technologies need to be strengthened to withstand unintentional/ intentional attacks. Li and Xue (2003) presented an audio watermarking based on digital holographic technique. A digital watermark image to be hidden is firstly converted to hologram watermark using CGH technique. The resultant watermarked audio is robust to low-pass filter, noise addition and compression. To improve the audio holography watermarking, Chen, et al. (2011) used a binary Fourier hologram formed by using the nonlinear amplitude limiting algorithm. In this method, the hologram watermark phase and amplitude information are first recovered as input function and bias function, respectively. To obtain the binary Fourier hologram, the input function and bias function is combined by using the principle of holographic nonlinear limiter (Daqing, et al., 2011). Experiment results show that binary Fourier hologram offer better robustness than normal CGH hologram. Moreover, the lesser amount of data in binary hologram can further improve the audio watermarking performances.

In general, the digital holographic watermarking techniques are generally well studied. This included embedding the hologram into the frequency domain to obtain the highest watermarking performances. However when compare to 2D image watermark, the digital hologram has a large file size as it contains the object information's complex amplitude. Besides that the security of the watermarking schemes is weak, as the optical experiment parameters such as recording distances of the object and wavelength of the laser and be easily deducted through research. Table 2.1 shows the summary of literature survey for digital holographic watermarking

Table 2.1: Summary of literature survey for digital holographic watermarking.

Author	Year	Done	Pros	Cons
Takai and Mifune	2002	First to proposed digital holographic watermarking	• Robust against image cropping and occlusion	• Low pass filter to remove the high frequency components of the host image before the embedding stage.
Chang and Tsan	2005	Embed hologram using DCT	• Remove the need low pass filter requirement. • Improve the perceptual quality.	• Weak against image compression
Chen, et al.	2005	Implement fully optical digital holographic watermarking	• High speed processing/ transmission	• Trade of between watermarking perceptual quality and robustness
Chen, et al.	2008	Design an efficient detector structures	• Optimal condition for best watermark performances	• Watermark Robustness is not fully tested
Osman, et al.	2007	Embed phase shifting hologram using DWT domain and Quantization Index Modulation (QIM).	• Watermark performances can be adjusted by changing the step-size quantizer	• Quantizer needs to be determined experimentally.
Chen, et al.	2008	Design an efficient detector structures	• Optimal condition for best watermark performances	• Watermark Robustness is not fully tested
Hyun-Jun et al.	2008	Embed 2D watermark into hologram domain	• Shows watermark robustness improved using DCT algorithmic	• Weak against image compression
Li and Kim	2009	Improve watermark capacity using combination of DWT and SVD	• Watermark (hologram) file sizes up to 384bit size	• Embed watermark above 384bit may degrade the watermarked image quality.
Wang ,.et al.	2010	Proposed digital holographic watermarking capable to survive print scan	• Survive image cropping up to 48%	• Weak against image compression
Huang	2010	Holographic watermarking based on Ridgelet transform	• Ridgelet transform solve the image edge fuzzy for line singularity cause by DCT watermarking	• Weak against image compression
Yong, et al.	2012	Compared digital holographic	• Holographic watermarking against	• Holographic watermarking weak

		watermarking and traditional digital image watermarking	most image processing attacks	against JPEG compression
Yong,et al.	2013	Color digital holographic watermarking	• Watermarking in R, B, C and Y offers best performances	• Robustness not fully tested.
Li, et al.	2013	Optical watermarking using modified Mach–Zehnder interferometer	• High processing speed	• Watermark recover is done digitally.
Daqing, et al.	2013	Audio watermarking using binary Fourier hologram	• High robust compare with CGH hologram	• Robustness not fully tested
Cheng ,et al.	2014	Fragile digital holographic watermarking	• Able to detect tampering attempt up to 1/16 pixels	• Key parameter can be easily guessed

2.10.3 Secure Holographic Watermarking

The encryption of 2D and 3D information has been well studied to provide copyright protection for digital content such as image, audio, and video (Bender, et al., 1996). On the other hand, progress continues to be made in the development of new optical recording devices and techniques allow researchers to introduce optical encryption techniques to protect the digital content stored in the material. Tajahuerce, et al. (2000) presented a digital phase-shifting interferometry is set up to record the complex amplitude (including the phase and amplitude) of the object. Prior to recording, an encryption is first done by illuminate the complex amplitude of the object through two random phase mask, one in the object plane and one in the Fresnel plane. Optical encryption offers high speed transmission and high security with many degrees of freedom. Nonetheless, once the encrypted data is decrypted, its information is no longer protected from then. Watermarking often complement with encryption technique by embedding an encrypted watermark into the host data in a way that it always remains present against potential attackers.

Réfrégier and Javidi (1995) proposed another optical encryption known as the double random-phase encoding (DRPE). Since its invention, double random-phase encoding (DRPE) has been used widely used in secure holographic watermarking for its high security level. In this method, a 2D watermark image to be hidden $f(x,y)$ is first multiply by a random phase mask $exp[j2\pi p(x,y)]$ in spatial domain before a multiply by another phase mask $exp[j2\pi h(v,w)]$ in Fourier domain:

$$\psi(x,y) = f(x,y)\, exp[j2\pi p(x,y)] \otimes exp[j2\pi h(v,w)]$$

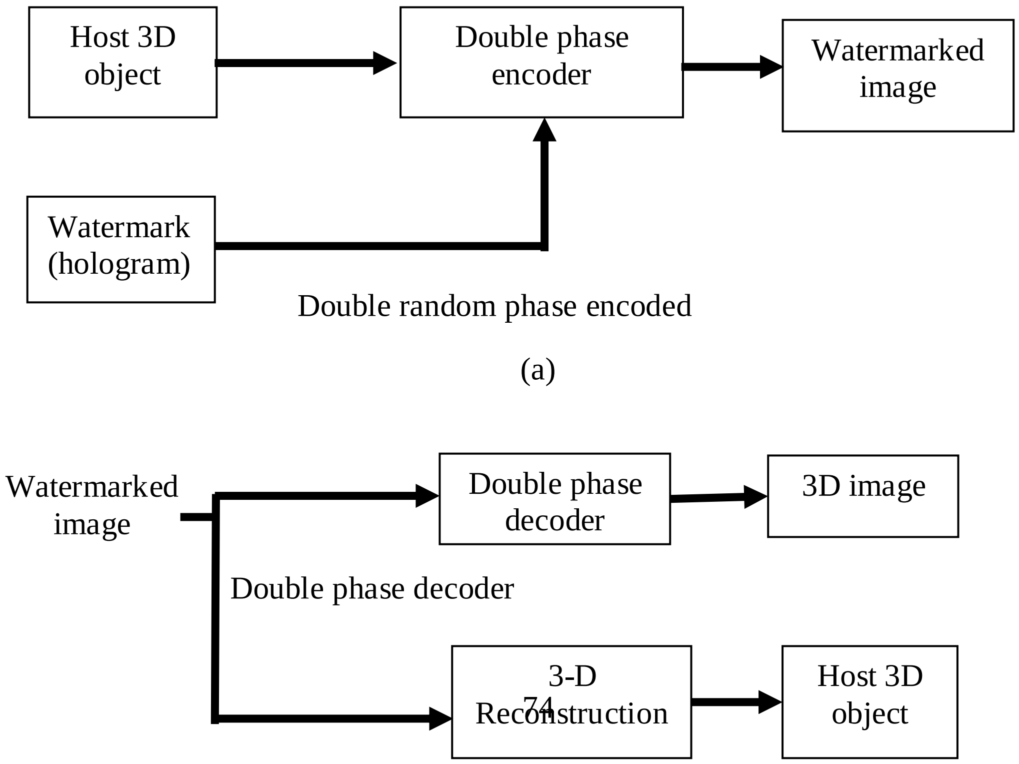
where $p(x,y)$ and $h(v,w)$ are the random phase mask uniformly distributed in [0, 2π] and $\otimes$ stand for convolution. The double encoded hidden image is embedded into the host 3D object by

$$H_w(x,y) = H_c(x,y) + \alpha\psi(x,y)$$

where α is the weighting constant. To recover the watermark image $f(x,y)$. The Fourier transformed watermarked hologram H_w is multiplied with $\exp[-j2\pi b(v,w)]$. The product is then inversed Fourier transforms, and multiplies by $\exp[-j2\pi p(x,y)]$. The recovered watermark object $\hat{f}(x,y)$ have the form:

$$\hat{f}(x,y) = \alpha f(x,y) + IFT\{\tilde{H}_c(v,w)\, exp[-j2\pi b(v,w)]\}\, exp[-j2\pi p(x,y)]$$

After a successful experiment using double random phase encoding to encrypt the 2D watermark image, Kishk and Javidi (2003) proceed to introduce the double random phase encoding (DRPE) algorithmic using digital holographic setup. The use of digital holographic setup and encryption algorithmic not only provides many degrees of security freedom, but it also enables the user to store, transmit and decode the encrypted image digitally. The introduction of encryption algorithmic into digital holographic gives rise to a new field which is called the secure holographic watermarking. First of all the hidden image and the 3D host object is optically recorded by using the phase shifting digital holographic setup. The hidden hologram image is then encrypted by double random phase encoding and embedded as watermark into the 3D host object. The resultant watermarked host image is encrypted again with another double phase encoded to ensure the whiteness of the transmitted hologram. Figure 2.22 shows the schematically diagram of the proposed system.



(a)

(b)

Figure 2.22: Block diagrams of the proposed watermarking system, (a) encoder (b) decoder by Kishk and Javidi (2003)

Experiment result shows that the system is able to recover the hidden hologram after intensive signal processing. For instance, the hidden hologram is recovered as 75% of the watermarked hologram pixels were occluded. The proposed method is reported to very secure due to the multi-key involved. The publication of Kishk and Javidi (2003) created an explosive interest in the field and the development of secure digital holographic watermarking was very intensive. To improve the least errors between the reconstructed host object and the decoded watermark, the optimum weighting factor is investigated (Hyun and Lee, 2005). They derived a formula for the optimum weighting factor which minimized the least errors between the reconstructed host object and the decoded watermark. However, the procedure suggested by Hyun and Lee is considered to be a trade-off between the perceptual quality and robustness in order to balance the reconstruction performance of the host image and watermark image.

Cai, et al. (2004) proposed a secure watermarking scheme where both image encryption and watermarking using three-step phase-shifting interferometry (PSI) method. The three step-phase shifting technique works by changing the phase of the reference waves using a piezoelectric transducer. When the object to be hidden is recorded using PSI, its information is stored into three interferograms with different phase (0, $\pi/2,\pi$) radian. These interferograms can be used as a key to recover the watermark information. To confuse unauthorized receiver, each interferograms are embed into three different or same host image. These watermarked host images are needed to send over to the authorized user via internet. Once obtained the watermarked host image, the authorized user needs to extract and combine the inteferograms followed by numerical simulated in the computer to obtain the true watermark information. The security of the proposed method is safe due to multi-key involved. Figure 2.23 shows the block diagram of the proposed system (Cai, et al. 2004).

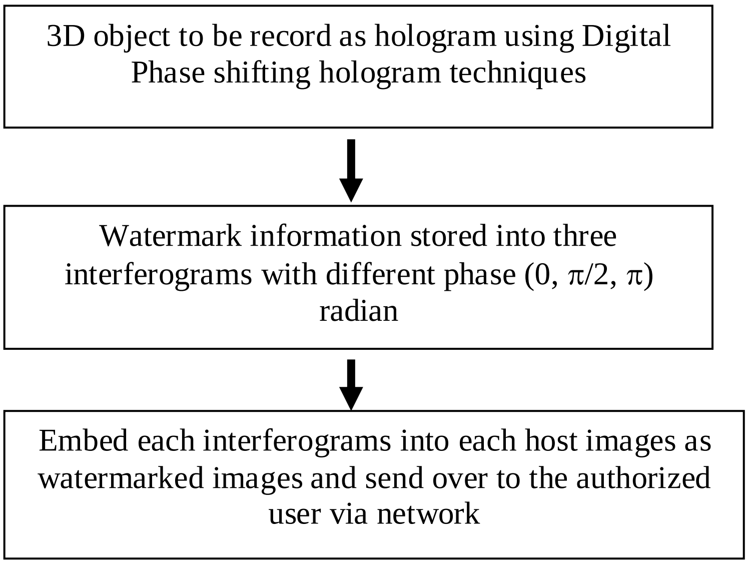

3D object to be record as hologram using Digital Phase shifting hologram techniques
Watermark information stored into three interferograms with different phase (0, π/2, π) radian
Embed each interferograms into each host images as watermarked images and send over to the authorized user via network

Figure 2.23 Block diagram of the proposed watermarking system by Cai, et al. (2004).

As color information is essential for image pattern recognition as it not only beautiful in vision but also they offer more information compared with grayscale image. An extra effort has been made into introduction of color image encryption. Chen and Zhao (2004) proposed an optical color image encryption system by employing three channels each with difference type of lasers (Red, Green and Blue). The three channels are then illuminated the object to be recorded separately before they are encrypted using two random phase masks each placed at each channel to encrypt the red (R), green (G), and blue (B) wavelength separately. The three wavelength image is then combined and recorded using a CCD camera. Naturally, the use of multichannel will increase the security of the system complexity, as the wavelength of the laser and random phase masks are used as the keys. Zhang and Karim (1999) proposed to encrypt a single-channel using a random phase encoding, which obviously has better data transmission efficiency and convenience than the multichannel method. However this method does not deal with digital image watermarking.

Meng, et al. (2007) were the first to present a single-channel color image watermarking. In this method the original watermark object image is first encrypted using the double random phase encoding DRPE. The encrypted image watermark is then split into four interferograms by using four frame phase shifting interferometry (PSI). The complex amplitude of the object is determined by combining the four inteferograms using Equation 2.15. After determine the object complex amplitude, the watermark is then embeds into one chosen channel transformed color host image using the DCT algorithmic. To reduce the cross-talk noise due to interference between host image and watermark image, the neighboring pixel value subtraction algorithm is applied. The two random phase mask and the geometrical parameters such as wavelength and recording distance can be regarded as the key to decrypt the watermark information. But secure holography watermarking based on PSI methods are inconvenient for practical usage, because three to four interferograms are needed to be send over to the authorized user for decryption. The literatures mentioned directly embed hologram as watermark into the host image or a transformed host image (Takai and Mifune, 2003, Chang and Tsan, 2005 and Osman, et al., 2007). This process created cross-talk noise due to the direct embedding the watermark into the host image. In a bid to reduce the cross talk or interference between the watermark image and the host image, Meng, et al. (2007) proposed to combine both the double random phase mask (DRPM) and the random scattering matrix (RSM). In this method, the hologram host image $G(x, y)$ and the watermark $f(x, y)$ is first multiply by a random phase mask $\exp[j2\pi p(x, y)]$ in spatial domain before a multiply by another phase mask $\exp[j2\pi h(v, w)]$ in Fourier domain

$$\psi_G(x, y) = G(x, y)\, exp[\, j2\pi p(x, y)] \otimes exp[\, j2\pi h(v, w)] \quad (2.35)$$

$$\psi_f(x, y) = f(x, y)\, exp[\, j2\pi p(x, y)] \otimes exp[\, j2\pi h(v, w)] \quad (2.36)$$

where $\psi_G(x, y)$ and $\psi_f(x, y)$ are the encrypted host image and watermark image using double random phase encoding. Cai, et al. (2003) proposed the three-frame phase shifting interferometry (PSI) where two set of three holograms of intensities each from encrypted hologram host image $I_1^{(1)}$, $I_2^{(1)}$and $I_3^{(1)}$ and from the encrypted watermark $I_1^{(2)}$,$I_2^{(2)}$, and $I_3^{(2)}$. Instead of embeds the encrypted watermark into the encrypted hologram host image as per normal watermarking process, three composite holograms is formed by using the Random Scattering Matrix (RSM), which randomly distributes the pixels of hologram image intensity $I_j^{(2)}$ and $I_j^{(2)}$ (j = 1,2,3) into larger image I_j without overlapping one and another. Since there is no addition between the two set hologram, there will be no cross-talk between two images. Therefore, each of the hologram images will be recovered perfectly with correct keys. Furthermore the use of the random scattering matrix (RSM) will provide a much higher level of security as it will ensure the whiteness of the transmitted data. But three composite holograms together are needed to transfer over to the authorized user for decryption. Hence this technology is limited only to those with adequate bandwidth hardware.

Nishchal, et al. (2010), recently proposed a watermarking scheme which combine the Double Random Phase Encoding (DRPE) and Fractional Fourier transform domain (FRT). The FRT provides extra degree of freedom and it comes at no addition cost in digital computation/ optical implementation. In this method, the watermark $f(x , y)$ is encrypted using double random phase in fractional Fourier domain with an order parameter A two dimensional function is given as: $\psi(x, y) = f(x, y) exp[j2\pi p(x, y)]$ with an order of $(\sigma_1 = p_1 \pi/2)$ is given by $p(\xi , \eta)$.

$$p(\xi, \eta) = K\iint \psi(x, y) exp\left(\frac{j\pi(x^2 + y^2 + \xi^2 + \eta^2)}{tan\ \sigma_1} - j2\pi \frac{xy\xi\eta}{sin\ \sigma_1} \right)$$

The (x , y) and (ξ , η) represent the space and fractional domain coordinates, respectively. The parameter K is given as

$$K = \frac{exp\left[- j(\frac{1}{4} \pi \ sgn(sin \ \sigma) - \frac{1}{2} \sigma_1 \right]}{\left| sin \ \sigma_1 \right|^{1/2}}$$

The function $p(\xi , \eta)$ is multiplied by another random phase mask, with an order of $(\sigma_2 = p_2 \pi/2)$

$$q(\rho, \sigma) = K \iint p(\xi, \eta) \exp\left(j2\pi p(x, y) \right) \exp\left(\frac{j\pi(x^2 + y^2 + \xi^2 + \eta^2)}{\tan \sigma_2} - j2\pi \frac{xy\xi\eta}{\sin \sigma_2} \right)$$

The $q(p , \sigma)$ is the encrypted image of the watermark $f(x , y)$ .The encrypted watermark is embedded into the host image given by

$$H_w(\rho, \sigma) = H_c(\rho, \sigma) + \alpha q(\rho, \sigma)$$

Since the order σ of transform can be chosen between 0 and 1 freely, it can be considered as an extra key to protect the safety of the embedded watermark information. .Li (2014) proposed a particle swarm optimization to determine the optimum condition for secure holographic watermarking using double random phase encoding (DRPE) and three- step phase shirting interferometry (PSI). Particle swarm optimization is an intelligent system used to determine the best optimization to offer watermarking both imperceptibility and the robustness. In this method, a particle, which represents the quantization step of watermark is determined and used to find suitable quantization step for embedding watermark. The proposed watermarking scheme offers satisfactory performance against different kind of image common image processing especially against the filtering, noise attack and JPEG compression. Besides that with the huge key transform of the encrypted watermark, the security strength of the scheme is significantly increased. Yet the keys data quantity is very large and is needed to transfer over the internet for the user to recover the watermark information.

While some holography watermarking technology offers image security especially for those based on Optical Fresnel hologram as watermark image. These technologies use the recording distances and wavelength of the laser as the encrypting keys and governed only by the authorized user. Yet, both keys can be easily deduced though research. In an attempt to reduce the key data quantity and yet offers high security, a single phase encryption mask is used (Huang et al., 2006). Just before the hologram (interference pattern) was formed, a phase encryption mask is illuminated with the reference wave $R(x, y)$ as given below

$$R(x, y) = exp[j\phi_e(m, n)]$$

where $\phi_e(m, n)$ is the phase encryption mask. To numerical reconstructed the hologram information the phase encryption mask together with recording distance and the wavelength of the laser is needed. For unauthorized user without the correct keys, they are unable to retrieve the watermark image successfully. The use of phase encryption mask reduces the key data quantity but the robustness of this method is not fully tested. This is because if the watermark robustness is weak, the watermark information will be severely deteriorate and unable to be detected after severe image processing. Therefore, the security of the watermark has no meaning as its watermark information is destroyed.

Giuseppe and Michele (2011) proposed a watermarking scheme where the computer generated hologram (CGH) is encrypted using an asymmetric cryptographic algorithm known as Rivest-Shamir-Adleman (RSA) algorithm. In asymmetric cryptography, the key used for image encryption is different from the key used for decryption. In other words, each authorized user has two different type keys namely: a Public Key (PK), which is known to everyone and a Private Key (SK), which is governed only by the authorized user. Furthermore RSA algorithmic requires both the public and private keys for encryption and decryption. The private key is used to decrypt message that has been encrypted with public key. Thus, if the public key is exposed, the message cannot be recovered. But an authorized user is able to recover the message using the private key. Furthermore the proposed watermarking scheme is used for digital image authentication, thus if there is a slight modification to the work, the watermark is destroyed. The use of RSA algorithmic offer high security and lesser key data quantity compared to double random phase encoding (DRPE) and three-step phase shifting interferometry (PSI). Although RSA does offer high security, the algorithmic involved large number of modular exponentiation operations which in turn consume high computational complexities. Furthermore optical encryption still offer higher degree of security freedom compared with RSA algorithm.

2.11 Summary

Holographic watermarking is a challenging task with high demand for real life application. For holographic watermarking, there are two groups of researcher focusing to improve the holographic watermarking performances and security, but rarely on both. Watermarking using digital hologram offers high resistant especially to attacks like image cropping and occlusion. However compared with two-Dimensional image, the optical hologram image has a large file sizes as it contains the object complex amplitude. Furthermore the security of the watermarking system is weak as the optical parameter such as (Wavelength of laser and recording distance between the object and (CCD) can be easily deducted. Hence, the first part of the project is to reduce hologram total file size. This is done by using parts (100%, 90%, 80%, 70%, 60%) of the hologram file size as watermark image and embed into the Baboon host image using the SVD algorithmic.

On the other hand, secure holography watermarking technologies have proved its security can be enhanced by increasing the number of keys. The Double Random Phase Encoding (DRPE), three step phase shifting interferometry (PSI) and Fractional Fourier transform (FRT) are some of the popular encryption choice for secure holographic watermarking. This is because they offer multiple keys during encryption and it ensures the whiteness of the transmitted watermark. However the holographic technologies are still limited by the issue of key management and transmission. This is because large quantity of the key is needed to transmit to the authorized user to recover the watermark information. For example three step phase shifting interferometry (PSI) requires to transmit three keys to the authorized user to recover the watermark image. Therefore in the second part of the project, a secure watermarking scheme based on Digital Holographic Interferometry (DHI) technique is presented here. This method made use of double exposure technique which captured two different holograms of an object in different states. The resultant complex amplitude, due to the superposition of the two holograms; contains the information of an object deformation appeared in the form of fringes pattern. The holographic interferometry watermarking scheme uses two holograms, one used as watermark and the other serves as a key. Since the key is a hologram, one can reduce the sizes of the key using part of the holograms. One of the criteria for secure watermarking scheme is robustness. Therefore the experiments are mainly focused on the robustness of the proposed scheme. Moreover the proposed scheme offers a second layer of security as the recovery of watermark interference pattern would require the knowledge of key. Table 2.2 shows the literature survey for digital holographic watermarking.

Table 2.2: Summary of literature survey for secure digital holographic watermarking

Author	Year	Done	Pros	Cons
Kishk and Javidi	1997	Proposed DRPE based watermarking	• High security due to multiple keys involved during encryption	• Multiple keys need to be send over to the user
Kishk and Javidi	2003	Proposed secure holography watermarking		
Cai, et al.	2003	Three-step Phase shifting hologram	• Watermark information split into three inteferogram.	• Multiple keys need to be sent over to the user.
Chen and Zhao	2004	Three-channel color image watermarking based on DRPE	• High security due to multiple keys involved during encryption	• Multiple keys need to be send over to the user
Hyun and Lee	2005	Optimize DRPE performances	• Watermarking offers both quality and robustness.	• Tradeoff between perceptual quality and robustness.
Huang, et al.	2006	Watermark encrypt using single phase mask	• Less complex and reduce the key data quantity.	• Robustness not fully tested.
Meng, et al.	2007	Single channel Color image watermarking using DRPE combined with neighboring pixel value subtraction to reduce cross-talk noise	• Transmission of single channel color image encryption is much efficient than multichannel encryption	• Multiple keys need to be send over to the user
Meng, et al.	2007	Holographic Watermarking based on DRPE and RSM	• Eliminated cross talk noise effect. Since no interference between host image and wateramark	• Multiple keys need to be send over to the user
Nishchal, et al.	2010	Combine FRT and DRPE	• High security due to multiple keys involved during encryption.	• Multiple keys need to be send over to the user
Giuseppe and Michele	2010	RSA based holographic watermarking	• High security with lesser key file size compare with optical encryption	• Optical encryption offers key with high degree freedom
Li	2014	Intelligent system to detect Optimal condition for secure holographic based on DRPE and PSI	• High perceptual quality and robustness using particle swarm theory	• Multiple keys need to be send over to the user.

CHAPTER 3

METHODLOGY

3.1 Introduction

There are three experiments in this project:

1) To investigate the embedding domain that offers the best perceptual quality for digital holographic watermarking
2) Embedding a portion of digital hologram as watermark to reduce the watermark file size and investigate the performances in terms of perceptual quality.
3) Develop a secure watermarking scheme based on the digital holographic interferometry (DHI) technique, where two holograms are used, one is embedded as watermark and the other is used as the key.

3.2 To investigate which embedding domain offers the best perceptual quality for digital holographic watermarking.

There are few embedding algorithm mentioned back in chapter 2.6, In order to determine which domain offers the best perceptual quality , 100%

portion watermark (hologram) is embed into Baboon image using LSB, DCT, DWT and SVD domains. Experimental results in chapter 4.2 have shown that SVD domain offers best perceptual quality. Therefore, in this project SVD domain will be used

3.3 Watermark Embedding using Portion of Hologram

In this experiment, the watermark is a pyramid-shaped object digital hologram (as shown in Fig. 2.15 (b)). The proposed watermarking scheme, as shown in Figure 3.1, is divided into two major steps.

Step-1: Embedding the watermark into the host mage

In this first step to transform the 512 × 512 grayscale Baboon host image (as shown in Fig. 2.16 (a) into transform domain and then. After that, the different portion of the watermark (hologram) is embedded into the host image diagonal (S) matrix.

Step-2: Robustness testing of the watermark scheme

In this second step to attack the watermarked image with image processing attacks such as Gaussian Filter, Gaussian Noise, JPEG Compression, Image cropping, Occlusion and Rotation. The robustness of the watermarking system is determined by comparing the recovered watermark and the original watermark using the Normalized Correlated Coefficient (CC). The watermark is recovered using the Equation 2.30.

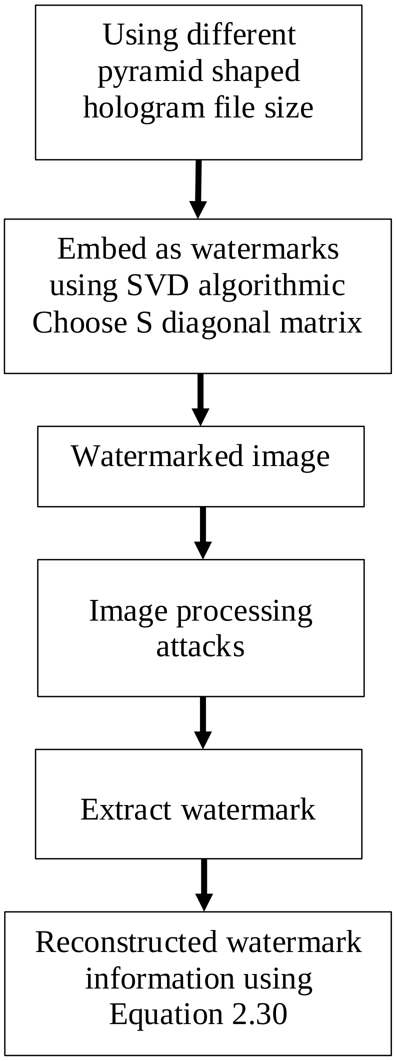

Using different pyramid shaped hologram file size
Embed as watermarks using SVD algorithmic Choose S diagonal matrix
Watermarked image
Image processing attacks
Extract watermark
Reconstructed watermark information using Equation 2.30

Figure 3.1: Flowchart of the watermarking scheme using different portion of hologram as watermark.

Figure 3.2 shows the flowchart of the intensity reconstruction of the watermark (hologram) recovered using SVD method. The numerical reconstruction is written in Matlab2006 programming language. Basically the program consists of three major steps. First the watermark is recovered using the SVD transformation. The second step is to read the amplitude transmittances of and calculate the complex amplitude $\Gamma(m,n)$ of the hologram by using the 2-dimensional Discrete Fourier Transform. Lastly, the intensity of the watermark information is calculated and rescale the watermark into grayscale image.

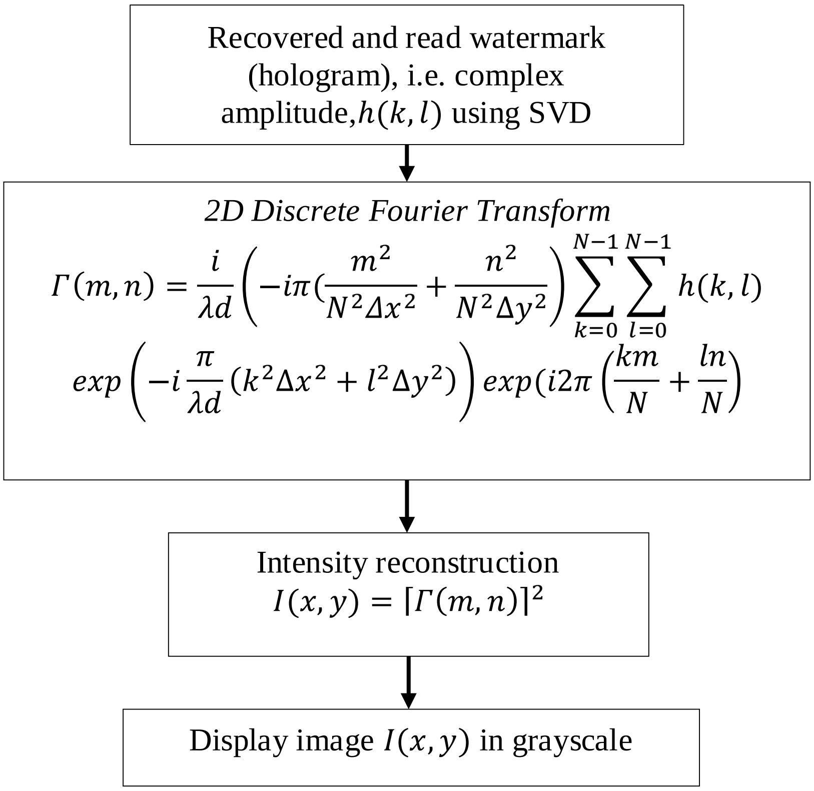

Recovered and read watermark (hologram), i.e. complex amplitude,$h(k,l)$ using SVD
2D Discrete Fourier Transform
$\Gamma(m,n)=\frac{i}{\lambda d}\left(-i\pi(\frac{m^2}{N^2\Delta x^2}+\frac{n^2}{N^2\Delta y^2}\right)\sum_{k=0}^{N-1}\sum_{l=0}^{N-1}h(k,l)$
$exp\left(-i\frac{\pi}{\lambda d}(k^2\Delta x^2+l^2\Delta y^2)\right)exp(i2\pi\left(\frac{km}{N}+\frac{ln}{N}\right)$
Intensity reconstruction
$I(x,y)=\lceil\Gamma(m,n)\rceil^2$
Display image $I(x,y)$ in grayscale

Figure 3.2: Flowchart of the intensity reconstruction of the watermark (hologram) recovered using SVD method

3.4 To develop secure digital holographic watermarking using Digital Holographic Interferometry

Digital holographic watermarking using digital holographic interferometry required two holograms, one as watermark, and the other as key. In order to create two holograms, a cantilever beam is used as object.

This experiment is divided into three sections: recording procedure, embedding process, and recover process using SVD domain

3.4.1 Recording Procedure

Figure 3.3 shows the experimental set-up for implementation of digital holographic interferometry. The experiment is carried out with a 30-mW Single Frequency Diode Pumped Solid state. The laser light is divided into two paths by a beam splitter as into reference and an object illuminating beam. The object in this experiment is a cantilever beam, where its base is clamped and its free end is loaded. The dimension of the cantilever beam was $1cm \times 1cm$ and placed $0.30m$ from CMOS camera. A micrometer screw applied the load toward the direction of the CMOS. In digital holographic interferometry, instead of single hologram, two holograms are captured. First of all, the undisturbed state of the cantilever beam is recorded, before a second hologram is captured from now disturbed beam. After that, both the object waves and reference waves are combined using the beam splitter and the resulted holograms are stored separately in the computer for processing.

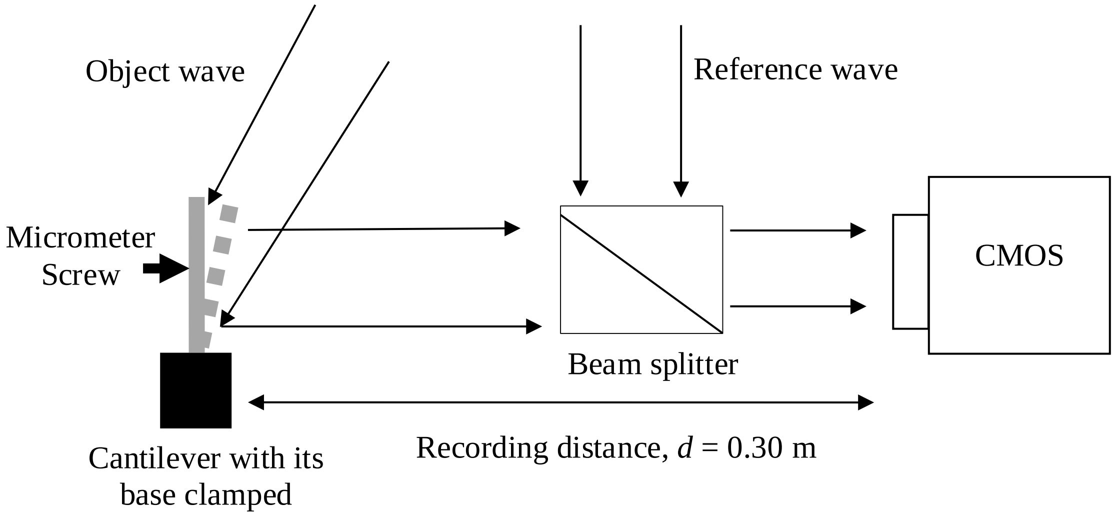

Object wave
Reference wave
Micrometer Screw
CMOS
Beam splitter
Cantilever with its base clamped
Recording distance, *d* = 0.30 m

Figure 3.3 Experimental setup for digital recording of an off-axis cantilever hologram.

The CMOS used throughout the experiment is the Compact USB 2.0 CMOS Cameras. The CMOS camera specification are given in Table 3.1

Table 3.1 Specification of the Compact USB 2.0 CMOS Camera system.

Resolution	1280 x 1024 pixels
Sensing area	1/3 -inch size
Pixel Size	$3.6\ \mu m \times 3.6\ \mu m$

Table 3.2 shows the specification for optical component used in the experiment setup

Table 3.2 Specification for optical components.

Single Frequency Diode Pumped Solid State Laser	Wavelength: 532nm
Spatial Filter system	20x objective lens + 15µm mounted pinhole
Visible non-polarizing cube beam splitter	Antireflection coating: 400-700nm
Broadband dielectric mirror	Antireflection coating: 400-750nm, Surface Flatness: λ/10

3.4.2 Embedding the watermark using SVD domain

To implement this project, the undisturbed hologram is used as the watermark and the disturbed hologram is used as key. The proposed watermarking scheme is divided into three major steps. The first step is to applied SVD transform using Equation 2.11 on the host image before embedded the watermark into its diagonal (S) matrix. The second step is to attack the watermarked image with image processing attacks. There are two ways to recover the cantilever watermark information, firstly to cantilever watermark information using the optical parameters (wavelength of the laser & recording distance). Secondly, to recover the interference pattern of the deformed cantilever, the key (disturbed hologram) and optical parameters are needed. Figure 3.4 illustrate the flowchart of the proposed watermarking scheme.

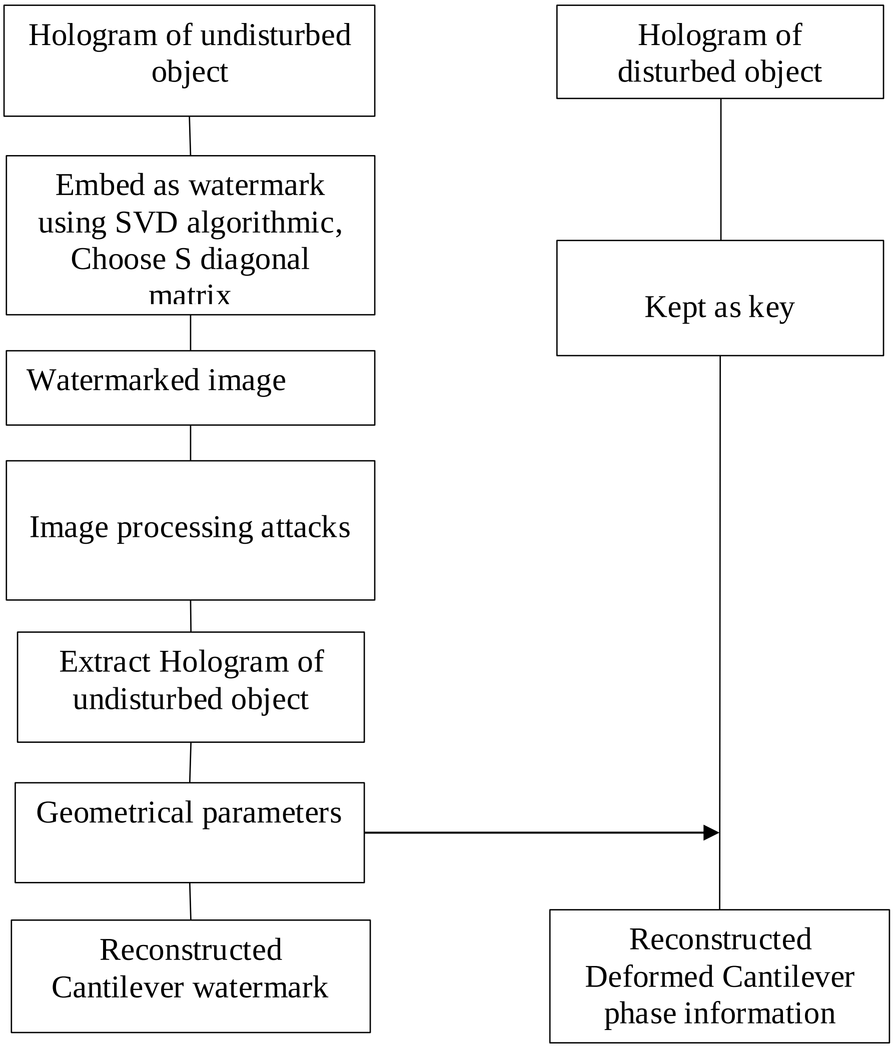

Hologram of undisturbed object
Embed as watermark using SVD algorithmic, Choose S diagonal matrix
Watermarked image
Image processing attacks
Extract Hologram of undisturbed object
Geometrical parameters
Reconstructed Cantilever watermark
Hologram of disturbed object
Kept as key
Reconstructed Deformed Cantilever phase information

Figure 3.4: Flowchart of the watermarking scheme based on digital holographic interferometry and SVD.

3.4.2 Recover the watermark using SVD domain

To process the digitally stored hologram in digital holographic interferometry, each of the object state is reconstructed separately and the phases are calculated. The interference pattern is then determined. Figure 3.5 shows the detailed numerical reconstruction flow chart of interference pattern. It consisted of four major steps. First the, the watermark from the watermarked diagonal matrix is recovered using the SVD transformation. The second step is to read the amplitude transmittances of both the watermark and the key. The next step is to calculate the complex amplitude $\Gamma(m, n)$ of each hologram by using the 2-dimensional Discrete Fourier Transform. Lastly, the interference pattern $\Delta\varphi(\xi, \eta)$ of the watermark information is calculated and rescale the into grayscale image. Note that, the watermark information (cantilever hologram) can be easily recovered using Equation 2.29. However the interference interference pattern $\Delta\varphi(\xi, \eta)$ or watermark interference pattern can only be recovered using the key complex amplitude, $h_2 = (k, l)$ using Equation 2.32. Thus the proposed method offers a second layer of security,

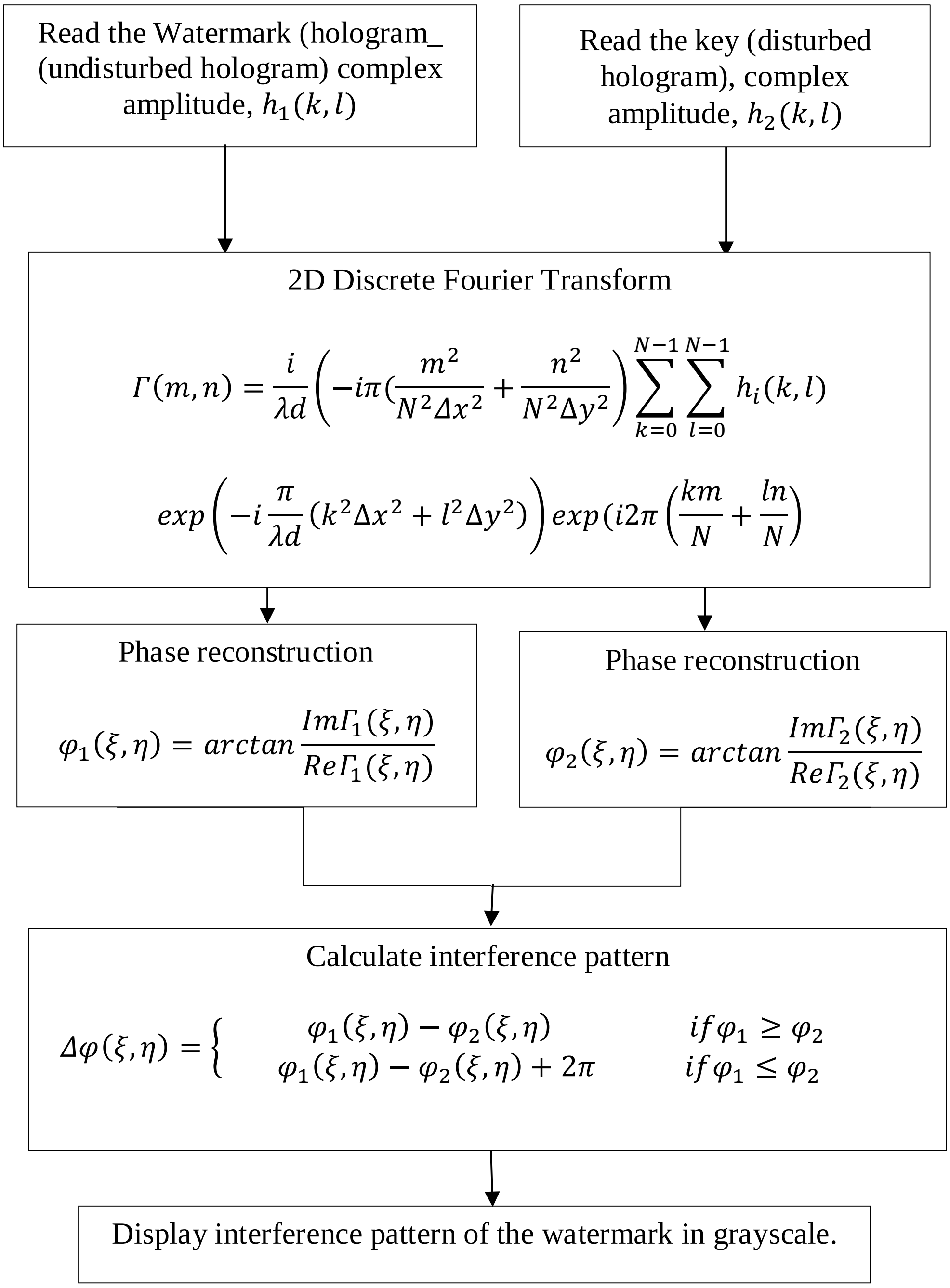

Read the Watermark (hologram_ (undisturbed hologram) complex amplitude, $h_1(k,l)$
Read the key (disturbed hologram), complex amplitude, $h_2(k,l)$
2D Discrete Fourier Transform
$\Gamma(m,n) = \frac{i}{\lambda d}\left(-i\pi(\frac{m^2}{N^2\Delta x^2} + \frac{n^2}{N^2\Delta y^2}\right)\sum_{k=0}^{N-1}\sum_{l=0}^{N-1} h_i(k,l)$
$exp\left(-i\frac{\pi}{\lambda d}(k^2\Delta x^2 + l^2\Delta y^2)\right)exp(i2\pi\left(\frac{km}{N} + \frac{ln}{N}\right)$
Phase reconstruction
$\varphi_1(\xi,\eta) = arctan\frac{Im\Gamma_1(\xi,\eta)}{Re\Gamma_1(\xi,\eta)}$
Phase reconstruction
$\varphi_2(\xi,\eta) = arctan\frac{Im\Gamma_2(\xi,\eta)}{Re\Gamma_2(\xi,\eta)}$
Calculate interference pattern
$\Delta\varphi(\xi,\eta) = \begin{cases} \varphi_1(\xi,\eta) - \varphi_2(\xi,\eta) & if\,\varphi_1 \geq \varphi_2 \\ \varphi_1(\xi,\eta) - \varphi_2(\xi,\eta) + 2\pi & if\,\varphi_1 \leq \varphi_2 \end{cases}$
Display interference pattern of the watermark in grayscale.

Figure 3.5: **Flowchart of the interference pattern reconstruction of the watermark (hologram) recovered using SVD method.**

CHAPTER 4

DIGITAL HOLORAPHIC WATERMARKING USING PORTION OF HOLOGRAM AS WATERMARK

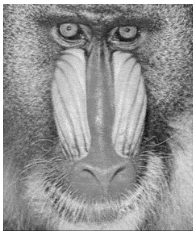
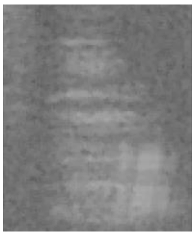
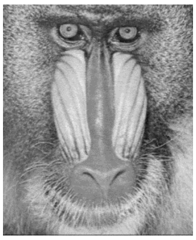
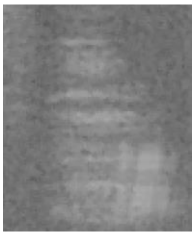
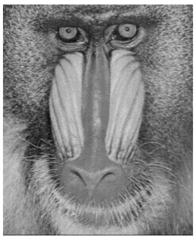
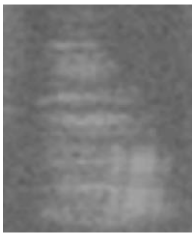
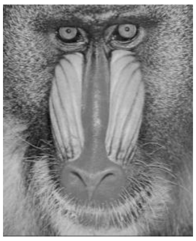
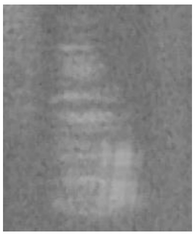
4.1 Introduction

In this chapter, the best embedding algorithmic that offer highest perceptual quality is first investigated. Secondly, digital hologram is used as watermark because it processed certain unique characteristics which every part of the hologram contains the entire information of an object (Schnars and Juptner, 2002). This is demonstrated in Figure 4.1, where only 90%, 80%, 70%, 60% and 50% of the hologram are used for reconstruction.

4.2 To determine the best embedding domain

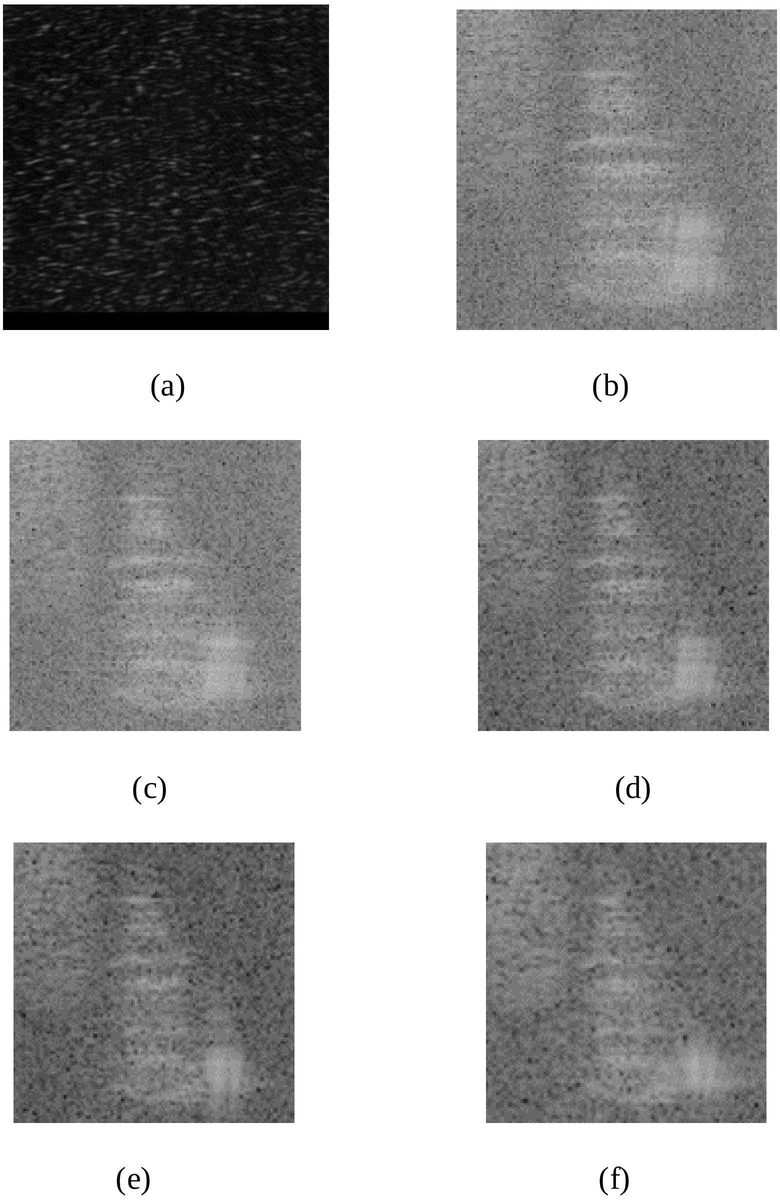
Table 4.1 shows a simple experiment using the LSB, DCT, DWT and SVD algorithm with weighing factor $\alpha = 0.59$**.** The weighting factor value $\alpha = 0.59$, is chosen because it offers the best perceptual quality and robustness as demonstrated by Hyun and Lee (2005). From the table, SVD domain offers the best watermarked image quality compared to LSB (9.48%), DCT (10.4%) and DWT (8.67%).

Table 4.1: The watermarked image and recovered watermark perceptual quality using different embedding algorithms.

Embedding algorithm	Watermarked Image	PSNR (dB)	Percentage different (%)	Recovered watermark	Correlated coefficient (CC)
LSB		43.13	0		0.953
DCT		42.76	-0.85		0.964
DWT		43.45	+0.74		0.971
SVD		47.22	+9.48		0.996

4.3 Proposed Watermarking Scheme using Different Portion of hologram

Before embedding portion of watermark (hologram) in the host image, the hologram unique characteristic is studied first. Figure 4.1shows hologram information can be reconstructed using 90%, 80%, 70%, 60% and 50% portion of the hologram. Due to image resizing and the low resolution in CMOS camera, the reconstructed image has poor quality.



(a) (b) (c) (d) (e) (f)

Figure 4.1: (a) Digital hologram of a pyramid-shaped object. Real image of the reconstructed hologram using (b) 90% (c) 80% (d) 70%, (e) 60% and (f) 50% portion of the hologram.

The unique properties of the hologram allow one to recover object information by using a portion of its data, which consequently reduced the hologram file sizes. Therefore, in this watermarking scheme, a portion of the hologram is embedded as watermark into the host image in the transform domain. The SVD domain is chosen for embedding algorithmic because it best quality among the transform domains algorithmic.

Table 4.2 shows the correlated coefficient values for each different portion of the total hologram used to reconstruct the real image. The real image holograms quality significantly reduced when compared with 100% hologram. Otherwise the hologram image quality it is still within the acceptable range until 60% of the total hologram file size is used. Most importantly the file size of the reconstructed hologram image is greatly reduced from 259 KB to 92.5 KB.

Table 4.2: The correlated coefficient (CC) values for each different portion of the hologram used to reconstruct the real image.

Real image hologram reconstructed by using portion (%) of the total hologram	100	90	80	70	60	50
Correlated Coefficient (CC)	1.000	0.906	0.868	0.815	0.753	0.677
Digital Hologram File Size (KB)	259	209	164	126	92.5	65

Table 4.3 and Table 4.4 represent the results of embedding different sizes of watermarks hologram in a host image using SVD transform. The Peak signal to noise ratio (PSNR) is used to calculate the watermarked image perceptual quality. Note that watermarked image quality increases by using smaller portion of the hologram file size. However, there is a trade-off between watermarked image quality and watermark file size. In other words, the watermark quality is sacrificed to increase the watermarking performances.

Table 4.3: Comparison when embedding watermark using 100% to 80% portion of the hologram into the Baboon image.

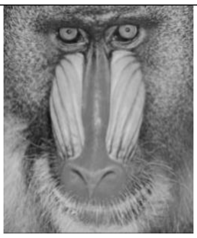
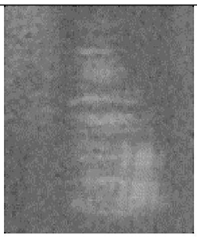
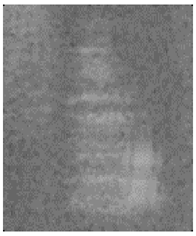
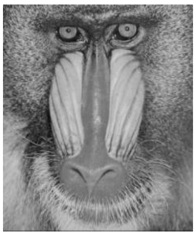
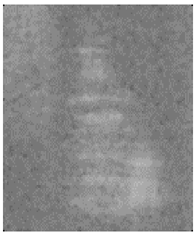
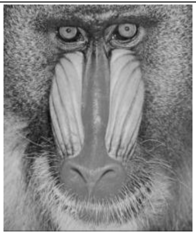
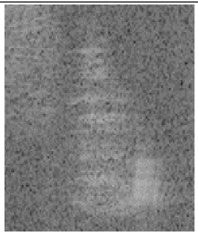
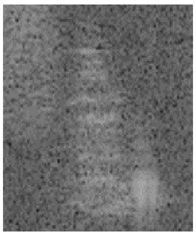
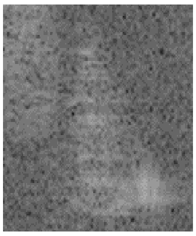
Portion (%) of the total hologram as watermark	Watermarked Image	PSNR (dB)	Percentage differences (%)	Recovered watermark	CC
100		48.22	0		0.987
90		48.30	+ 0.20		0.989
80		48.33	+ 0.27		0.993

Table 4.4: Comparison when embedding watermark using 70% to 50% portion of hologram into the Baboon image.

Portion (%) of the total hologram as watermark	Watermarked Image	PSNR (dB)	Percentage difference (%)	Recovered watermark	CC
70		48.39	+ 0.39		0.994
60		48.51	+ 0.64		0.995
50		48.86	+ 1.36		0.998

4.3 Robustness Testing

In this chapter the watermark robustness are tested using 100% to 60% of the hologram total file sizes. Note that 50% of hologram total file size is not used as its image quality is not within the Correlation Coefficient acceptable range. The watermarked image is tested against, noise addition, linear filtering, JPEG Compression, image cropping, Occlusion and Rotation.

4.3.1 Attack by Noise Addition

Figure 4.2 shows the Gaussian noise attacks on the proposed scheme. Although the robustness against noise increase by using smaller file sizes, the scheme is unable to withstand both noise. As a result, the reconstructed watermark is unrecognizable.

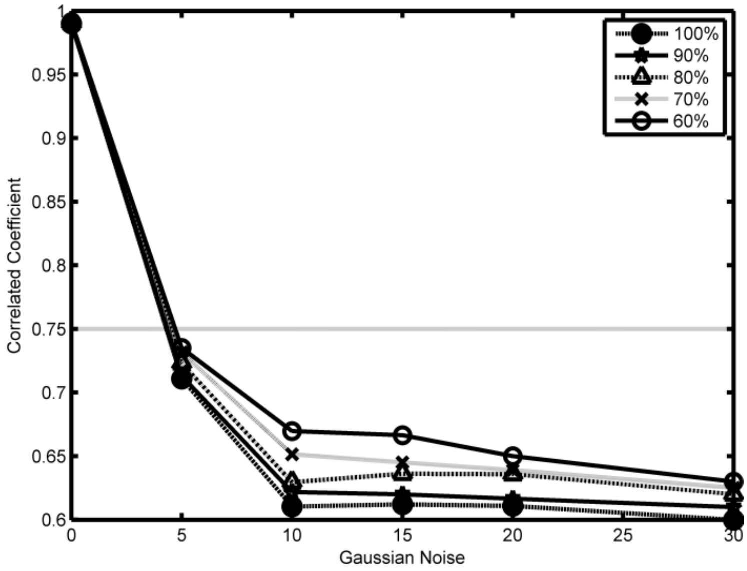


Figure 4.2: Correlation between original watermark and recovered watermark after Gaussian noise attack.

4.3.2 Attack by Linear Filtering

Figure 4.3 and Table 4.5 illustrate the watermark robustness against linear filtering attack. From the experimental results, it is obvious that the robustness against filters increases with smaller portion of watermark. However, the watermarking scheme is weak against mean filtering and median filtering.

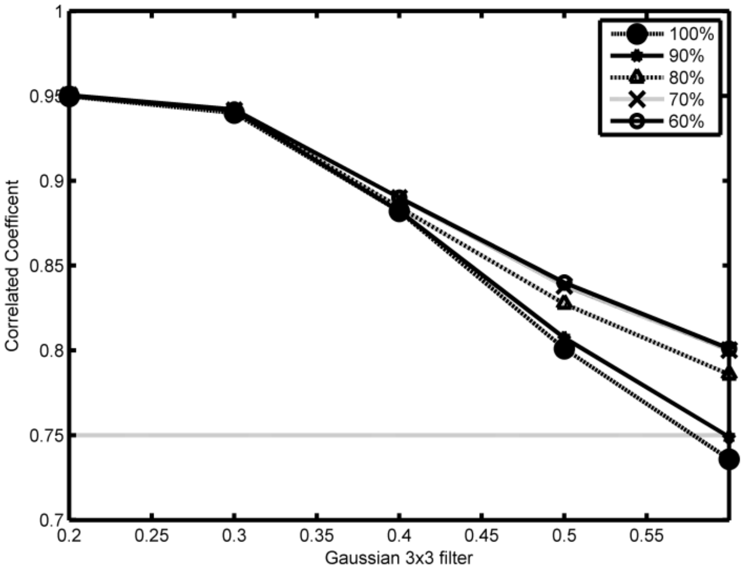


Figure 4.3: Correlation between original watermark and recovered watermark after Gaussian filter.

Table 4.5 Correlation between original watermark and recovered watermark after Mean and Median filtering.

Portion (%) of the total hologram as watermark	Correlated Coefficient (CC) Mean (3x3)	Median (3x3)
100	0.597	0.6258
90	0.599	0.6455
80	0.610	0.6476
70	0.630	0.6532
60	0.633	0.6601

4.3.3 Attack by JPEG Compression

Figure 4.4 shows the watermarked image robustness against JPEG compression. The experiment results show that the resistant against JPEG can be adjusted by changing the watermark total file sizes.

From the results, it obvious that the proposed method is unable to resist the JPEG compression with quality factor less than 50. Otherwise, the proposed method is still robust against JPEG compression unless the compression is high enough to destroy the watermark information. Reasonably, 60% watermark file sizes would be the best choice for robustness against JPEG compression.

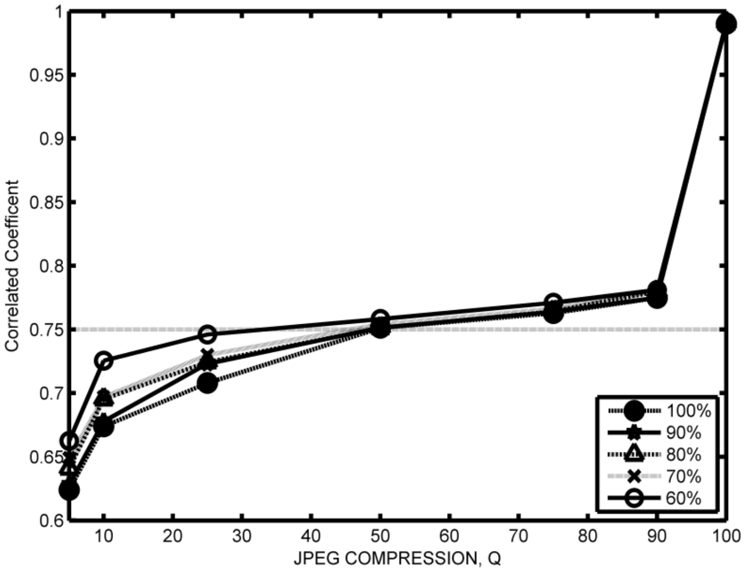


Figure 4.4 Correlation between original watermark and recovered watermark after JPEG compression.

4.3.4 Attacks of Image Cropping, Occasion and Rotation

Figure 4.5 and Figure 4.6 show the recovered watermark image after image cropping. Both experiment results show that the resistant to image cropping and occlusion can be increase with smaller watermark file sizes. Table 4.6 shows the correlated coefficient of the recovered watermark with embedded watermark. Similarly there is an improved on the robustness against rotation as the watermark file size decreases.

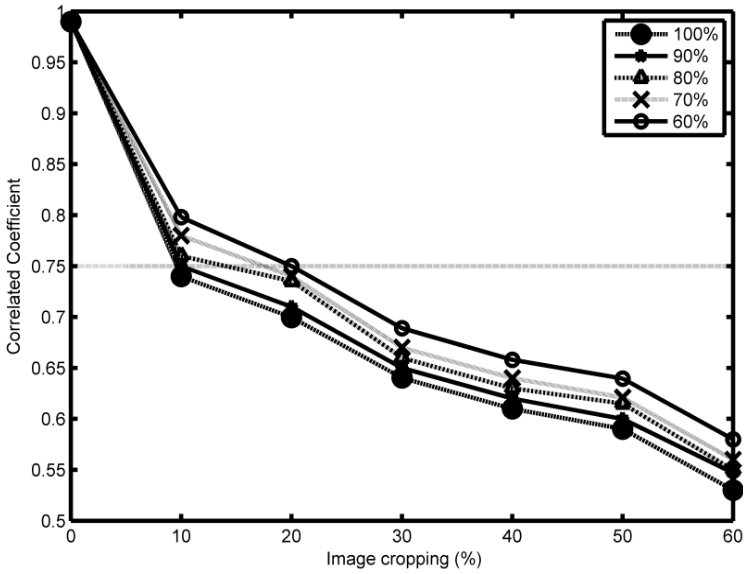


Figure 4.5 Correlation between original watermark and recovered watermark after image cropping.

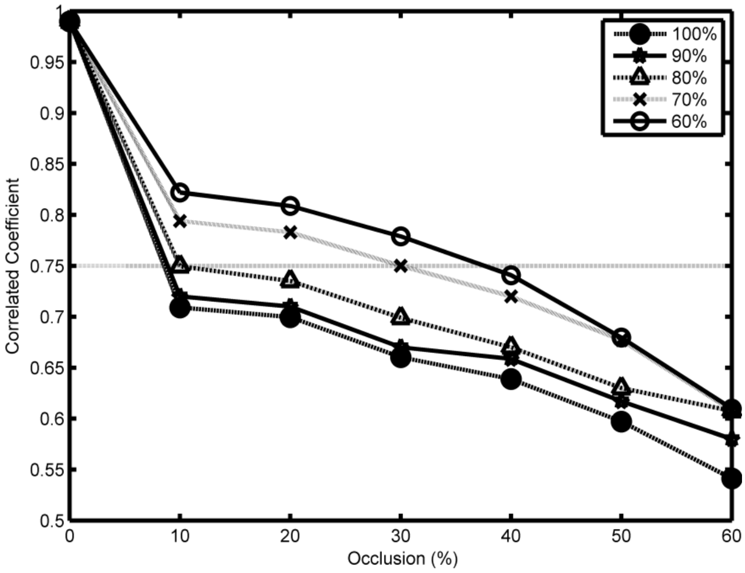


Figure 4.6 Correlation between original watermark and recovered watermark after Occlusion

Table 4.6 Correlation between original watermark and recovered watermark after rotation attack.

Portion (%) of the total hologram as watermark	Correlated Coefficient (CC)	
	-5° Rotation	+5° Rotation
100	0.696	0.699
90	0.713	0.721
80	0.762	0.768
70	0.777	0.783
60	0.806	0.812

4.3 Conclusion

In the first experiment, the SVD domain offers the best perceptual quality 47.22 dB (+ 9.48% improvement) compared to LSB, DCT and DWT. On the other hand, the watermark size can be reduced by taking smaller portion of the hologram. For instance, watermark size is reduced from 259 KB to 92.5 KB when using 60% portion of hologram. Furthermore the robustness of the watermarked baboon image improved when smaller watermark (hologram) size is used.

CHAPTER 5

DIGITAL HOLOGRAPHC WATERMARKING BASED ON DIGITAL HOLOGRAPHIC INTERFEROMETRY TECHNIQUE

5.1 Introduction

In this chapter, a secure digital watermarking based on holographic interferometry is presented. In holographic interferometry, two holograms at two different states are captured with double exposure technique. One of the holograms is used as watermark and the other hologram as key. Since the key is a hologram, as such one can reduce the key file size by using only portion of the hologram as demonstrated in Chapter 4.

As mentioned in Chapter 3.7, the watermark intensity information (cantilever hologram) can be easily recovered using Equation 2.16. However, the watermark interference pattern, $\Delta\varphi(\xi,\eta))$ can only be recovered using the key $h_2 = (k, l)$. Thus the proposed method offers an additional layer of security.

For the experiment to work, the undisturbed hologram is used as watermark; while the disturbed hologram is used as key. Figure 5.1(a) and Figure 5.1(b) show the digital hologram of the undisturbed (watermark) and disturbed state (key). Figure 5.2(a) shows the baboon host image. Figure 5.2(b) shows the recovered watermark information (cantilever hologram using the optical parameters (wavelength of laser and recording distance from the object to the camera). Figure 5.3(a) and Figure 5.3(b) show the reconstructed watermark interference pattern using the key in phase contrast image and amplitude contrast image. In this case, the watermark information reconstructed in phase contrast image is much detail than its amplitude contrast image. Therefore, only the phase contrast image is used for authentication. Figure 5.4 shows the reconstructed watermark interference pattern using the wrong key.

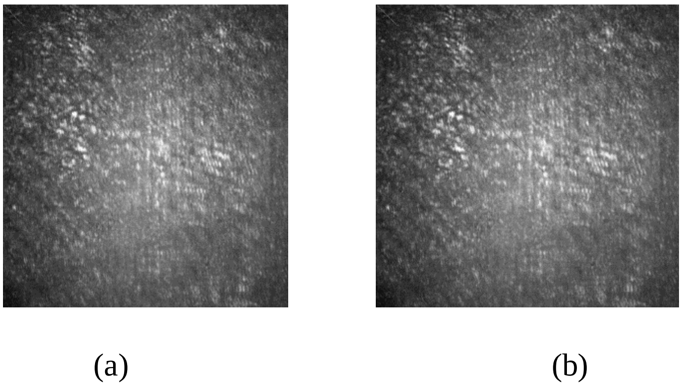


Figure 5.1: Digital hologram of (a) undisturbed state (used as watermark) (b) disturbed state (key).

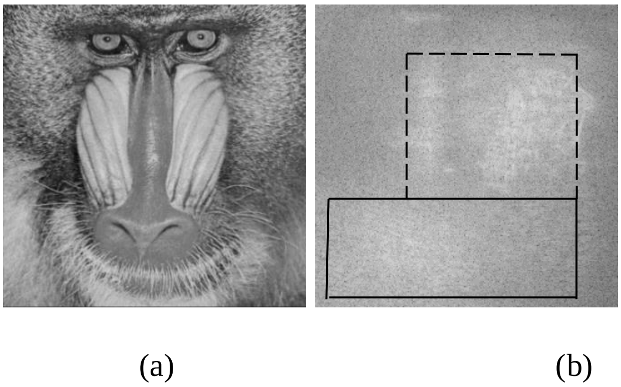
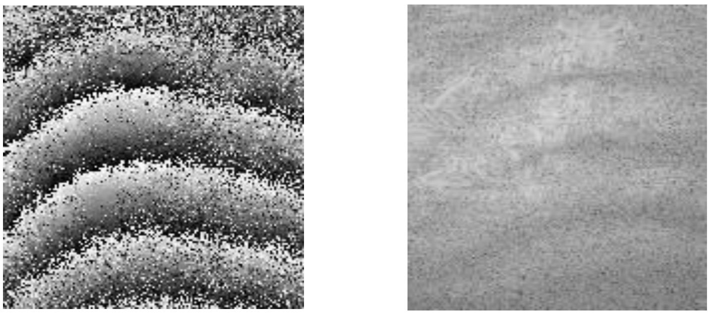


Figure 5.2: (a) Watermarked Baboon image. (b) Reconstructed intensity real image of the watermark (cantilever hologram)



(a) (b)

Figure 5.3: Reconstructed interference pattern as (a) phase contrast image and (b) amplitude contrast image.

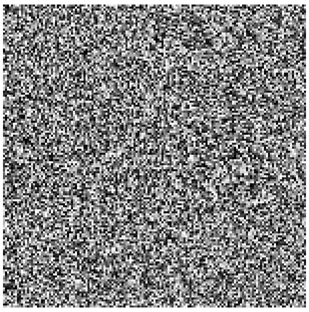


Figure 5.4 Reconstructed interference pattern, as phase contrast image, using the wrong key.

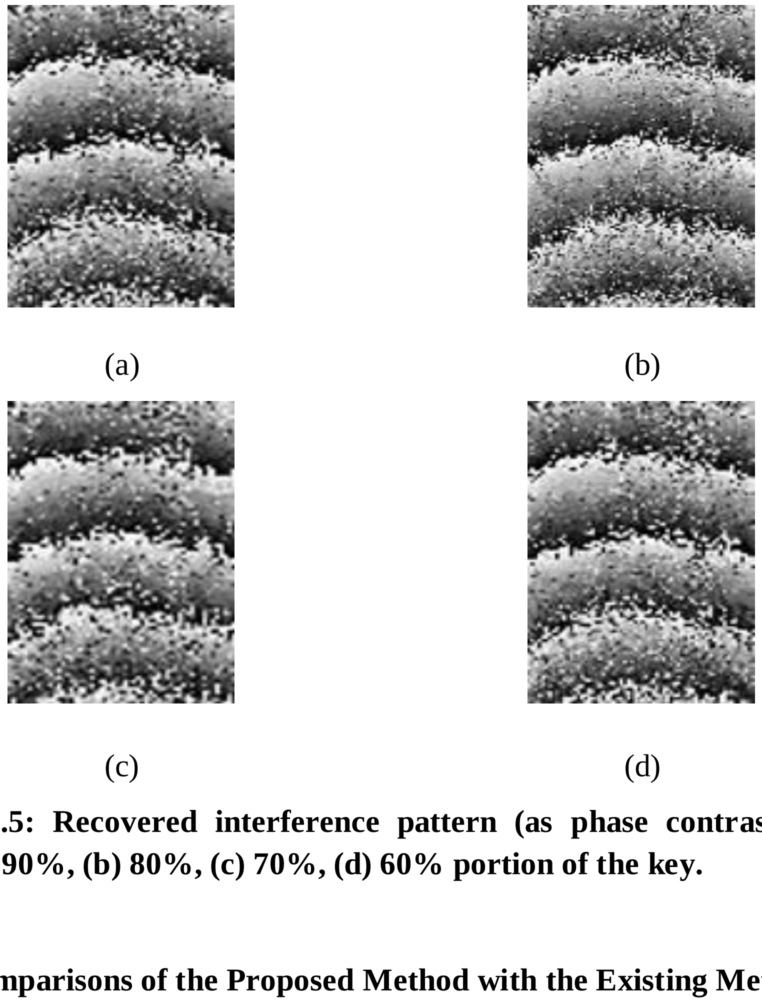
5.2 Recovery of Watermark Interference pattern by using Portion (%) of the Key

Table 5.1 shows the correlated coefficient results to reconstruct watermark interference pattern using portion (%) of the key**.** Experimental data shows that, by using 70% key total file sizes, one could reduce its total file sizes up to 65%. Furthermore, the quality of watermark interference pattern is still within the acceptable quality (CC = 0.803). However the watermark quality starts to deteriorate when using smaller portion of the key sizes, i.e. 60%

key file sizes. Figure 5.5 shows the recovered watermark phase image using different key total file sizes.

Table 5.1: The correlated coefficient results of the recovered watermark interference pattern by using portion (%) of the key

Portion (%) of the key	100	90	80	70	60
Correlated coefficient with original watermark hologram	1.000	0.861	0.810	0.803	0.72
Key file size (KB)	828	499	387	289	191



(a)

(b)

(c)

(d)

Figure 5.5: Recovered interference pattern (as phase contrast image) using (a) 90%, (b) 80%, (c) 70%, (d) 60% portion of the key.

5.3 Comparisons of the Proposed Method with the Existing Methods

In this chapter, the robustness of the proposed method is tested against Javidi, et al. (2003) and Nishchal, et al. (2010) method. This is because Cai, et al. (2004) and Li (2014) method is not suitable for comparison as phase-shifting hologram is used as the watermark. The 2-dimensional (2-D) watermark image is used in Javidi, et al. (2003) and Nishchal, et al. (2010) but since off-axis digital fresnel holograms is used in the project, Javidi, et al. (DRPE) and Nishchal, et al. (DRPE-FRT) methods are implemented by using the undisturbed hologram as watermark. The results can be divided into two categories, firstly to compare with Javidi et al. method, the proposed scheme and DRPE are embedded into host image using SVD domain as DHI-SVD and DRPE-SVD, respectively. Whereas to compare with Nishchal, et al. method, the proposed scheme and DRPE are embedded into host image using FRT technique as DHI-FRT and DRPE-FRT, respectively. Their robustness is tested against image processing attacks including noise addition, linear filtering, JPEG compression, image cropping, occlusion and rotation. The difference of the recovered watermark and original watermark is calculated by using the 2-D correlation coefficient given in Equation (2.2). If the correlation coefficient between the embedded and recovered holograms watermark is above 0.75, the watermark is within the acceptable range. From the results in Table 5.2, the DHI-SVD perceptually quality improved by 27.6%, when compared with DRPE-SVD. Table 5.3 shows that DHI-FRT perceptual quality improved by 19.7 % when compared with DRPE-FRT. Table 5.4 shows the proposed scheme performances against existing method using different host image.

Table 5.2: Perceptual quality of the watermarked image and recovered watermark using Javidi, et al. (2003) method.

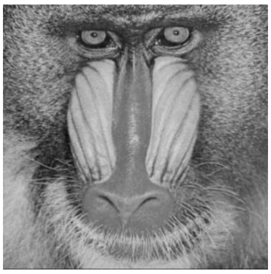
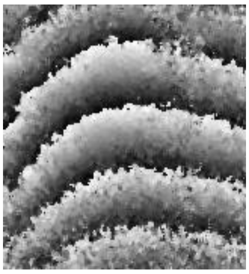
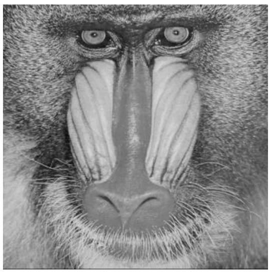
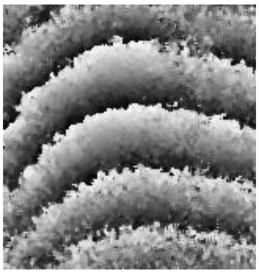
Methods	Watermarked Image	PSNR (dB)	Recovered Watermark	CC
DHI-SVD		46.49		0.993
DRPE-SVD Javidi et al.		35.63		0.990

Table 5.3: Perceptual quality of the watermarked image and recovered watermark using Nishchal, et al. (2010) method.

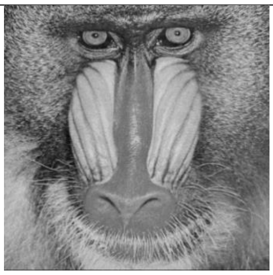
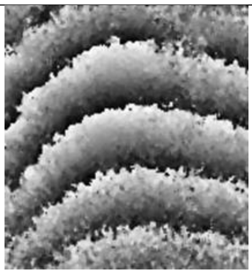
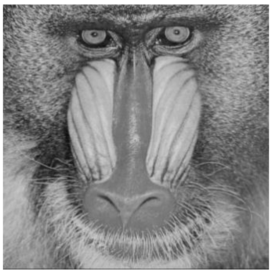
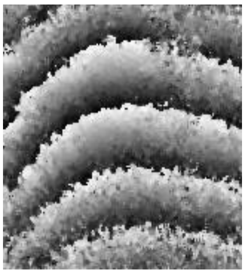
Methods	Watermarked Image	PSNR (dB)	Recovered Watermark	CC
DHI-FRT		46.57		0.991
DRPE-FRT Nishchal et al.		37.37		0.992

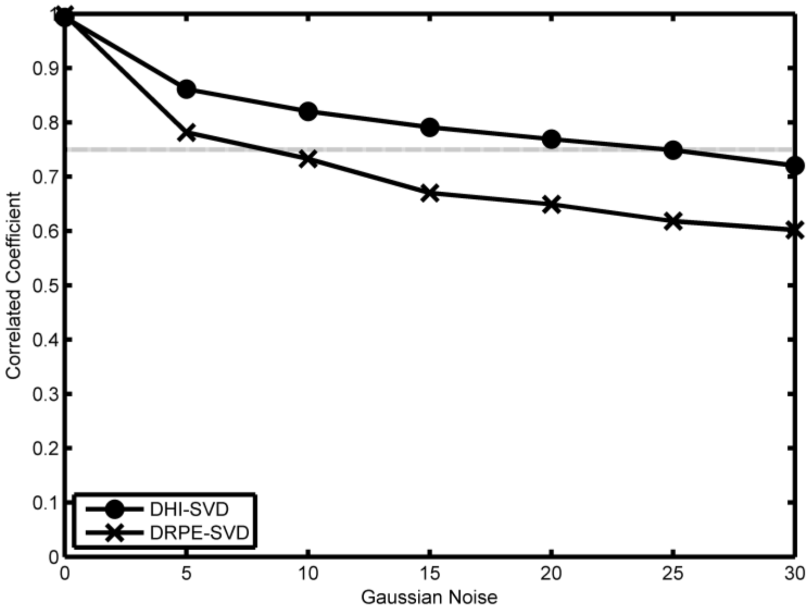
Table 5.4: Perceptual quality comparisons with different test image of the recovered watermark using the proposed method, Javidi et al. (2003) and Nishchal, et al. (2010) methods.

Perceptual Quality	Methods		Test Images				
			Baboon	Lena	Cameraman	House	Peppers
PSNR (dB) of Watermarked Baboon image	Proposed method	DHI-SVD	47.11	49.03	47.79	47.09	48.09
	Javidi, et al.	DRPE-SVD	38.32	38.28	38.08	37.95	38.02
	Proposed method	DHI - FRT	46.57	48.03	46.21	46.21	46.75
	Nishchal, et al.	DRPE-FRT	40.92	40.09	39.61	38.97	38.02
Correlated Coefficient of Recovered Watermark	Proposed method	DHI-SVD	0.998	0.998	0.988	0.999	0.996
	Javidi, et al.	DRPE-SVD	0.976	0.976	0.976	0.976	0.976
	Proposed method	DHI - FRT	0.991	0.991	0.989	0.988	0.990
	Nishchal, et al.	DRPE-FRT	0.977	0.977	0.977	0.968	0.968

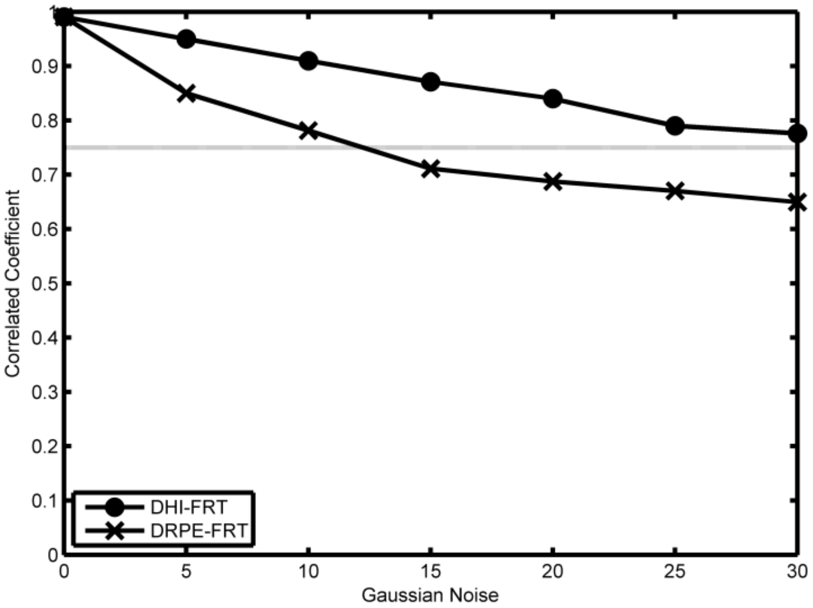
5.4 Robustness Testing

5.4.1 Attack by Additive Noise

To examine the effects of additive white noise on watermarking system, the watermarked baboon image is attacked by random Gaussian white noise. Figure 5.6 shows the correlation results between original watermark and recovered watermark after Gaussian noise attack using Javidi, et al. methods and Nishchal, et al. methods. The results show that the DHI's method overall robustness is better than the DRPE method.



(a)

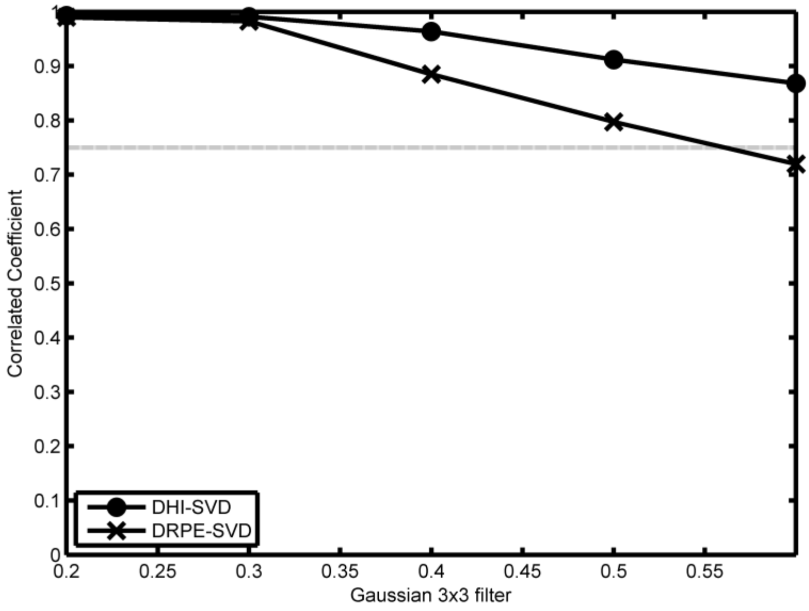


(b)

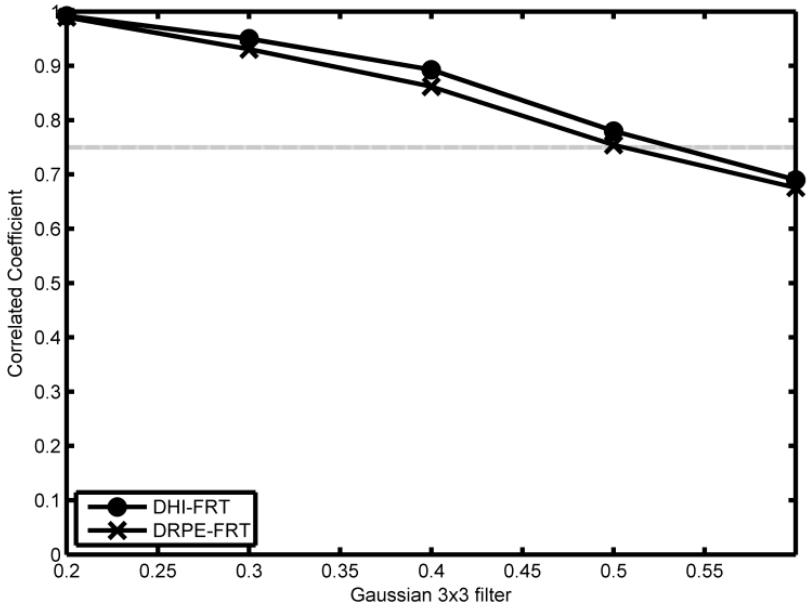
Figure 5.6: Correlation between original watermark and recovered watermark after Gaussian Noise using (a) proposed method versus Javidi, et al. (2003), and (b) proposed method vs Nishchal, et al. (2010) methods.

5.4.2 Attack by Linear Filtering

The Gaussian filtering, mean filtering and median filtering are used to attack the watermark image. The proposed method has the highest robustness compares with Javidi, et al. method and Nishchal, et al. method, as shown in Figure 5.17 and Table 5.5.



(a)



(b)

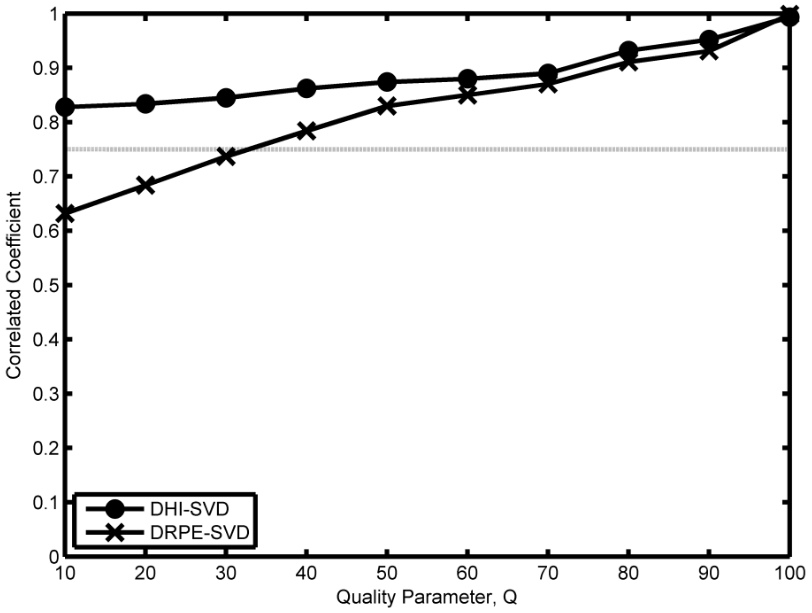
Figure 5.7: Correlation between original watermark and recovered watermark after Gaussian filter using the proposed method (a) proposed method versus Javidi, et al. (2003), and (b) proposed method vs Nishchal, et al. (2010) methods.

Table 5.5: Correlation between original watermark and recovered watermark after mean filtering and median filtering using Javidi, et al. . (2003) and Nishchal, et.al. . (2010) methods.

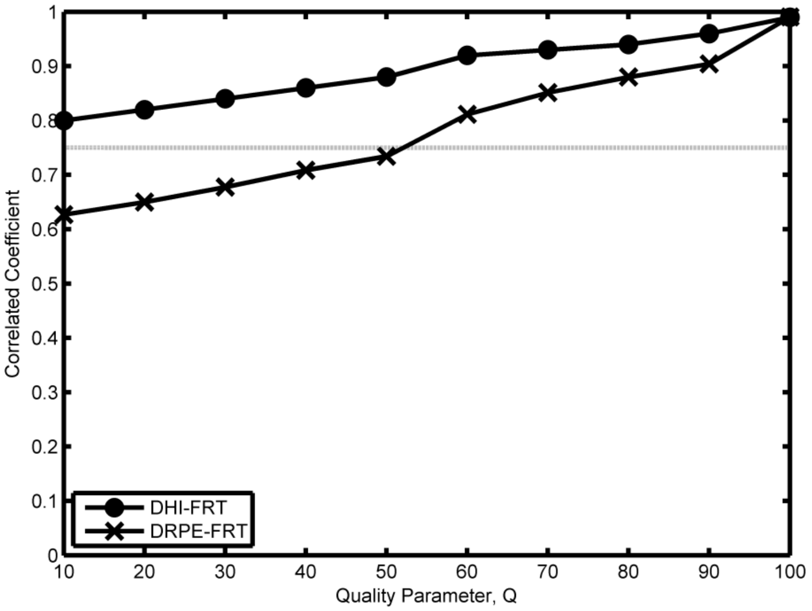
Method		Mean 3x3	Median 3x3
		Correlated Coefficient	
Proposed method	**DHI-SVD**	0.825	0.900
Javidi, et al.	**DRPE-SVD**	0.582	0.710
Overall Improvement (%)		+ 29.4%	+ 21.11
Proposed method	**DHI-FRT**	0.806	0.844
Nishchal, et al.	**DRPE-FRT**	0.547	0.674
Overall Improvement (%)		+ 32.13	+20.14

5.4.3 Attack by JPEG Compression

Figure 5.8 shows the correlations between the embedded and recovered holograms watermark with different quality parameters. From the graph, it is obvious that the proposed method has the highest resistant against JPEG compression compared to existing methods.



(a)

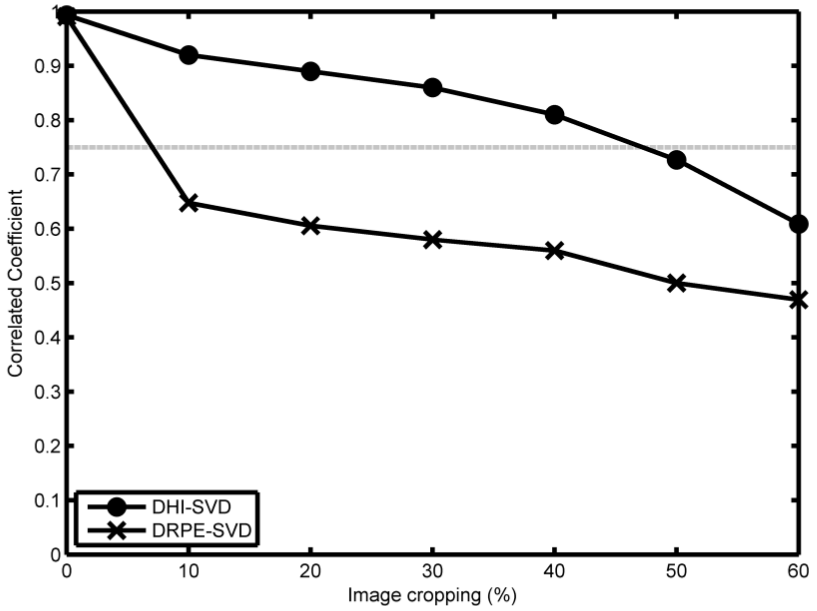


(b)

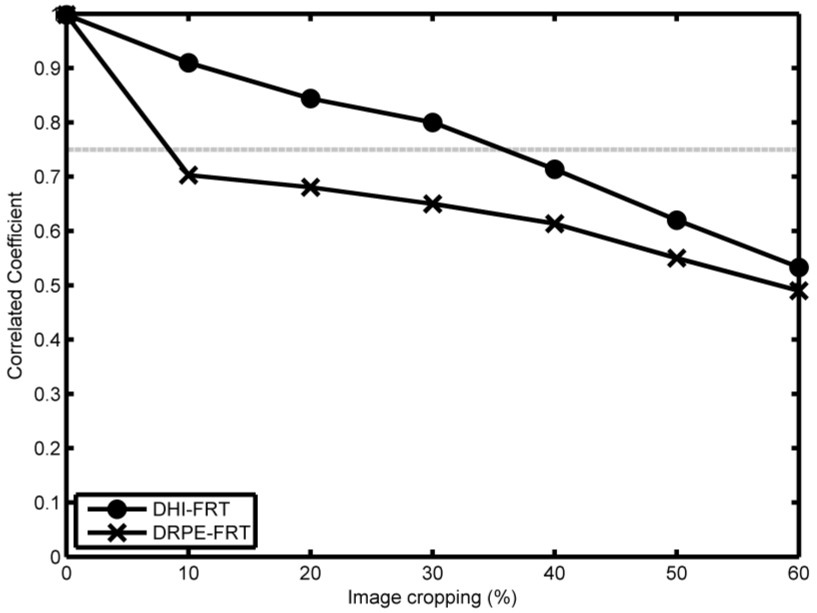
Figure 5.8: Correlation between original watermark and recovered watermark after JPEG compression using proposed method (a) proposed method versus Javidi, et al. (2003), and (b) proposed method vs Nishchal, et al. (2010) methods.

5.4.4 Attack by Image Cropping, Occlusion and Rotation

Since hologram can be reconstructed from using a piece of itself, the holographic watermarking is robust to image cropping/ occlusion. For instance it is still possible to detect the watermark by using 60% cropped watermarked baboon image which is shown in Figure 5.9 and Figure 5.10 . When the watermarked baboon image is rotated by 5 degree, the DHI method robustness improves by 29.7% and 37.0% against Javidi, et al. and Nishchal, et al. methods, respectively. Vice versa, the watermarked baboon image is rotated at - 5 degree, the DHI method robustness improves by 29.7% and 37.0% against Javidi, et al. and Nishchal, et al. methods, respectively

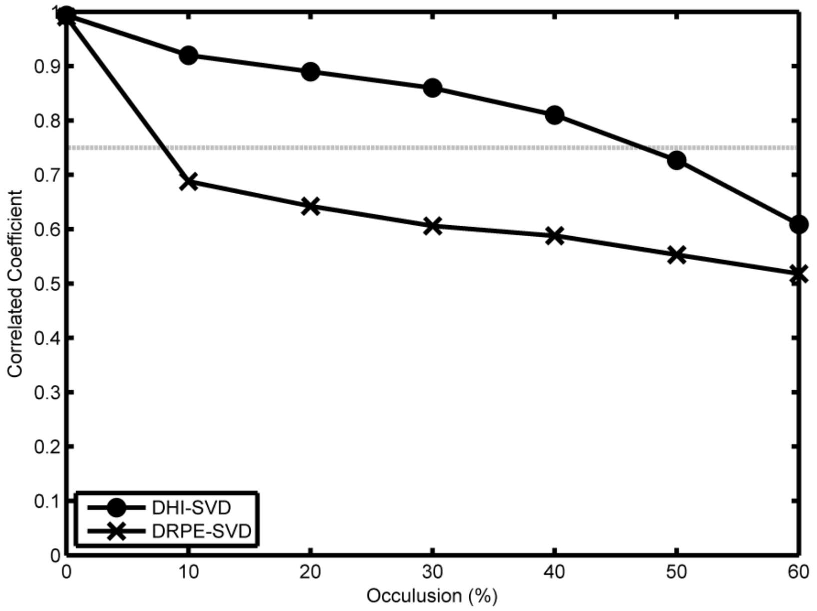


(a)

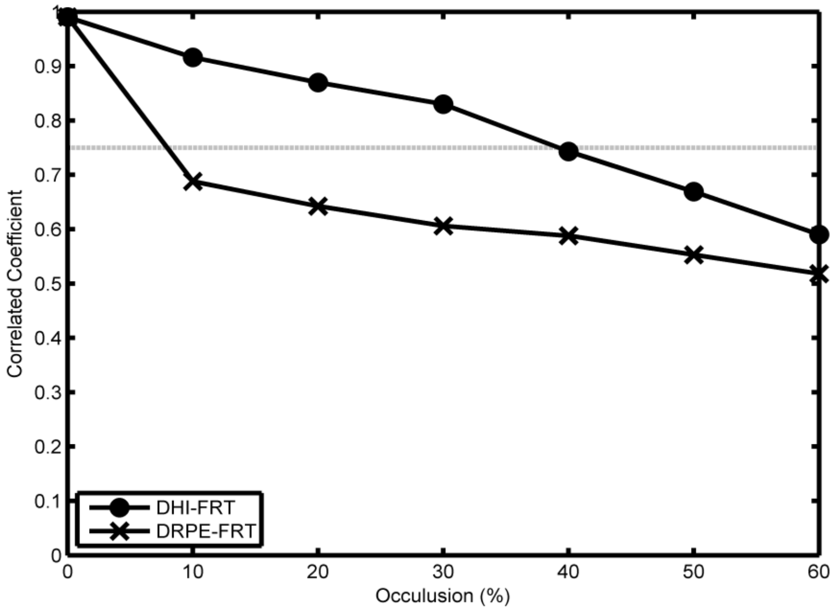


(b)

Figure 5.9: Correlation between original watermark and recovered watermark after image cropping using the proposed method (a) proposed method versus Javidi, et al. (2003), and (b) proposed method vs Nishchal, et al. (2010) methods.



(a)



(b)

Figure 5.10: Correlation between original watermark and recovered watermark after occlusion using the proposed method (a) proposed method versus Javidi, et al. (2003), and (b) proposed method vs Nishchal, et al. (2010) methods.

Table 5.6: Correlation between original watermark and recovered watermark after rotation attack.

Methods		Rotation Correlated Coefficient	
		-5°	5°
Proposed method	**DHI - SVD**	0.945	0.943
Javidi, et al.	**DRPE-SVD**	0.666	0.643
Overall improvement (%)		+29.6	+31.8
Proposed method	**DHI - FRT**	0.925	0.920
Nishchal, et al.	**DRPE-FRT**	0.582	0.571
Overall improvement (%)		+37.0	+37.9

5.5 Key Space Analysis for Digital holographic Interferometry Method

To estimate the key space of the proposed scheme, 256 quantization levels (pixels) are chosen for a pixel in the key hologram. Then the combination for key hologram with a size of $N \times M$ image is given as, $L^{N \times M}$, where L is the quantization level for grayscale image. Since the key hologram has a size of 1024×1024, the number of attempts to decode the interference pattern is given as $256^{1024 \times 1024}$. The proposed method is within the current benchmark for security, 2^{2048}, which is enough to resist any form of brute-force attacks.

In an attempt to reduce the number of key combination, the key hologram quantization level is reduced from 256 until 4. Figure 5.11 shows the reconstructed quality of interference pattern recovered with different quantization levels. Note that the interference pattern quality is not acceptable after 32 quantization levels and below. Table 5.7 shows the correlation between the key hologram sizes and key length. It is obvious that the combination of the key reduced as smaller portion of the hologram is used, for instance, 70% portion of the key hologram gives key length a total of $256^{718 \text{ x } 718}$ or $2^{8\times718 \text{ x } 718}$ possible combination. Moreover, the security of the DHI is a tradeoff between key hologram sizes and key length.

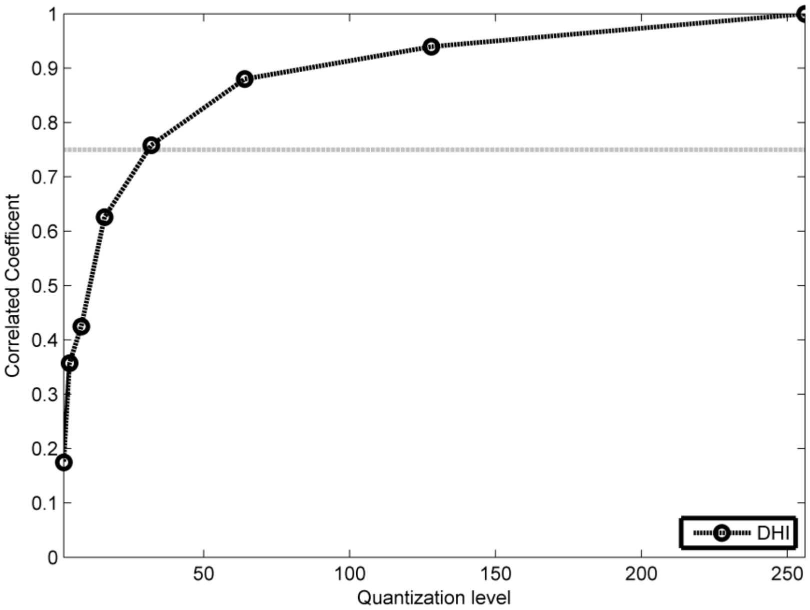


Figure 5.11: Reconstructed interference pattern (as phase contrast image) quality using different quantization level.

Table 5.7: Key length in 256 gray scale of portion of hologram used as the key.

Portion of the hologram used as the key	Pixel sizes of the hologram used	Key length for 256 quantization level
100	1024 × 1024	$256^{1024\times1024}$
90	922 × 922	$256^{922\times922}$
80	820 × 820	$256^{820\times820}$
70	718 × 718	$256^{718\times718}$
60	616 × 616	$256^{616\times616}$
50	512 × 512	$256^{512\times512}$

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 Introduction

A secure holographic watermarking scheme based on digital holographic interferometry is presented here. Before establishing a method for the secure watermarking approach, the embedding algorithmic that offer the best perceptual quality is investigated. The SVD domain offers the best perceptual quality against LSB, DCT and DWT. The characteristics of the holograms are investigated especially for reducing its total file size. Since the hologram can be reconstructed using a part of itself, the total file sizes of the hologram is greatly reduced from 256KB to 92.5KB. The holograms with different file sizes are then embedded into the host image and tested with image processing attacks. Experiment results shows that the robustness of the watermarking system can be adjusted using different watermark file sizes.

Digital holographic interferometry capture two holograms from different object states using double exposure techniques, either one as watermark or as a key. An observer with only optical parameter (wavelength of laser and recording distance) can recover up to the watermark information of cantilever hologram. However the authorised user with right key can recover the watermark interference pattern. Thus this method offers a second layer of security. Since the key is a hologram, one can further reduces its file sizes by using a portion of the key. From experimental results, the key file sizes can be reduced up to 70% of its total file sizes with acceptable image quality.

One of the criteria for secure watermarking scheme is the robustness. The obtained experiment results are compared with Javidi, et al. (2003) and Nishchal, et al. methods (2010). The robustness of the proposed method shows high resistant against common processing attack. The weakness of this method is there is a tradeoff between the key file sizes and reconstructed watermark quality. For instance by reducing the key sizes to 70%, the reconstructed phase image quality is reduced by 17%.

On the other hand, the security for DHI method (i.e. 70% portion of the key hologram) gives key length a total of $256^{718\times718}$ or $2^{8\times718\times718}$ possible keys which is still within the key length benchmark of 2^{2048}. The security of the DHI is a tradeoff between watermark key sizes and key length. In other words, smaller watermark file sizes equals to shorter key lengths.

6.2 Future Work

Since there is a trade-off between the watermark quality and the robustness, an optimum condition for secure watermarking using digital holographic interferometry needs to be investigating. Besides that an optimum weighting factor can be formulated to produces the least errors in the reconstructed 3-D host object and the decoded watermark. On the other hand, it is suggested to investigate another embedding algorithm which offers resistant to noise attack. Hence, it becomes possible to embed the watermark into the host image optimally.

Furthermore, the digital recording, numerical reconstruction and digital watermarking have to be integrated into a single system to increase the processing speed and user-friendly.

REFERENCES

1. Bracewell, N.R., 2000. *The Fourier Transform and Its Applications* (*3^{rd} Ed.*). Singapore: McGraw-Hill.

2. Barni, M., Bartolini, F. and Piva, A., 2001. Improved wavelet-based watermarking through pixel-wise masking. *Image Processing, IEEE Transactions*, 10(5), 783-791.

3. Barni, M., Bartolini, F., Vito. C. and Piva, A., 1998. A DCT-domain system for robust image watermarking. *Signal Processing*, 66(3), 357-372.

4. Chang, C.C., Tsai, P. and Lin, C.C., 2005. SVD-based digital image watermarking scheme. *Pattern Recognition Letters,* 26(10), 1577-1586

5. Celik, M. U., Sharma, G., Saber, E., and Tekalp, A.M., 2002. Hierarchical watermarking for secure image authentication with localization. *IEEE Transactions on Image Processing Focuses on Signal-Processing Aspects of Image Processing, Imaging Systems, and Image Scanning, Display, and Printing.* 11(6), 585-595.

6. Chung, K.L., Shen, C.H. and Chang, L.C., 2001. A novel SVD- and VQ-based image-hiding scheme. *Pattern Recognition Letters,* 22(9), 1051-1058.

7. Cox, I.J., Miller, M.L. and Bloom, J.A., 2000. Watermarking applications and their properties. *Information Technology: Coding and Computing, Proceeding*, 6 (12), 1673–1687.

8. Cuche, E., Marquet, P. and Depeursinge, C., 2000. Spatial filtering for zero-order and twin-image elimination in digital off-axis holography. *Applied Optics,* 39(23), 4070-4075.

9. Cai, L.Z., He, M.Z., Liu,Q. and Yang X.L., 2004. Digital image encryption and watermarking by phase-shifting interferometry," *Applied Optics,* 43, 3078-3084.

10. Chang, H.T. and Tsan, C. L., 2005. Image watermarking by use of digital holography embedded in the discrete-cosine-transform domain, *Applied Optics,* 44, 6211-6219.

11. Lai, C.C. 2011. An improved SVD-based watermarking scheme using human visual characteristics. *Optics Communications*, 284(4), 938–944

12. De, L. and Kim, J.W., 2010. High capacity robust forensic marking using computer generated hologram. *Digital Content, Multimedia Technology and Its Applications (IDC), 6th International Conference.* 194(197), 16-18.

13. Dainty, J.C. and Welford, T.W., 1971. Reduction of speckle in image plane hologram reconstruction by moving pupils. *Optics Communications,* 3(5), 289-294.

14. Gabor, D., 1949. Microscopy by recorded wavefronts. *Proc. R. Soc.,* 191(1051), 454-487.

15. Hencht, E., 2002. *Optics* (*4th Ed.*). San Francisco: Addison Wesley.

16. Higham, J.D. and Highnam, J.N. 2005. *Matlab Guide (2nd Ed).* Philadelphia: Siam.

17. Hyun, J.C., Seo.Y., Yoo, J.S. and Kim, D. W., 2008. Digital watermarking technique for holography interference patterns in a transform domain. *Optics and Lasers in Engineering,* 46(4), 343-348.

18. Juergen, S., 2005. *Digital Watermarking For Digital Media*. Hershey, Pennsylvania: Idea Group Inc.

19. Kishk, S. and Javidi, B., 2003. 3D object watermarking by a 3D hidden object. *Optics Express,* 11, 874-888.

20. Kishk, S. and Javidi, B., 2002. Information hiding technique using double phase encoding. *Applied Optics,* 41, 5470-5482.

21. Kishk, S. and Javidi, B., 2003. Watermarking of three-dimensional objects by digital holography. *Opt. Lett.* 28, 167-169

22. Kreis, T., 2005. *Handbook of Holographic Interferometry: Optical and Digital Methods*. Weinheim, Baden- Württemberg: Wiley-Vch.

23. Kim, H. and Lee, Y.H., 2005. Optimal watermarking of digital hologram of 3D object. *Optics Express,* 13, 2881-2886.

24. Hameed, K., Mumtaz, A. and Gilani, S.A.M., 2006. Digital Image Watermarking in the Wavelet Transform Domain. *World Academy of Science, Engineering and Technology*, 13, 86-89.

25. Ingemar, C., Matthew, M., Jeffrey, B., Jessica, F. and Ton, K. 2007. *Digital Watermarking and Steganography (2nd Ed.)*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.

26. Li, J. Z., 2014. An optimized watermarking scheme using an encrypted gyrator transform computer generated hologram based on particle swarm optimization. *Optics Express*, 22, 10002-10016.

27. Lyon, D. A., 2009. The discrete Fourier transform, part 2: Radix 2 FFT. *Journal of Object Technology,* 8(5), 21-33.

28. Leith, E. N. and Upatnicks, T., 1946. Wavefront reconstruction with diffused illumination and three-dimensional objects. *J. Opt. Soc. Am*., 54, 1295-1301.

29. Mahasweta, J.J., Zankhana, H.S.K. and Bragnvgatt, N., 2011. Watermarking in DCT-DWT Domain. *(IJCSIT) International Journal of Computer Science and Information Technologies*, 2 (2), 717-720.

30. Mcandrew, A. 2004. *An Introduction to Digital Image Processing with Matlab*. Victoria: Course Technology.

31. Meng, X. F., Cai, L. Z., He, M. Z., Dong, G. Y., and Shen, X. X., 2007. Cross-talk free image encryption and watermarking by digital holography and random composition. *Optics Communications*, 269(1), 47-52.

32. Meng, X.F., Cai. L.Z., Yang. X.L., Xu. X,F., Dong. G.Y., Shen. X.X., Zhang. H. and Wang, Y.R., 2007. Digital color image watermarking based on phase-shifting interferometry and neighboring pixel value subtraction algorithm in the discrete-cosine-transform domain. *Applied Optics,* 46, 4694-4701.

33. Nishchal, N.K., Pitkäaho, T. and Naughton, T.J., 2010. Digital Fresnel hologram watermarking. *9th Euro-American Workshop on Information Optics*, 1-3.

34. Okman, O.E. and Akar, G.B., 2007. Quantization index modulation-based image watermarking using digital holography. *J. Opt. Soc. Am.*, 24(1), 243–252.

35. Ozaktas, M.H. and Onural, L., 2008. *Three-dimensional television: Capture transmission, Display*. New York: Springer Berlin Heidelberg.

36. Refregier, P. and Javidi, B., 1995. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.*, 20(7), 767–769.

37. Spagnolo, G.S. and Santis, M.D. 2011. Holographic watermarking for authentication of cut images. *Optics and Lasers in Engineering*, 49(12), 1447-1455.

38. Schnars, U. and Jüptner, W., 2002. Digital recording and numerical reconstruction of holograms. *Meas. Sci. Technol.*, 13, 85-101.

39. Salvador, M., Prauzner, J., Kober, S., Meerholz, K., Turek, J. J., Jeong, K. and Nolte, D.D., 2009. Three-dimensional holographic imagine of living tissue using a highly sensitive photorefractive polymer device. *Optical Society of America*, 17(14), 11834-11849.

40. Sun, R., Sun, H. and Yao, T., 2002. A SVD-and quantization based semi-fragile watermarking technique for image authentication. *Signal Processing*, 2, 1592-1595.

41. Wang, F.H., Pan, J.S. and Jain, L.C., 2009. *Innovations in Digital Watermarking Techniques* (*XIV Ed.*). Warsaw: Springer.

42. Steinebach, M., Dittmann, J. and Saar, E., 2002. Combined fingerprinting attacks against digital audio watermarking: methods, results and solutions. *Advanced Communications and Multimedia Security*, 100, 197-212.

43. Wang, S. Z., Huang, S. J, Zhang, X. P. and Wu, W., 2010. Hologram-based watermarking capable of surviving print-scan process. *Applied Optics*, 49(7), 1170–1178.

44. Takai, N. and Mifune, Y., 2002. Digital watermarking by a holographic technique. *Applied Optics*, 41, 865-873.

45. Yong, T.K., Low, K.S. and Kwek, K.H., 1998. Digital recording and reconstruction of holograms. *Proceeding of international Meeting on Frontiers of Physics*, 421-424.

46. Yong, T.K., Low, K.S. and Kwek, K.H., 1998. Digital recording and application to laser metrology. *Proceeding of International Meeting on Frontiers of Physics*, 433-436.

47. Yong, X., Shan, W.Y., Cao, X.L. and Feng. Q. Q., 2012. Analysis and comparison of holographic and traditional digital image watermarking in DWT domain. *Computer Science & Education (ICCSE*). 790-793.

48. Xia, F., Zhang, H., Peng, D., Hui, L. and Longhu. X., 2009. Research of Digital Watermarking Based on DWT and Holography Image. *2nd International Image and Signal Processing (CISP*), 1(5), 17-19.

49. Stefan, K. and Fabien A.P., 2000. *Information Hiding Techniques for Steganography and Digital Watermarking (1st Ed.)*. MA, Norwood, MA: Artech House.

50. Cheng, C.J. and Lin, L.C., 2005. Correlation-based watermarking by a digital holographic technique. *Opt. Eng.*, 44, 010501-010502.

51. Li, J., 2010. Robust image watermarking scheme against geometric attacks using a computer-generated hologram. *Applied Optics*, 49 (32), 6302–6312.

52. Kim, H., Kim D.H., and Lee, Y.H., 2004. Encryption of digital hologram of 3-D object by virtual optics. *Optics Express*, 12, 4912–4921.

53. Unnikrishnan, G., Joseph, J., Singh, K. 2000. Optical encryption by double-random phase encoding in the fractional Fourier domain. *Opt. Lett.*, 25, 887– 889.

54. Matoba, O. and Javidi, B., 1999. Encrypted optical memory system using three-dimensional keys in the Fresnel domain. *Opt. Lett*., 24, 762–764

55. Nomura, T., Mikan, S., Mikan, Morimoto, Y. and Javidi, B., 2003. Secure optical data storage with random phase key codes by use of a configuration of a joint transform correlator. *Applied Opt*ics, 42, 1508 – 1514.

56. Yong, X., Shan, W.Y., Feng, Q. Q., Juan, L. and Wang, J.J., 2013. Performance comparison of holographic watermarking for color images in RGB and CMYK channels. *Control and Decision Conference (CCDC), 2013 25th Chinese*, 3024-3027.

57. Yong, X., Shan, W.Y., Feng, Q.Q. and Cao, X.L., 2012. Analysis and comparison of holographic and traditional digital image watermarking in DWT domain. *7th International Conference on Computer Science & Education (ICCSE)*, 790-793.

58. Huang, Q. L., Liu, J. L., Mao, H. and Chen, J., 2006. Blind digital watermarking technique using Fresnel hologram and phase encryption mask. *IET International Conference in Wireless, Mobile and Multimedia Networks*, 1-4.

59. Li, J. Z., 2014. An optimized watermarking scheme using an encrypted gyrator transform computer generated hologram based on particle swarm optimization. *Optics Express*, 22, 10002-10016.

60. Chen, L.S., Zhou, X.H. and Shao,J.A., 2005. Digital Hologram Watermarking with Large Information Contents Based on Binary Phase Encryption Method. *Acta Photonica Sinica*, 34(4), 616-620.

61. Seto, H., Aoki, Y. and Kang S., 2001. An image data watermarking technique using the average of a Fresnel-transformed pattern. *International Conference on Image Processing*, 534-537.

62. Huang, Q.L. and Liu, J.L., 2006. Blind digital watermarking technique based on optical Fresnel diffraction. *IET International Conference on Wireless, Mobile and Multimedia Networks,* 1-4.

63. Yamaguchi, I. and Zhang, T., 1997. Phase-shifting digital holography. *Opt. Lett.* 22, 1268-1270.

64. Awatsuji, Y., Fujii, A., Kubota, T. and Matoba, O., 2006.Parallel three-step phase-shifting digital holography. *Applied Optics,* 45, 2995-3002.

65. Wang, S.Z., Huang S.J., Zhang, X.P. and Wu, W., 2010. Hologram-based watermarking capable of surviving printscan process. *Applied Optics,* 49(7), 1170–1178.

66. Cheng, C.J., Hwang, W.J., Zeng, H.Y. and Lin, Y.C., 2014. A Fragile Watermarking Algorithm for Hologram Authentication. *J. Display Technol.,* 10, 263-271.

67. Levy, A. and Shaked, D., 2001. A transform domain hardcopy watermarking scheme. *Tech. Rep. HPL-2001-309 (Hewlett Packard*).

68. Zain, J. M., Baldwin, L. P. and Clarke, M., 2004. Reversible watermarking for authentication of DICOM images. *In Proc. 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 3237-3240.

69. Zain, J. M. and Fauzi, A. R. M., 2006. Medical Image Watermarking with Tamper Detection and Recovery. *Proc. 28th IEEE EMBS Annual International Conference,* 3270-3273.

70. Rivest, R., Shamir, A. and Adleman, L., 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2), 120–126.

71. Termont, P., De Strycker, L., Vandewege, J., Haitsma, J., Kalker, T., Maes, M., Depovere, G., Langell, A., Alm, C. and Norman, P., 1999. Performance measurements of a real-time digital watermarking system for broadcast. *IEEE International Conference in monitoring, Multimedia Computing and Systems,* 2, 220-224.

72. Low, C. Y., Teoh, A. B. J. and Connie, T., 2007. A preliminary study on biometric watermarking for offline handwritten signature," in *International Conference in Telecommunications and Malaysia International Conference on Communications,* 691-696.

73. Vatsa, M., Singh, R. and Noore, A., 2009. Feature based RDWT watermarking for multimodal biometric system. *Image and Vision Computing,* 27(3), 293-304.

74. Stingson, D. R., 2006. *Cryptography: Theory and Practice, 3^rd^ Ed., (Discrete Mathematics and Its Applications).* NW: Taykor & Frabcus Group.

75. Chen, T., Wang, J. and Zhou, Y., 2001. Combined Digital Signature and Digital Watermark Scheme for Image Authentication. *International Conferences on Info-tech and Info-net,* 5, 78-82.

76. Giakoumaki, A., Pavlopoulos, S. and Koutsouris, D., 2006. Secure and efficient health data management through multiple watermarking on medical images. *Med Biol Eng Comput.,* 44(8), 619-31.

77. Aggarwal, A. and Singla, M., 2011. Robust Watermarking of Color Images under Noise and Cropping Attacks in Spatial Domain. *(IJCSIT) International Journal of Computer Science and Information Technologies*, 2(5), 2036-2041.

78. Chang, C. C., Tsai, P. and Lin, C. C., 2005. SVD-based digital image watermarking scheme. *Pattern Recognition Letters,* 26(10), 1577-1586.

79. Chung, K. L., Shen, C. H. and Chang, L. C., 2001. A novel SVD- and VQ-based image hiding scheme. *Pattern Recognition Letters*, 22 (9), 1051-1058.

80. Sun, R., Sun, H. and Yao, T., 2002) A SVD- and quantization based semi-fragile watermarking technique for image authentication. (2002). *6th International Conference in Signal Processing.* 2, 1592-1595.

81. Djurovic, I., Stankovic, S. and Pitas, I., 2001. Digital watermarking in the fractional Fourier transformation domain. *Journal of Network and Computer Applications*, 24(2), 167-173.

82. Lang, J. and Zhang, Z. G., 2014. Blind digital watermarking method in the fractional Fourier transform domain, *Optics and Lasers in Engineering*, 53, 112-121.

83. Abookasis, D. and Rosen, J., 2003. Computer-generated holograms of three-dimensional objects synthesized from their multiple angular viewpoints. *J. Opt. Soc. Am. A*, 20, 1537-1545.

84. Vikas, R. and Barman, K. K., 2005. A report on print-scan resilient information hiding in images. *Tech Report, Hewleet Packard Labs India, Bangalore.*

85. Lin, L. C. and Chen, C. L., 2008. Statistical detection of digital holographic watermarking system. *Optics Communications*, 281(17), 4282-4290.

86. Cheng, C.J., Lin, L.C. and Dai, W. T., 2005. Construction and detection of digital holographic watermarks. *Optics Communications,* 248(1), 105-116.

87. Li, X. W. and Kim, S. T., 2013. Optical 3D watermark based digital image watermarking for telemedicine. *Optics and Lasers in Engineering*, 51 (12), 1310-1320.

88. Li, W. and Xue, X.Y., 2003. An Audio Watermarking Technique That Is Robust Against Random Cropping. *Journal Computer Music Journal Archive*, 27 (4), 58-68.

89. Chen, D.Q., Gu, J.H. and Zhou, H., 2011. Digital audio watermarking based on holographic nonlinear limiter. *International Conference* in *Electronics and Optoelectronics,* 2, 91-94.

90. Daqing, C., Hao, Z., Zhi, T. and Gu, J., 2011. Fourier computer generated hologram digital watermarking with nonlinear amplitude limiting", *Acta Optica Sinica*, 31(2), 52-58.

91. Tajahuerce, E., Matoba, O., Verral, S.C. and Javidi, B., 2000. Optoelectronic information encryption with phase-shifting interferometry. *Applied Optics*, 39, 2313-2320.

92. Kronrod, M.A., Merzlyakov, N.S. and Yaroslavskii, L.P., 1972. Reconstruction of a hologram with a computer. *Sov. Phys. Tech. Phys*., 17, 333–334.

93. Stern, A. and Javidi, B., 2006. Improved-resolution digital holography using the generalized sampling theorem for locally band-limited fields. *J. Opt. Soc. Am.*, 23, 1227-1235.

94. Jones, R. and Wykes, C., 1989. *Holographic and Speckle Interferometry, 2nd Ed*. Cambridge: Cambridge University Press.

95. Vest, C. M., (1979). *Holographic Interferometry*. New York: Wiley.

96. Collier, R. J., Burckhard, C. B. and Lin, H. L., 1971. *Optical Holography*. New York: Academic.

97. Schnars, U., 1994. Direct Phase determination in hologram interferometry with use digitally recorded holograms. *J. Opt. Soc. Am. A*, 11(7), 2011-2015.

98. Chen L.F. and Zhao, D., 2006. Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms. *Optics Express*, 14, 8552-8560.

99. Zhang, S. and. Karim, M,A., 1999. Color image encryption using double random phase encoding. *Microwave and Optical Technology Letters*, 14 (5), 318-323.

APPENDIX

PUBLICATIONS

Conference Papers (

1. Tan, H.Q., Yong, T.K. and Goi, B.K., 2012. Holographic watermarking Based On Off-axis Hologram and DWT. *IEEE Conference on Sustainable Utilization and Development in Engineering and Technology (STUDENT 2012),* 222-226.

2. Tan, H.Q., Yong, T.K. and Goi, B.K., 2014. A Comparative Analysis of Digital Holographic Watermarking Performances Using DWT and DCT. *13th International Conference on Electronics, Information, and Communication (ICEIC 2014), Kota Kinabalu, Malaysia*.

3. Tan, H.Q., Yong, T.K., Goi, B.K., and Chai T.Y., 2014. Digital Watermarking Using A Fusion of Digital Holographic interferometry and Singular Value Decomposition. *4th International Cryptology and Information Security Conference 2014 (Cryptology2014), Putrajaya, Malaysia.*

Journal Papers

1. Tan, H.Q., Yong, T.K. and Goi, B.K., 2013. Holographic Watermarking Based On Off-Axis Hologram and DWT-SVD. *International Journal of Cryptology Research*. 4(1), 17 – 31.

2. Tan, H.Q., Yong, T.K. and Goi, B.K., 2015. Digital Image Watermarking Using Digital Holographic Interferometry (DHI) Technique. *International Journal of Cryptology Research* 5(1), 77-87.

Journal Paper to be summited to Applied Optics

1. Tan, H.Q., Yong, T.K., Goi, B.K., and Chai T.Y. Secure and Robust Watermarking Schemes Based On Digital Holographic Interferometry Technique.