# ON EFFICIENT AND SECURE MODIFIED BUYER-SELLER WATERMARKING PROTOCOL

*Thesis submitted in fulfillment for the requirement of the degree of*

## DOCTOR OF PHILOSOPHY

by

**Ashwani Kumar**

**Enrollment No. 126204**

## UNDER THE SUPERVISION OF

**Prof. S.P. Ghrera**
**Prof. Vipin Tyagi**

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING AND INFORMATION TECHNOLOGY

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY WAKNAGHAT
SOLAN (H.P)

MAY 2016

# ABSTRACT

The rapid growth of internet and e-commerce needs a copyright protection mechanism for multimedia information. The advancement in internet and multimedia technologies consists huge amount of multimedia data in the form of audio, video and images is being practiced in many fields like medical fields, satellite information, digital forensics, surveillance systems, etc. This has contributed to higher demand for multimedia information like images with high optical quality. This protocol is basically used to extend the digital rights of both the purchaser and the vendor. The protocol uses digital watermarking and cryptography techniques to protect digital rights and digital copyrights for purchaser and the vendor during the transmission of digital contents over the internet.

Although in that respect are many published articles on buyer-seller watermarking protocol, but still many problems to be solved in the buyer, seller watermarking protocol such as if we resolve the customer’s right problem then unbinding will occurs. If we employ a double watermark insertion technique, conspiracy problem will occurs. In this protocol, the insertion of watermark should not degrade the quality of the image. Buyer-seller watermarking protocol consists of three main sub-protocols, i.e. watermark insertion protocol, watermark extraction protocol and dispute resolution protocol. In this dissertation, the writer has concentrated on managing the watermarks means the business is only watermark insertion protocol and watermark extraction protocol and made out his research in this focal point in order to get to the watermarking embedding and extracting algorithm more robust, imperceptible and improve the optical appearance of watermarked images.

The existing buyer-seller watermarking protocol uses some traditional methods for embedding and extracting the watermark. These methods were not robust and efficient. The author has proposed a robust and efficient watermarking embedding and extraction system based on discrete wavelet transform to improve the robustness and imperceptibility of the watermark. Further, the author has offered a lightweight watermarking embedding and extraction scheme as an improved variation of the above scheme which makes purpose of principal component analysis with wavelets together for further increasing the validity of the watermark. The buyer seller digital watermarking protocol basically depends upon the underline cryptosystems and digital watermarking techniques. Previously, the author has figured out on digital watermarking schemes which embed the watermark into original digital content and improved the validity of the watermark and imperceptibility of digital content. Here, the author has worked on a cryptosystem because traditional cryptosystem did not explain much about how a watermark is generated, embedded, and detected. For that author used Id-based public key cryptography with digital watermarking systems for both the purchaser and the vendor.

Hence, in this dissertation the research study of the author concentrates on embedding and extraction of the watermarks author do not uses new trust model, but design robust method for embedding and extracting the water lines. The primary focuses of author are to improve the validity of the watermark and imperceptibility of digital content. So, he has presented his major donation to the watermark embedding and extracting scheme into the buyer seller watermarking protocol. One can further increase robustness and imperceptibility of the embedding and extracting algorithm by applying some novel methods.

# ACKNOWLEDGEMENT

First, I would like to thank God the merciful, the gracious who has given me the ability, intelligence and energy to accomplish my Doctorate degree in Computer Science.

I would now like to take this opportunity to express my heart-felt gratitude to my supervisors, **Prof. Brig. Satya Prakash Ghrera (Retd.),** HOD, Computer Science and Engineering and Information Technology, JUIT, Waknaghat and **Prof. Vipin Tyagi,** Department of Computer Science & Engineering, Jaypee University of Engineering & Technology, Guna for sparing time from their busy schedule and providing me their valuable suggestions and discussions that stimulated me to work towards my thesis. They have been a constant source of motivation, ideas and guidance. I am highly grateful to them for their rich experience and expertise in various research areas, which proved to be very important in my research.

I would also like to thanks to **Dr. Vivek Sehgal,** Ph.D Coordinator and **Dr. Yashwant Singh**, **Dr. Pardeep Kumar**, **Dr. Shruti Jain**, **Dr. Pradeep Kumar Gupta**, Faculty, Jaypee University of Engineering & Technology and other DPMC (Doctoral Program Monitoring Committee) members for providing me assistance, moral support, valuable suggestions and necessary facilities during the course of my research work. I also wish my gratitude to Director **Prof. Samir Dev Gupta**, and Vice Chancellor **Prof. (Dr.) Vinod Kumar**, for their encouragement and help during the course of my research tenure at JUIT. I would like to thank the authorities of Jaypee University of Information Technology, Waknaghat for providing the financial support during my research work.

I also like to thank **Mr. Ashish Kistwal**, **Mr. Hardeep Rana**, and Lab. technicians of all computer labs in JUIT, for their help and cooperation.

I am very much thankful to my dear parents, my wife and family members for their affectionate encouragement and blessings to complete this research work.

**(Ashwani Kumar)**

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY
(Established by H.P. State Legislative vide Act No. 14 of 2002)
Waknaghat, P.O. DumeharBani, Kandaghat, Distt. Solan – 173234 (H.P.) INDIA
Website :www.juit.ac.in
Phone No. (91) 07192-257999 (30 Lines)
Fax: (91) 01792 245362

Date: 20, May, 2016

## DECLARATION

I hereby declare that the work reported in the Ph.D. thesis entitled **"On Efficient And Secure Modified Buyer-Seller Watermarking Protocol"** submitted at **Jaypee University of Information Technology, Waknaghat India,** is an authentic record of my work carried out under the supervision of Professor Brig. (Retd.) Satya Prakash Ghrera and Professor Vipin Tyagi. I have not submitted this work elsewhere for any other degree or diploma.

(Signature of the Scholar)

Ashwani Kumar

Department Of Computer Science & Engineering and Information Technology

Jaypee University of Information Technology, Waknaghat, India

Date (20, May, 2016)

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY

(Established by H.P. State Legislative vide Act No. 14 of 2002)
Waknaghat, P.O. Dumehar Bani, Kandaghat, Distt. Solan – 173234 (H.P.) INDIA
Website : www.juit.ac.in
Phone No. (91) 07192-257999 (30 Lines)
Fax: (91) 01792 245362

# CERTIFICATE

This is to certify that the work reported in the Ph.D. thesis entitled "**On Efficient and Secure Modified Buyer-Seller Watermarking Protocol**", submitted by **Ashwani Kumar** at **Jaypee University of Information Technology, Waknaghat**, **India,** is a bonafide record of his original work carried out under my supervision. This work has not been submitted elsewhere for any other degree or diploma.

| | |
|---|---|
| Brig. (Retd.) Satya Prakash Ghrera | Prof. Vipin Tyagi |
| Supervisor-1 | Supervisor-2 |
| Date:- | |

# LIST OF FIGURES

# LIST OF TABLES

# TABLE OF CONTENTS

## CHAPTER 5

## CHAPTER 6

# CHAPTER #1

## INTRODUCTION

### 1.1 Introduction

The speedy development of internet and e-commerce needs a copyright protection mechanism for multimedia data. Straight off a day's digital watermarking becomes an important technique for protecting the digital rights [1]. This hidden information can subsequently be taken out to prove the ownership of the digital content [2, 3]. With the increasing use of the internet, there is always a need to protect the multimedia data over the network. Data hiding in still images has two main applications such as fingerprinting and copyright protection. However, important aspects of digital watermarking systems include imperceptibility, robustness, capacity and security of the embedding and extracting process.

Digital multimedia has become innovative in the field of internet application and multimedia content can be easily stored, distributed and replicated in digital form enabling the illegal copying and distribution of digital products. The research in the area of digital watermarking has focused on the design of robust and secure watermarking techniques for piracy tracing and copyright protection [4] of multimedia content.

The principal object of digital watermarking technique is to retain digital copyright or watermark, embedded into the cover object. The desirable secure digital watermarking scheme is one, which integrates public key cryptosystem and digital watermarking technique for protecting the buyer and marketer in a digital content transaction. Digital watermarking [5] techniques use encrypted domain for embedding and extracting the watermarks. The rapidly growing of the internet encourages some bad usage too, similar operations such as transformation, duplication, and redistribution of digital content. With the accessibility of some software tools, one can easily identify these bad users and redistribution of digital capacity can be identified. Digital Rights Management (DRM) scheme has been suggested as the answer to the security problem in digital watermarking. It is the core system that allows digital content to disseminate their cinematic assets in a secure and restricted fashion. As content owners define the operations and the conditions under which they can be performed on the contentedness, a DRM system will assure that a digital content can simply be accessed according to the regulations stipulated by the producing studio.

Even though one stresses to protect digital content from unauthorized access and manage its use rights. No matter how secure the access control mechanism. Digital content eventually needs to be confronted in the clear to the viewing audience.

In general, secure digital watermarking [6] scheme should satisfy the following requirements.

**Robustness:** The capability of watermark to resist various image processing attacks such as rotation, scaling, clipping etc.

**Imperceptibility:** The optical distortion of the watermarked image should not have on the quality of the original painting.

**Effectiveness:** The algorithms for embedding and extracting the watermark into the digital content should be effective.

Digital image watermarking is a well-explored topic in the field of image processing where the prime objective is to improve the visual quality of an image and to make the watermark more robust against various types of attacks. Numerous digital watermarking techniques have been developed to minimize the effect of attack. A major challenge is to preserve the watermark into the digital content when the digital content is transferred between two parties over a non-secure communication channel. Figure 1.1 shows the proposed research model for buyer-seller watermarking protocol. First, author has taken an input Lena image then he performs the embedding operation with the help of some algorithm and secret key after embedding the watermark then he applies various types of attacked into watermarked image to check the robustness of the watermark.

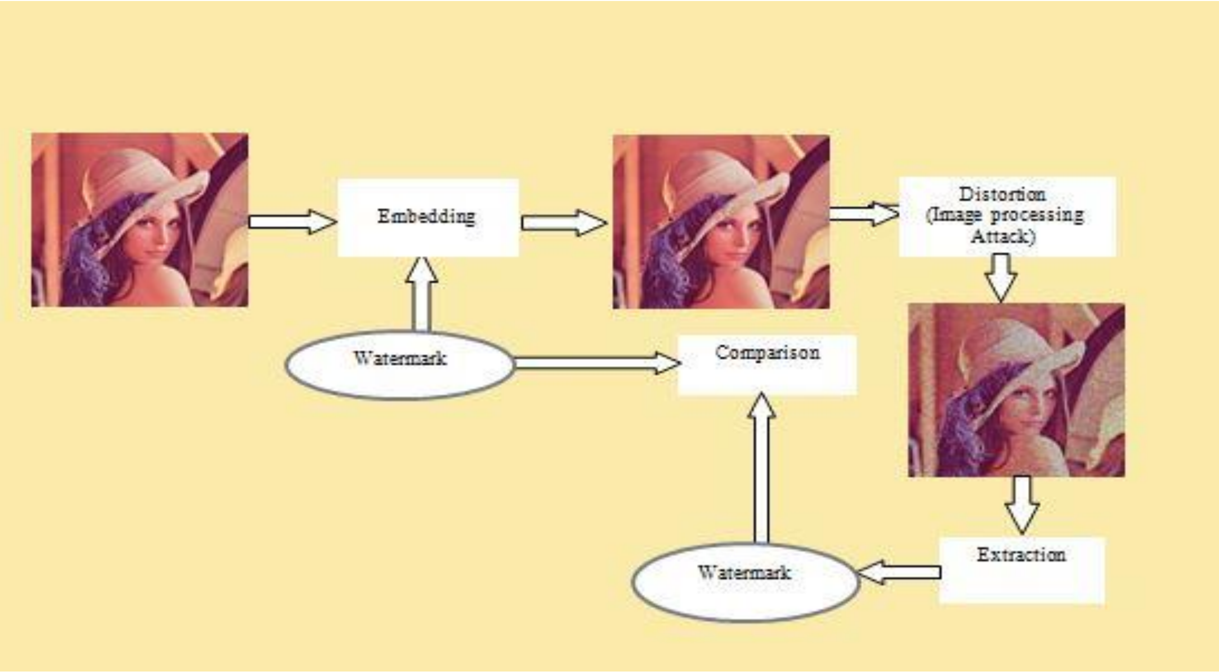


***Figure 1.1.1*** *Research model for Proposed Buyer-Seller watermarking protocol*

## 1.2 Buyer-Seller Watermarking Protocol (BSWP)

The (BSWP) [7] uses the techniques of cryptography and digital watermarking for digital right and illegal protection of digital content for the seller and at the same time it also preserves the buyer's rights to privacy. The buyer–seller watermarking protocol [8] is a three-party protocol among a service provider (seller), a customer (buyer) and a trusted watermark certificate authority (WCA). A (BSWP) [9], [10] is expected to solve the following problems:

- *Certification authority obligation*- The problem is to provide a digital certificate for both purchaser and vendor. A vendor may fabricate piracy to frame the purchaser.
- *Copy detection problem*- Pirated copy of content or data must be detectable and traceable back to the owner of the original copy.

- *Customer's rights problem*- This problem indicates that after legally purchasing the digital content still the seller attempt to frame an innocent buyer, because the seller may make and distributed a copy of digital content which the buyer has purchased.
- *Piracy tracing* - The protocol should be able to trace the pirated copy when it found. The seller should be able to trace and identify the copyright violator.
- *The unbinding* - Unable to bind a watermark for a particular digital content or transaction. The seller may distribute pirated by transplanting the buyer's watermark into other contents.
- *Anonymity* - The purchaser should be anonymous during transactions. The identity of the buyer should not be exposed until he is adjudicated to be guilty.
- *Non-repudiation*- The seller may not acknowledge the payment receipt and/or the innocent buyer may disagree with the receipt.

The whole process of buyer, the seller watermarking protocol is given below.

1. Requesting for a valid watermark to the WCA
2. Returning the generated watermark back to the buyer
3. Sending out the purchase order to the seller
4. Making the delivery back to the buyer

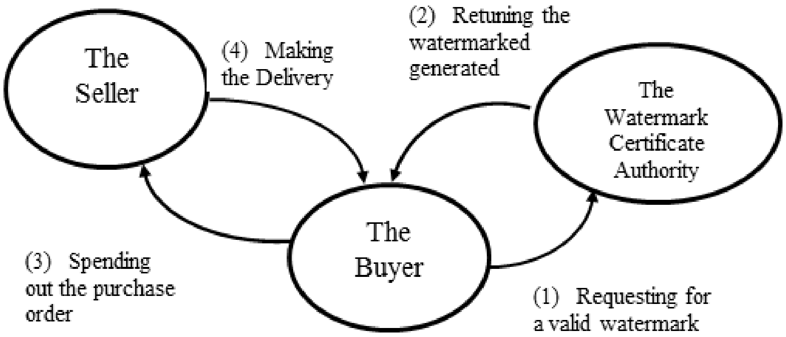

The Seller
(4) Making the Delivery
(2) Retuning the watermarked generated
The Watermark Certificate Authority
The Buyer
(3) Spending out the purchase order
(1) Requesting for a valid watermark

***Figure 1.2.1*** *Interactions among the buyer, the seller, and the watermark certification authority [10]*

A (BSWP) consists four main sub-protocols, i.e. Watermark generation protocol, Watermark insertion protocol, Copyright violator identification protocol and Dispute resolution protocol as presented in Figure 1.2.2.

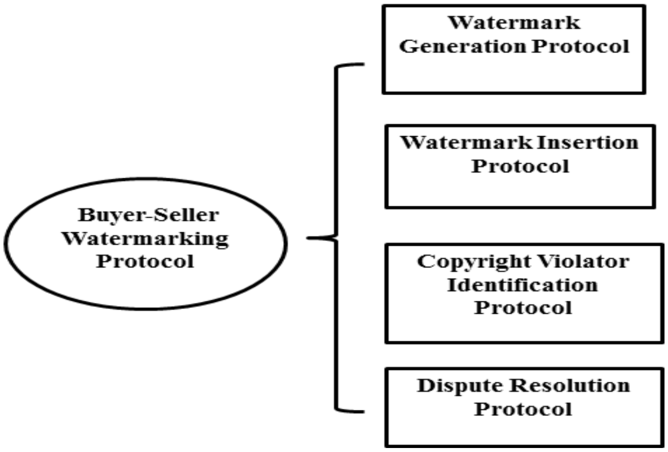

Buyer-Seller Watermarking Protocol
Watermark Generation Protocol
Watermark Insertion Protocol
Copyright Violator Identification Protocol
Dispute Resolution Protocol

***Figure 1.2.2*** *Four sub-protocols that comprise the buyer-seller watermarking protocol (BSWP) [10]*

### *A. Watermark Generation Protocol*

In this protocol, purchaser sends a digital certificate of his individuality and his public key to the trusted third party and requests a valid watermark.

### *B. Watermark Insertion Protocol*

This is a two-party protocol between seller and buyer in which buyer sends to seller the encrypted watermark along with the signature sign of the watermarked certification authority. Seller verifies signatures in order to be assured that is indeed a valid watermark generated by watermarked certification authority. The watermark insertion protocol uses digital watermark embedding algorithm for inserting the watermark into the digital content.

### *C. Copyright Violator Identification Protocol*

On discovering, an unauthorized copy of seller can determine the buyer from whom this copy has originated by detecting the unique watermark that seller inserted for each buyer. This is done by means of a watermark extraction function which is depending on the watermarking technique.

### *D. Dispute Resolution Protocol*

In case in which purchaser denies that unauthorized copy has originated from his version of the image, then the seller can reveal and sign to the judge. The judge first verifies signatures. He would then ask the buyer for his private key which he can compute and check for the presence of a watermark in unauthorized copy.

## 1.3 Attacks on Buyer-Seller Watermarking Protocol

In this section, author has discussed various types of attacks, which are found in various algorithms. Attacks are divided mainly into three parts: attack on buyer's security; attack on seller's security; and in last the attack upon the watermark. Generally, a watermarked cover may be altered either intentionally or unintentionally, so the watermarking system should still be able to detect and extract the watermark.

## 1.4 Problem Identification

In this thesis, the author has focused on the design of robust and secure watermarking techniques for piracy tracing and copyright protection of multimedia content. In this research work, the author has focused on the following problems

1. In the literature survey of BSWP author has found that the existing buyer-seller watermarking protocol are still not full filling the actual requirements of the user i.e. how to provide full freedom to the customers.

2. Some protocols are very good in comparison to others and some are the extended or modified versions of the other protocol.
3. So one need to discover more efficient and robust buyer-seller watermarking protocol, which takes less computational time and increase security, robustness, efficiency and flexibility.
4. The cryptosystem and digital watermarking scheme used by traditional (BSWP) are not much efficient.
5. For embedding and extracting the watermark the traditional buyer-seller watermarking protocol does not use the robust watermarking scheme.
6. The time taken by watermark insertion protocol and generation protocol can be reduces.
7. The security of this buyer-seller watermarking protocol lies on the security and robustness of the encryption standard and group signature techniques to improve the efficiency of the protocol.

## 1.5 Performance Evaluation

The standard simplified digital watermarking problem is to find a reasonably good estimate quality of watermark without losing much information. One of the common and simplest performance metric is the mean square error (MSE), defined as

$$MSE = \sum_{i=1}^{x} \sum_{j=1}^{y} \frac{(|A_{i,j} - B_{i,j}|)^2}{x * y} \qquad \textbf{(1.4.1)}$$

Where x is width of the image and y is height and x*y is the no. of pixels.

Most digital watermarking schemes uses the peak signal-to-noise ratio (PSNR) as a performance metric, which is defined in decibels (dB) for 8-bit grayscale images as

$$PSNR = 10 * log \frac{255^2}{MSE} \qquad \textbf{(1.4.2)}$$

A higher value of PSNR normally reflects the better performance of a digital image quality.

To check quality of the watermark, which is inserted into the digital content, author has used normalized correlation coefficient as follows.

$$NC = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} A_{i,j} B_{i,j}}{\sum_{i=1}^{m} \sum_{j=1}^{n} A_{ij}^{2}} \tag{1.4.3}$$

The MSE, PSNR, and NC are appealing performance metrics because these are easy to calculate and have clear physical meanings, which are also mathematically convenient in the context of optimization.

The performance metrics MSE, PSNR, and NC defined in Eqs. (1.4.1), (1.4.2) and (1.4.3), respectively, have been used for evaluation and comparison of the performances of proposed digital watermarking methods with existing methods.

## 1.6 Objectives of Thesis

Multimedia technology is buyer-seller watermarking protocol which plays important role in digital content distribution because it supports copyright information (such as the owner's identity, transaction dates, and serial numbers) for embedded as unperceivable signals into digital contents. Author purposed a modified buyer-seller watermarking protocol which is secure and efficient which gives more security from the previous proposed protocol.

Objective of this thesis are

- To propose a robust and efficient watermarking embedding and extraction scheme based on discrete wavelet transform to improve the robustness and imperceptibility of the watermark.
- To propose a lightweight watermarking embedding and extraction scheme as an improved variation of the above scheme which makes use of principle component analysis with wavelets together for further increasing the robustness of the watermark.
- To propose a cryptosystem with digital watermarking scheme which uses id-based public key cryptography for providing more security to the buyer and seller. In this, author also makes use of a tamper resistance device to reduce the overhead on WCA as TTP.

- To propose a scheme in which time-stamp can be used by TTP to keep accountability of digital signature based on composite signal representation to provide a secure communication between buyer and seller.
- To propose an approach for supporting multi-transaction and dispute resolution and also avoid double watermark insertion.

- To propose such a digital watermarking scheme that has the ability to overcome the problems which were existing in previously published protocol and increase the efficiency as well as security between buyer and seller.

Author has designed a digital watermarking protocol with cryptographic technique to obtain several objectives and identified number of problems in existing buyer-seller watermarking protocol and their solutions are proposed.

The contributions towards this research work are published as follows:

- A. Kumar, S.P. Ghrera, and V. Tyagi, Survey of Buyer-Seller Watermarking Protocol, International Journal of Technology & Management, volume VI September 2013.
- A. Kumar, S.P. Ghrera, and V. Tyagi, Implementation of Wavelet Based Modified Buyer-Seller Watermarking Protocol, WSEAS Transactions on Signal Processing, Volume 10, April 2014, pp. 212-220.
- A. Kumar, S.P. Ghrera, and V. Tyagi, A Comparison of Buyer-Seller Watermarking Protocol (BSWP) Based on Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Vol. 1, Springer International Publishing, 2015.
- A. Kumar, S.P. Ghrera, and V. Tyagi, Modified Buyer-Seller Watermarking Protocol based on Discrete Wavelet Transform and Principal Component

Analysis, Indian Journal of Science and Technology, Vol. 8, no. 35, December 2015.

- A. Kumar, S.P. Ghrera, and V. Tyagi, A new and efficient buyer-seller digital watermarking protocol using Identity based technique for copyright protection, International Conference on Image Information Processing (ICIIP -2015) proceedings IEEE Computer Society Press in IEEE Explore, pp. 531-535, 21-24 Dec 2015.
- A. Kumar, S.P. Ghrera, and V. Tyagi, An ID-based Secure and Flexible Buyer-seller Watermarking Protocol for Copyright Protection, Science & Technology, Pertanika J. Sci. & Technol. Vol. 25, no. 1, pp. 57 – 76, January 2017.

## 1.7 Outline of Thesis

In this dissertation, the possible solution to protecting illegal reproduction of digital content have been produced. The thesis has been organized into eight chapters. Each chapter gives distinct concept.

In CHAPTER 1, the author has given the introductory part of the thesis. Review and background has been explained in CHAPTER 2.

In CHAPTER 3, author has presented a robust and efficient watermarking embedding and extraction scheme based on discrete wavelet transform to improve the robustness and imperceptibility of the watermark.

In CHAPTER 4, author has presented a lightweight watermarking embedding and extraction scheme as an improved variation of the above scheme which makes use of principle component analysis with wavelets together for further increasing the robustness of the watermark.

CHAPTER 5 represents a comparison of buyer-seller watermarking protocol (BSWP) based on discrete cosine transform (DCT) and discrete wavelet transform (DWT).

In CHAPTER 6, author presents a cryptosystem with digital watermarking scheme which uses id-based public key cryptography for providing more security to the buyer and seller. He proposed an ID-based secure and flexible buyer-seller watermarking protocol for copyright protection.

In CHAPTER 7, author has presented a scheme in which time-stamp can be used by TTP to keep accountability of digital signature based on composite signal representation to provide a secure communication between buyer and seller. He proposed a lightweight buyer-seller watermarking protocol based on composite signal representation and time-stamping based techniques for multimedia data distribution.

In CHAPTER 8, the author has given conclusions of all chapters and also presents the future scope of the research work. References and list of publications are given after CHAPTER 8.

# CHAPTER # 2

## REVIEW AND BACKGROUND

### 2.1 INTRODUCTION

A Buyer-Seller Watermarking Protocol [12] is a protocol that incorporates techniques of digital watermarking and fingerprinting to protect the rights of both the customer i.e. buyer and the content provider i.e. seller. Buyer-Seller watermarking protocol (BSWP) is fundamentally applied to continue the digital rights of both the purchaser and vendor and it use digital watermarking scheme with cryptography techniques in society to protect privacy rights and digital copyrights for the purchaser and the seller during the transmittal of digital contents over the cyberspace.

In history, there are many watermarking protocols have been proposed [13]. The very first protocol was introduced by Memon et al. [10], and it was improved by Ju et al. [14]. From then many alternative protocols have been proposed in [11], [14, 15].

However, discrete wavelet transform [16] are used more frequently in digital image watermarking [17, 18, 19].

### 2.2 OVERVIEW OF DIGITAL WATERMARKING

The rapid growth of multimedia content over internet demands effective technique for secure and efficient access to information.

### 2.3 TYPES OF DIGITAL WATERMARKING SYSTEMS

There are several types of robust copyright marking systems. They are defined by their inputs and outputs.

**2.3.1 Public watermarking:** This scheme is also known as blind watermarking. In this scheme, the detection process is fully known to anyone as opposed to private watermarking where a secret key is required. Indeed such systems really extract n bits of information (the mark) from the marked image.

**2.3.2 Asymmetric key watermarking:** Asymmetric watermarking is a technique where different keys are used for embedding and detecting the watermark. It should have the property that any user can read the mark, without being able to remove it.

**2.3.3 Symmetric key watermarking:** In symmetric watermarking (or symmetric key watermarking), the same keys are used for embedding and detecting watermarks.

**2.3.4 Blind watermarking:** In blind watermarking scheme, one can perform verification of the watermark without use of the original image. Other techniques rely on the original to detect the watermark.

## 2.4 TYPES OF DIGITAL WATERMARKS

The different authors use different meanings for the word watermark it is mostly agreed that the watermark is one, which is imperceptibly added to the cover object in order to convey the hidden data. The process of embedding information into another object is called digital watermarking [20]. There are different types of watermarks such as:

**2.4.1 Visible watermarks:** The visible watermarks are designed in such a way to be easily identified by the viewer, and clearly identified by the owner.

**2.4.2 Invisible watermarks:** Invisible watermarks are designed to be imperceptible. This type of watermark is not visible in the watermark image without degradation of image or data. Invisible watermark may be any logo or any signature.

**2.4.3 Fragile watermarks:** The fragile watermarks are designed to resist some distortion, or to be broken, under the slightest changes to the image.

**2.4.4 Robust watermarks:** These are the watermarks, which survive any reasonable processing inflicted on the original object. These watermarks are embedded [21] in such a way that any signal transformation of reasonable strength cannot remove the watermark.

## 2.5 CHARACTERISTICS OF WATERMARK

In this section, various characteristics of watermark are discussed one by one. These characteristics are very important a watermark should hold these characteristics.

- **Unambiguous:**

  The extraction of the watermark should unambiguously identify by the owner and the accuracy of identification should degrade gradually in the face of attacks.
- **Imperceptible:**

  Imperceptibility means the difference between the watermarked image and the original image should not noticeable by human eyes or the human vision system.
- **Robustness:**

  The ability of watermark to survive under normal image processing of digital content. The embedded watermark should survive after a number of common image processing operations such as cropping, scaling and lossy compression.
- **Lossless:**

  It should imply no loss of relevant information while an attack is taking place.

## 2.6 APPLICATION OF DIGITAL WATERMARKING

In this section, various application of digital watermarking are discussed one by one. These applications [22] are very important a watermarking system should give these applications, Owner Identification, Copy Protection, Broadcast Monitoring, Medical applications, Fingerprinting, Data Authentication, Video Watermarking, Audio Watermarking, and Data Hiding.

## 2.7 PAPER REVIEWED

Authors have reviewed various research papers related to buyer-seller watermarking protocol. He has also discussed the pros & cones of the existing watermarking protocol.

**2.7.1** L. Qiao, and K. Nahrstedt, Watermarking Schemes and Protocols for Protecting Rightful Ownership and Customer's Rights, Journal of Visual Communication and Image Representation, vol. 9, no. 3, pp. 194–210, 1998.

Conclusion: In this paper, L Qiao and K Nahrstedlt [23] have proposed watermarking schemes and protocols for protecting rightful ownership and customer's right in 1998. In this paper the authors have identified the traditional watermarking problem i.e. mainly two problems first one is the resolution of rightful ownership problem and the second is a customer's right problem. In this paper authors have given the solution of the identified problem. They have proposed a novel watermarking approach for the rightful ownership problem and customer's right problem for that they have used watermark generation algorithm, using an encryption function in the construction of the watermark, as well as a watermarking insertion algorithm. They have discussed technique in which a customer (or buyer) forwards encrypted version of a predefined bit-sequence to the owner (or seller).

**2.7.2** N. D. Memon, and P. W. Wong, A Buyer-Seller Watermarking Protocol. IEEE Transactions on Image Processing, vol. 10, no. 4, pp. 643–649, 2001.

Conclusion: In this paper, Memon et al. [10] proposed the first known buyer-seller watermarking protocol in 2001. They have presented an interactive buyer–seller protocol for invisible watermarking in which the seller does not get to know the exact watermarked copy that the buyer receives. Hence the seller cannot create copies of the original content containing the buyer's watermark. The authors have used for protocols i.e. watermark generation protocol, watermark insertion protocol, copyright violator identification protocol and dispute resolution protocol. The protocol was quite simple and was used by various watermarking techniques. Memon’s protocol has a weakness in that the seller can frame a buyer with a higher-value image.

**2.7.3** H.S. Ju, H.J. Kim, D.H. Lee, and J.I. Lim, An Anonymous Buyer-Seller Watermarking Protocol with Anonymity Control, Proc. ICISC, LNCS 2587, pp. 421-432, 2002.

Conclusion: Ju et al. proposed An Anonymous Buyer-Seller Watermarking Protocol with Anonymity Control [15] in 2002. In this paper, the authors have identified the anonymity problem. They have discussed that a buyer can purchase digital content anonymously but the anonymity can be controlled. The main feature of this paper is to provide anonymity for both the seller and the buyer. The proposed protocol has limited robustness. Author used two trusted parties watermark certificate authority and judge for resolving the anonymity problem.

**2.7.4** J.G. Choi, and K. Sakurai, Does it need trusted third party? design of buyer-seller watermarking protocol without trusted third party, In Applied Cryptography and Network Security, LNCS 2846, pp. 265–279, 2003.

Conclusion: In this paper, Jae-Gwi Choi et al. [14] Proposed design of buyer-seller watermarking protocol without a trusted third party in 2003. The authors have identified the anonymity problem. In this the authors have used two identities WCA and arbiter to resolve the anonymity problem. This scheme must assume the existence of trusted third party i.e. watermark certificate authority (WCA). They compare their protocol with Ju et al.

**2.7.5** C.-L. Lei, P.-L. Yu, P.-L. Tsai, and M.-H. Chan, An Efficient Anonymous Buyer-Seller Watermarking Protocol, IEEE Transactions on Image Processing, vol. 13, no. 12, pp. 1618– 1626, 2004.

Conclusion: In this paper, Lei et al. [11] proposed An Efficient and Anonymous Buyer-Seller Watermarking Protocol in 2004. In this paper, they have inserted a second watermark into the cover image. The second watermark is generated by a watermark cortication authority (WCA) and sent to the buyer securely.

**2.7.6** B.-M. Goi, R. C.-W. Phan, Y. Yang, F. Bao, R. H. Deng, and M. U. Siddiqi, Cryptanalysis of Two Anonymous Buyer-Seller Watermarking Protocols and An Improvement for True Anonymity, In Applied Cryptography and Network Security, LNCS 2587, pp. 369–382, 2004.

Conclusion: In this paper, B.-M.Goi et al. [24] proposed a Cryptanalysis of two anonymous buyer-seller watermarking protocol and an improvement for true anonymity in 2004. In this the author analyzes the security of two recent anonymous buyer seller watermarking protocols proposed by Ju et al. and Choi et el. respectively and prove that they do not provide security and features as claimed. The commutative cryptosystem used by Choi et al. fails to prevent the watermark certificate authority (WCA) from discovering the watermark. In this paper the author enhanced the previous buyer-seller schemes with the same computational complexity. This paper uses asymmetric cipher, Hence the cover image has to be separated and encrypted independently in the previous schemes.

**2.7.7** M. Kuribayashi, and H. Tanaka, Fingerprinting protocol for images based on additive homomorphic property, IEEE Transactions on Image Processing, vol. 14, no. 12, pp. 2129–2139, 2005.

Conclusion: In this paper, Kuribayashi and Tanaka proposed fingerprinting protocol for images based on additive homomorphic property [25] in 2005. In this paper the author proposes a new fingerprinting protocol applying additive homomorphic property of Okamoto–Uchiyama encryption scheme. They study the problem of implementation of watermarking technique and propose a successful method to embed encrypted information without knowing the plain value. The perceptual qualities of the embedded image survive against several attacks and give robustness. They use anonymous fingerprinting that improves the enciphering rate with interactive Zero-knowledge proof. However, it is computationally intensive and bandwidth is not efficient.

**2.7.8** J. Zhang, W. Kou, and K. Fan, Secure Buyer-Seller Watermarking Protocol, IEEE Proceedings of Information Security, vol. 153, no.3, pp. 15–18, 2006.

Conclusion: In this paper, J. Zhang et al. [26] proposed a secure buyer–seller watermarking protocol in 2006. In this paper no assistance of a trusted third party (TTP) is required, so that it avoids the conspiracy problem, piracy tracing problem & customer's right problem. In this paper authors have use registration protocol, watermarking protocol, identification and arbitration protocol for the proposed protocol. There are only two participants, a seller and a buyer. The protocol can simultaneously resolve many problems. This paper is based on the Lei et al. and in this no third party is introduced, therefore the proposed protocol is simpler and more secure than the existing watermarking protocol. But there is a drawback in the J. Zhang protocol i.e. the buyer's assistance is required to resolve the piracy dispute.

**2.7.9** F. C. Chen, T. Ming, and S. Wei-Zhe, Buyer-Seller Watermarking Protocols with Off-line Trusted Parties, MUE '07. International Conference on Multimedia and Ubiquitous Engineering, pp. 1035–1040, 2007.

Conclusion: In this paper, Chun-I Fan et al. [27] proposed a buyer-seller watermarking protocol with off-line trusted parties in 2007. In this paper a tamper-resistant WCA device is required to produce the necessary watermarks and signatures. The proposed protocol can guarantee the anonymity of the buyers as well. In this paper, the authors have proposed a robust watermarking scheme to protect the ownerships of digital contents. The scheme can withstand all of the known attacks and problems. The performance of the protocol can be further improved.

**2.7.10** I. M. Ibrahim, S. H. N. El-Din, and A. F. A. Hegazy, An effective and secure buyer-seller watermarking protocol, In Third International Symposium on Information Assurance and Security, IAS 2007, pp. 21–28, Aug. 2007.

Conclusion: In this paper, I. M. Ibrahim, S. H. N. El-Din and A. F. A. Hegazy proposed an effective and secure buyer-seller watermarking protocol [28] in 2007. They proposed an effective and secure buyer-seller watermarking protocol that encapsulates flexible and yet convenient solution to all of the previously mentioned problems. In this paper a novel idea of generating buyer's dual signature of both the purchase order and the buyer's associated unique watermark. Authors use two sub-protocols (watermark generation/insertion protocol and dispute resolution protocol). The security of the proposed protocol is based on the security of the public key infrastructure (PKI). Authors use the trusted certification authority (TCA) which is considered the only trust anchor between the buyer and the seller.

**2.7.11** S. Katzenbeisser, A. Lemma, M. U. Celik, M. van der Veen, and M. Maas, A buyer-seller watermarking protocol based on secure embed-ding, IEEE Trans. Inf. Forensics Security, vol. 3, no. 4, pp. 783–786, Dec. 2008.

Conclusion: In this paper, Stefan Katzenbeisser, et al. [29] proposed A Buyer–Seller Watermarking Protocol Based on Secure Embedding on 2008. Author shows that the existing functionality of the buyer seller watermarking protocol can be achieved efficiently using recently proposed secure watermark embedding algorithms.

**2.7.12** Y. Hu, and J. Zhang, A secure and efficient buyer-seller watermarking protocol, Journal of Multimedia, vol.3, no.4, pp.161-168, 2009.

Conclusion: Yuping Hu, and Jun Zhang [30] proposed A Secure and Efficient Buyer-Seller Watermarking Protocol in 2009. In this paper, the authors use memory less watermark certification authority (WCA) that can offer a number of watermarks for a buyer simultaneously, avoiding itself being involved in each digital transaction operated between the buyer and the seller. In this authors use the three sub-protocols that comprise the proposed protocol the watermark generation protocol, the transaction protocol, and the identification and arbitration protocol. But Anonymity can be revoked if the arbitrator adjudicates him to be guilty.

**2.7.13** A. Kumar, M. D. Ansari, J. Ali, K. Kumar, A New Buyer-Seller Watermarking Protocol with Discrete Cosine Transform, in CNC CCIS 142, pp. 468–471, 2011 © Springer-Verlag Berlin Heidelberg 2011.

Conclusion: In this paper, Kumar, Ashwani et al. [31] proposed a new buyer-seller watermarking protocol with the discrete cosine transform in 2011. In this author use public key infrastructure (PKI), arbitrator and watermarking certificate authority (WCA) for better security. The authors have used a discrete cosine transform to produce the watermarks. The protocol is secure and flexible and gives more security from previous watermarking protocols to both buyer and seller.

**2.7.14** A. Kumar, V. Tyagi, M. D. Ansari, and K. Kumar, A Practical Buyer-Seller Watermarking Protocol based on Discrete Wavelet Transform, International Journal of Computer Applications, pp. 46-51, 2011.

Conclusion: In this paper, Kumar, Ashwani et al. [32] proposed a practical buyer-seller watermarking protocol based on discrete wavelet transform in 2011. In this paper authors propose a practical buyer-seller watermarking protocol based on discrete wavelet transform (DWT) which is secure, effective, flexible and gives more robustness.

**2.7.15** A. Rial, J. Balasch, and B. Preneel, A privacy-preserving buyer seller watermarking protocol based on priced oblivious transfer, IEEE Transactions on Information Forensics and Security, pp. 202–212, 2011.

Conclusion: In this paper, [7] Alfredo Rial, et al. proposed A Privacy-Preserving Buyer-Seller Watermarking Protocol Based on Priced Oblivious Transfer in 2011. In the privacy-preserving buyer-seller watermarking protocol allows copyright protection and in which buyers purchase from sellers without the seller learning the items they buy.

To solve this customer's right problem, the concept of Buyer-Seller Watermarking Protocol accommodating the rights of both the buyer and the seller was introduced. However, all existing solutions that successfully solve this problem rely on the trustworthiness of Watermark Certification Authority (WCA) as a party generating the watermark used in every transaction. Since buyer-seller watermarking protocol was, in the first place, introduced to eliminate the assumption on seller's honesty, a requirement of a new trusted third party is not desirable.

## 2.8 Conclusion

In this way, the authors have explained about the buyer-seller watermarking protocol and the various problems, which is expected to be solved by the buyer-seller watermarking protocol. Further, the authors have given a brief description of earlier proposed solution for buyer-seller watermarking protocol but still some improvement are needed like the watermark which are inserted into the digital content is not as much robust as it should be and the visual quality of the watermark image is also need to be improved.

Hence, authors have proposed some robust methods for embedding and extracting the watermark. After an adequate literature review, authors have identified three problems out of these three problems first two problems are focusing on managing the watermark. Third problem is concerned with how to provide secure communication between buyer and seller; for that author have proposed identity-based (ID) public key cryptography and worked on the cryptosystem.

The author presents solution against these problems indicated above. The first two problems are solved in chapter 3 and 5 in chapter 5 the third problem is solved. He has mainly focused on managing the watermark means authors have worked upon how to make watermark more robust and how the perceptual quality of the watermark image can be improved.

# CHAPTER # 3

## IMPLEMENTATION OF WAVELET-BASED MODIFIED BUYER-SELLER WATERMARKING PROTOCOL (BSWP)

### 3.1 Introduction

The main characteristics of wavelet are wavelets' excellent spatial localization and multi-resolution. Wavelet-based watermarking is a promising technology for embedding the information as an unperceivable signal into the digital contents. Wavelet based modified buyer-seller watermarking protocols [33] integrate multimedia, watermarking techniques, fingerprinting and cryptography for copyright protection, piracy tracing, and privacy protection of the digital content. In this chapter author has implemented the wavelet-based modified buyer-seller watermarking protocol. The protocol focuses on managing the watermark. A binary watermarked image that is a logo is embedded in certain selected sub-bands of a 3-level DWT transformed of the original image. Then, the DWT sub-band is computed and the sequences of the watermark bits are embedded in the coefficients of the high frequency sub-bands. The quality of the watermarked image generated with wavelet-based method is better, using the same watermark strength. To check the imperceptibility and robustness of the watermarked image, PSNR and NCC parameters are used. Furthermore, the algorithm is robust against the various attacks such as JPEG Compression, Rotation, Gaussian Noise, Median Filter and Salt & Pepper Noise.

The wavelet-based modified buyer-seller watermarking protocol is one that combines encryption, digital watermarking, and other techniques to ensure rights protection for both the buyer and the seller in e-commerce. This protocol involves three steps. First, a seller embeds a watermark [32] that identifies the buyer into a digital product, such as a digital image. Second, when a pirated copy is found by the unauthorized person the seller will detect the watermark of the pirated copy. At last, once the watermark of a specific buyer is identified, the seller will take the case to a court. Digital watermarking can be applied in the spatial and transform domains to achieve robustness and imperceptibility. Spatial domain techniques are easier to implement, but lack in robustness, while transforming domain techniques embed the watermark in the host's transform domain, are more sophisticated, robust and getting popularity when compared to spatial domain techniques [34]. The development of spatial domain techniques due to their weakness in robustness is generally not chosen by the researcher and the frequency domain algorithm [35] based on discrete cosine transform (DCT) or discrete wavelet transform (DWT) is the focus of research. There are requirements and constraints in designing effective watermarking algorithms the three fundamental areas are.

Digital watermarking [36] is a promising technology employed by various digital rights management (DRM) systems to achieve digital rights. Wavelet-based watermarking techniques are gaining more popularity because DWT has a number of advantages over other transform such as it contains progressive low bit-rate transmission and quality scalability characteristics. A buyer-seller watermarking protocol is expected to solve the problems in [31, 9, 10].

## 3.2 Discrete Wavelet Transform

Discrete wavelet transforms (DWT) [32] is a signal analytic theory that can localize the signal in spatiotemporal. This theory has already been widely used. The basic idea of applying DWT to the image processing is that by using discrete wavelet transform, the host image can be decomposed into lower frequency sub-band and higher frequency sub-band. Especially, higher frequency components of the images have the self similarity between each frequency component, horizontally, vertically and diagonally. It contains progressive low bit-rate transmission and quality scalability characteristics. The wavelet-based modified buyer seller watermarking protocol to use the robust watermark technique. Wavelets are obtained from a signal prototype wavelet y(t) called mother wavelet by dilations and shifting. Equation (3.2.1) shows the general form of a discrete wavelet transform.

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}}\psi(\frac{t-b}{a}) \qquad \textbf{(3.2.1)}$$

Where a is scaling parameter and b is shifting parameter.

The 1 D discrete wavelet transform is given by the equation no. (3.2.2).

$$\mathrm{W}_{\mathrm{f}}(\mathrm{a,b}) = \int_{-\infty}^{\infty} \mathrm{x(t)}\varphi_{\mathrm{a,b}}\,\mathrm{(t)dt} \qquad \textbf{(3.2.2)}$$

The inverse 1D discrete wavelet transform is given by the equation no. (3.2.3).

$$x(t) = \frac{1}{C}\int_{0}^{\infty} \int_{-\infty}^{\infty} W_{f}(a,b)\varphi_{a,b}(t)db\frac{da}{a^{2}} \qquad \textbf{(3.2.3)}$$

Where

$$\mathrm{C} = \int_{-\infty}^{\infty} \frac{(|\varphi\omega|)^{2}}{\omega}$$

### 3.2.1 Wavelet decomposition

After 3-level wavelet transforms decomposition [32] the original image is decomposed into 10 sub-bands with different resolution and directions as shown in Figure 3.2.1. These sub-bands include one low frequency sub band labeled as LL3 and nine intermediate high frequency sub-bands labeled as LH1-3, HL1-3 and HH1-3. LL3 is selected in this algorithm as locating reference sub-band and LH2, HL2, HH2, LH3, HL3 and HH3 as watermarking embedding sub-bands.

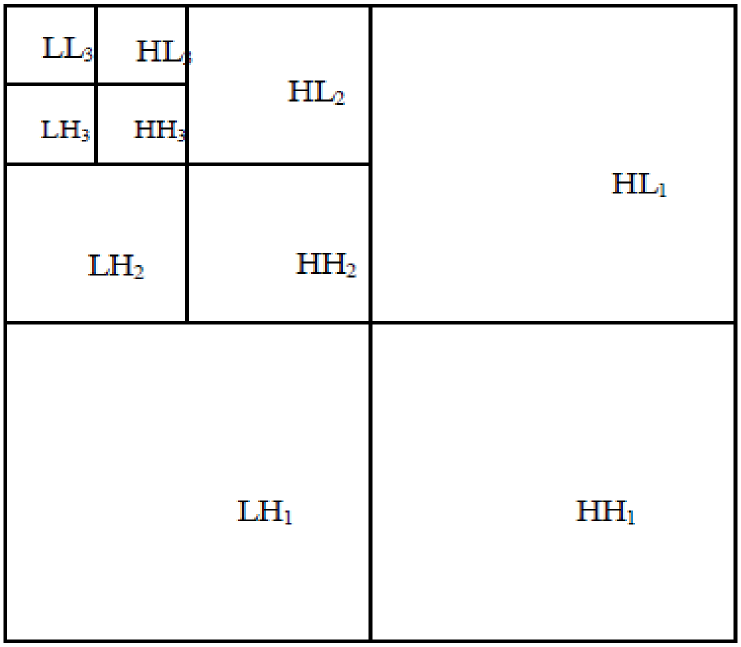


***Figure 3.2.1*** *Sub-band Distribution*

### 3.2.2 Determination of watermarking locations

Watermarking locating is a critical technique [32] of blind watermarking. To accurately detect watermarking, the location of embedding point must be stable. It is required that the feature points should have features preventing against noise image processing and geometric distortion. In Wavelet watermarking, Xia et al. [37] firstly proposed that significant large intermediate frequency coefficients could be chosen as embedding carrier and the locations of these coefficients were locations where watermarking were located at the time of embedding and indexed at the time of extraction. Watermarking can be located by means of recording the watermarking locations when embedding. This method makes high accuracy of watermarking locating and prevents watermarking against noise and image compression and processing which are specially used to attack digital watermarking. However, this kind of algorithm needs large amount of memory. It is apparently impractical because each image requires special memory to record the locations of watermarking. Using a secret key and a special algorithm to create watermarking embedding locations is an effective method. This kind of method can avoid too many memory spending.

Watermarking locates completely meet the requirements of inflexibility. Proposed spatial coordinates relationship between locating reference sub-band (LL3) and embedding sub-bands (LH1-3, HL1-3, HH1-3) is shown in Figure 3.2.2.

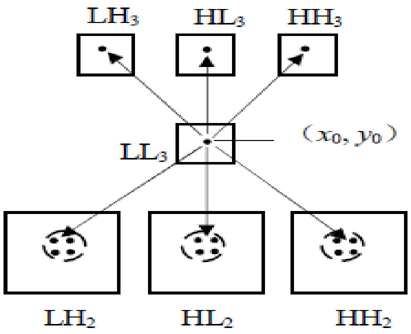


***Figure 3.2.2*** *Spatial coordinates relationship between LL3 and embedding sub-bands.*

## 3.3 Related Work

The possible solution for e-distribution of digital rights is based on a unique watermark for a transaction between seller and buyer. Since its inception in many variants have been proposed. Qiao and Nahrstedt [23] first pointed out the customer's rights problem in the watermarking protocols for piracy tracing. Ramin Eslami and Hayder Radha propose a new image coding scheme based on the proposed transform, the wavelet-based contourlet transform (WBCT) [18]. P. Kumhom et. al.'s proposed method is based on the wavelet packet transformation with the best basis [19] resulting from an entropy-based algorithm.

Author has implemented a wavelet-based modified buyer seller watermarking protocol to fulfill the design requirements, different from the predecessors, his approach makes improvements in the many aspects such as anonymous communication between buyer and seller, and it supports multi-transaction and dispute resolution and avoid double watermark insertion. The protocol is based on public key encryption standard.

## 3.4 Wavelet-Based Modified Buyer-Seller Watermarking Protocol (BSWP)

In this proposed protocol, author has used wavelets to provide more security for the buyer and the seller during the transmission of digital content. The proposed protocol focuses on managing the watermarks author does not design new method but simply use wavelets for embedding the watermarks. The trust model of proposed protocol is same as in [5, 11]. Here, author assures that his protocol is more robust and imperceptible compared to other previous protocols, because it uses wavelet special properties. The WCA device is integrated into the seller's computer system and it will generate the watermark with the help of DWT for the buyer. Author has assumed that every seller in a transaction has unique watermarking embedded function algorithm in their software and all messages are transferred in a secure manner and digital content is still image. Discrete wavelet transforms (DWT) [37, 38, and 39] is a signal analytic theory that can localize the signal in spatiotemporal.

Author has modified the existing algorithm proposed by Corina Nafornita [40] for embedding the watermarks the algorithms used to embed the watermark in the high frequency sub-bands i.e. HL, LH and HH because they show better results in terms of imperceptibility. In this approach author has chosen high frequency selected sub-bands i.e. HL and LH this reduces the area of embedding the watermark leads in great robustness, imperceptibility and minimize the effect of various attacks. Author has compared his approach with Corina Nafornita [40] and shows that the approach contains better result. Embedding of the watermark multiple times into the host image makes the scheme more robust.

### 3.4.1 Watermark Embedding Scheme

Let I be the original gray-level image and the watermark W an original watermark image. He starts the watermarking process by applying 3-level DWT to the original image. However, in this chapter, he embed the watermark into high frequency selected sub-bands i.e. HL and LH this reduces the area of embedding the watermark leads in great robustness as well. The watermark is repeatedly embedded of M >>1 times in the transform image. Since the watermark is embedded multiple times in every detail sub-band, this can be viewed as a form of transmitting the watermark in different sub-channels. It has been shown by Kundur et al [41]. In those diversity techniques can give very good results in detecting the watermark because that many watermark attacks are more appropriately modeled as fading like. Each repetition is denoted by $W_r$ with r = 1, 2, up to M. Figure 3.4.1 shows the flow chart of his proposed watermark embedding procedure. The basic steps for embedding the watermark are given below.

**Step 1:** Perform 3-level DWT to the original image I. The original image is decomposed into four sub domains as HH,HL,LH,LL for 1-level DWT according to different frequency of the original image.

$$Y = DWT\,(I) = \{LL_L, HL_L, LH_L, HH_L, HL_{L-1}, .., HH_1\}$$

**Step 2:** Select HL3 and LH3 high frequency sub-bands of the original image I for embedding the watermark.

**Step 3:** Compute the threshold for each selected sub-band HL3 and LH3. Let the approximation coefficients be a(m,,n) and the detail coefficients from the resolution level l and sub-band s be $d_{s,l}(m,n)$, where s Є {HL, LH} and l Є {1,…,L}. The threshold is computed using equation no. (3.4.1).

$$T_{s,l} = q_1 \max_{m,n}\{d_{s,l}(m.n)\} \qquad \textbf{(3.4.1)}$$

**Step 4:** Let W of size 128×128 an original watermark image after applying 3-level DWT he gets HL3 and LH3 high frequency sub-bands. For each sub-band that is HL3, LH3, if the detail coefficient is higher or equal to the above computed threshold, embed the watermark using the equation no. (3.4.2)

$$d^{w}_{s,l}(m,n) = d_{s,l}(m,n)[1+\alpha w_{r}(i)] \qquad \textbf{(3.4.2)}$$

Where α is a parameter used to control the level of the watermark.

**Step 5:** Repeat previous step M times, until every selected coefficient has been watermarked.

**Step 6:** Compute the IDWT from these new coefficients. He obtains the watermarked imageIw.

**Step 7:** Reshaping the decomposed image back to its normal dimension.

**Step 8:** Write the watermarked image to a file and display it.

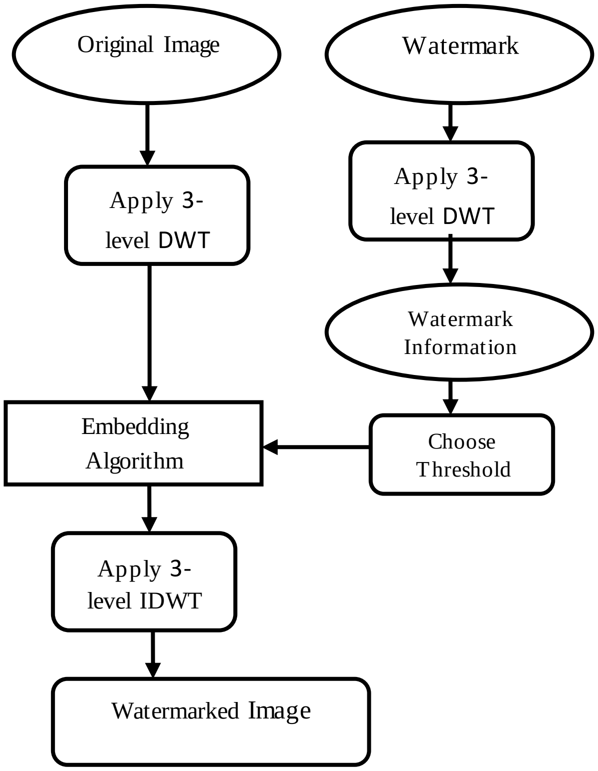


***Figure 3.4.1*** *DWT watermark embedding procedure.*

### 3.4.2 Watermark Extraction Scheme

The extraction process requires the original image I, or at least some significant vector extracted from the DWT of the cover work, specifically, the detail coefficients with a value above the computed threshold. Figure 3.4.2 shows the watermark extraction procedure. The basic steps for extracting the watermark are given below.

**Step 1:** Perform 3-level DWT on the watermarked imageIw to decompose it into four non-overlapping multi-resolution coefficient sets: LL3, HL3, LH3 and HH3.

**Step2:** Select HL3 and LH3 high frequency selective sub-bands of the watermarked imageIw.

**Step3:** Determine the size of the wavelet coefficients $d_{s,l}(m,n)$.

**Step4:** The estimate of each repetition of the watermark W from the watermarked and possibly distorted work $I^{w}$ is extracted using the wavelet coefficients $d_{s,l}(m,n)$ that should contain a watermark bit.

$$w_r(i) = \text{sgn}\left(\frac{d^{\wedge}{}_{s,l}(m,n) - d_{s,l}(m,n)}{d_{s,l}(m,n)}\right) \qquad \textbf{(3.4.3)}$$

The random guess is made, for the watermarked bit in the location (m,n) if $d^{\wedge}{}_{s,l}(m,n) = d_{s,l}(m,n)$ or if $d_{s,l}(m,n)= 0$.

**Step 5:** The original watermark is estimated from its repetitions using the majority rule i.e. the most common bit value is assigned for the recovered watermark bit.

**Step 6:** The watermark is reconstructed using the extracted watermark bits.

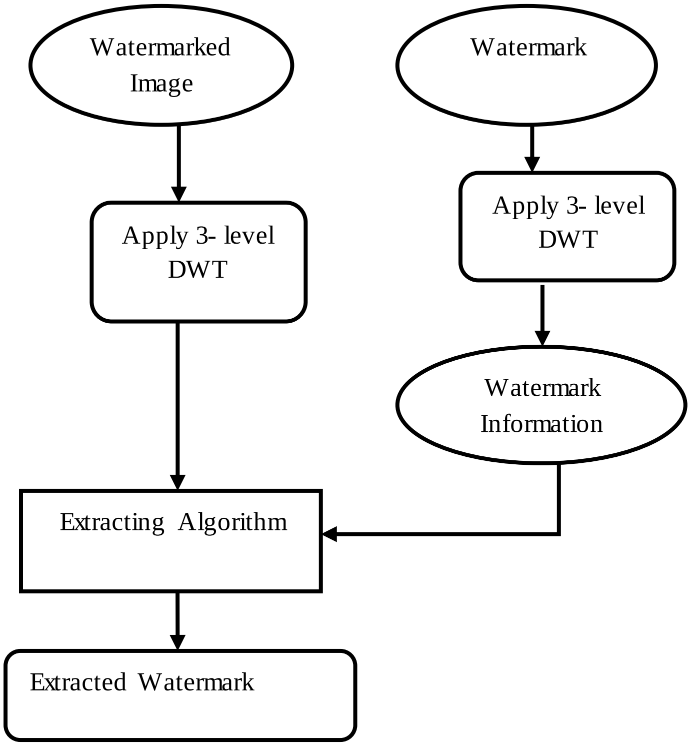


***Figure 3.4.2*** *DWT watermark extraction procedure.*

## 3.5 Result Analysis

In this section, author has given the various parameters through which he can analyze the performance of the protocol. These parameters are PSNR, MSE and NC measurements.

### 3.5.1 Peak Signal-To-Noise Ratio (PSNR)

Peak Signal-To-Noise Ratio is generally used to analyze quality of image. For that, he has used equation no. (3.5.1) and (3.5.2).

$$\text{PSNR} = 10 * \log \frac{255^2}{\text{MSE}} \qquad \textbf{(3.5.1)}$$

### 3.5.2 Mean Square Error (MSE)

The MSE represents the cumulative squared error between the compressed image and the original image. To compute the PSNR, first calculates the mean-squared error (MSE) using the following equation:

$$\mathrm{MSE} = \sum_{i=1}^{x} \sum_{j=1}^{y} \frac{(|A_{i,j} - B_{i,j}|)^2}{x * y} \qquad \textbf{(3.5.2)}$$

Where x is width of the image and $y$ is height and $x * y$ is the no. of pixels.

### 3.5.3 Normalized Correlation Coefficient (NCC)

Normalized Correlation Coefficient is used for evaluating the robustness of the algorithm. For m × n greyscale image, the NC is defined as follow:

$$\mathrm{NC} = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} A_{i,j} B_{i,j}}{\sum_{i=1}^{m} \sum_{j=1}^{n} A_{ij}^{2}} \qquad \textbf{(3.5.3)}$$

Where $A_{i,j}$ and $B_{i,j}$ denote the pixel values in row i and line j of the original watermark and the exacted watermark respectively.

Here author has shown the various results of wavelet-based modified buyer seller watermarking protocol. From the previous section [40] the details of the image such as edges and textures are well confined into the HH, LH, and HL sub-bands of the DWT of the image. He chose only HL3 and LH3 sub-bands of the image of the watermarking process. The DWT-based algorithm is tested for the various original and watermark images. The test set comprises various test images in which some images have been taken from the standard grayscale image dataset [http://decsai.ugr.es/cvg/CG/base.htm] and well-known images Lena, Cameraman, Baboon and House, respectively. Some results are given to evaluate the performance of the method. Author has calculated PSNR and NCC values for that. The images Lena, Cameramen, Baboon and House are presented in Figure 3.5.1. The presented method is implemented using MATLAB.

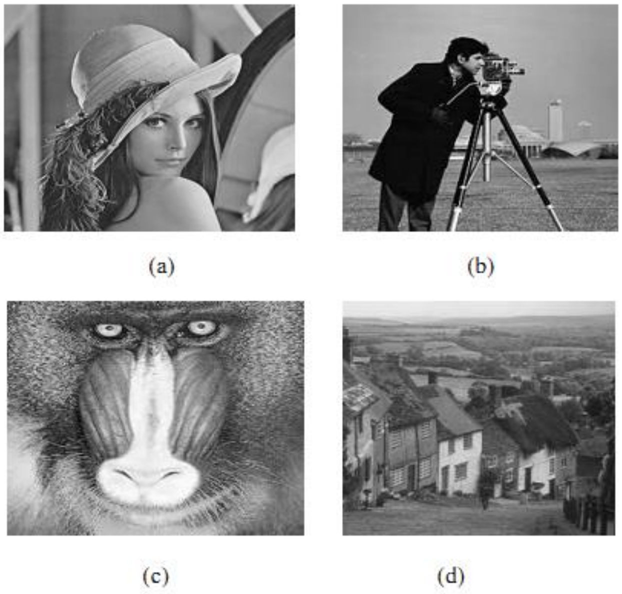


***Figure 3.5.1*** *Original images used for simulations: Lena (a), Cameramen (b), Baboon (c) and House (d).*

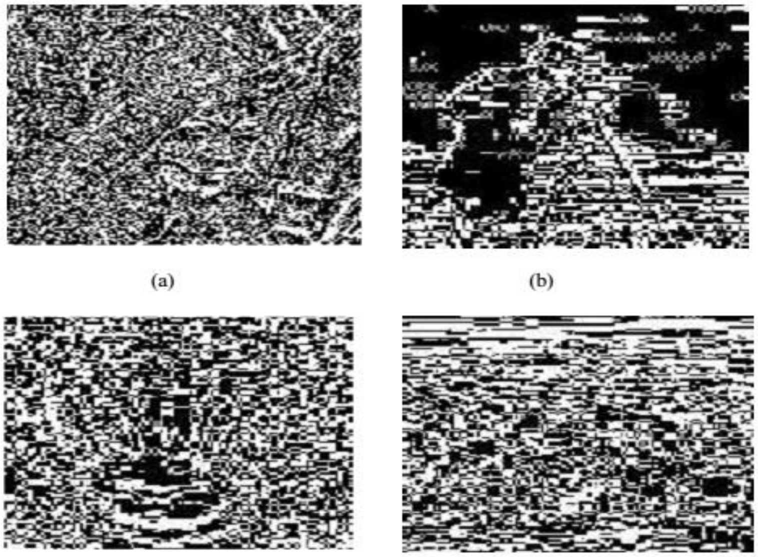
The watermark was an original binary gray scale JUIT logo. The Daubechies 10pt wavelet was used to produce the wavelet coefficients. The following parameters were used, number of resolution levels L = 3, the strength of the watermark α = 0.1, and he chose only HL3 and LH3 high frequency sub-bands for embedding the watermark. The performances of the protocol [40] are compared with the results of the method proposed by Cox in [42]. The watermarked images using the proposed protocol were not significantly distorted from the originals, whereas for the method presented by Cox et al. the difference was clearly visible, even upsetting. Table 3.5.1 contains the values of PSNR for each image and used watermark embedding coefficient α= 0.01.

**Table 3.5.1 shows PSNR [dB] values as a measure of the noise introduced by the watermark.**

| PSNR<br>Image | Our Method | C. Nafornita' Method | Cox's Method |
|---|---|---|---|
| Lena | 46.33dB | 45.39dB | 27.19 dB |
| Cameraman | 44.55 dB | 43.35 dB | 25.35 dB |
| Baboon | 45.39dB | 44.18dB | 26.44 dB |
| House | 45.67 dB | 45.35 dB | 25.75 dB |

**Table 3.5.1**

From the Table 3.5.1, one can see that the performance of the proposed algorithm i.e. wavelet-based buyer seller watermarking protocol, is better than pervious Cox's method [42] and C. Nafornita' method [40]. The difference between the watermarked and the original image is presented in Figure 3.5.2 (a) to (d). From the difference images, it is clear that the watermark was embedded in the edges and textures. For instance, for the Lena image, the watermark affects the details such as the feathers of the hat. It has been demonstrated on four different images that the watermarking process has clearly not affected their visual quality.

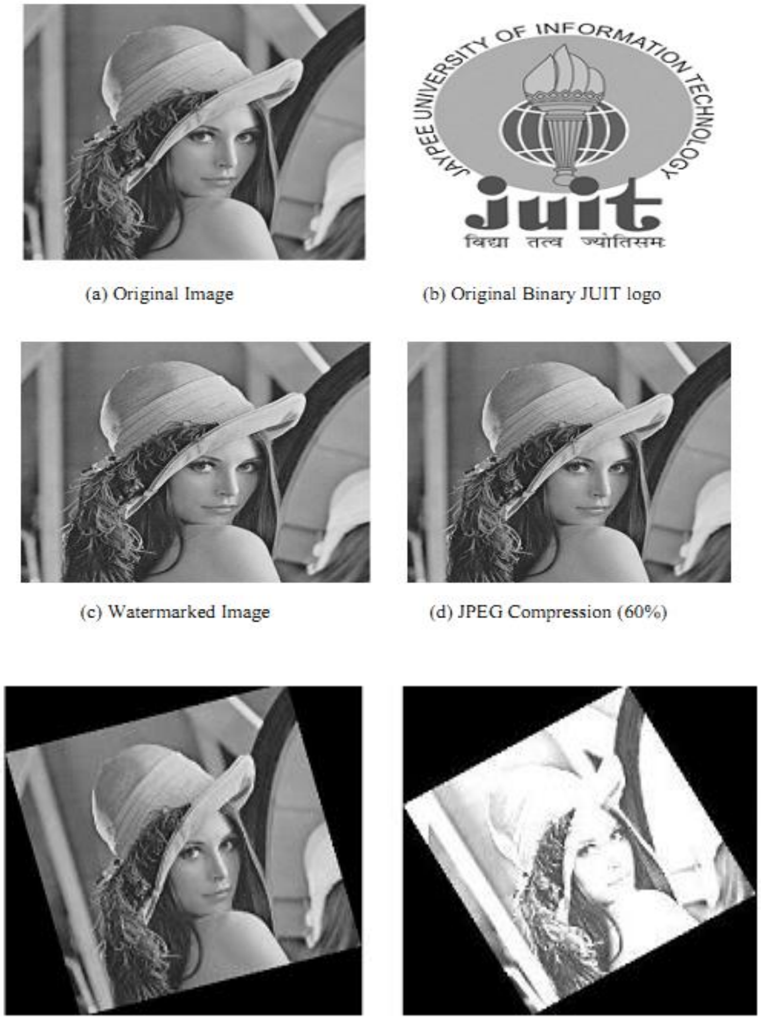


(a) (b)

(c) (d)

***Figure 3.5.2*** *Difference images between watermarked image and original image, for Lena (a), Cameraman (b), Baboon (c), and House (d).*

Author has given the results of his method against the various types of attacks. He has compared his result with the results of the method proposed by Ben Wang in [43]. For instance, here author has taken only the Lena image for producing his result. Therefore, author has taken of 512 × 512 8bit grayscale image Lena image and 128 × 128 8-bit grayscale watermark original binary JUIT logo. The embedding coefficient α= 0.01. The robustness is tested under 5 types of attacks i.e. JPEG Compression, Rotation, Gaussian noise, Salt & Peeper noise and median filter. The images with attacks are shown in Figure 3.5.3.



(a) Original Image

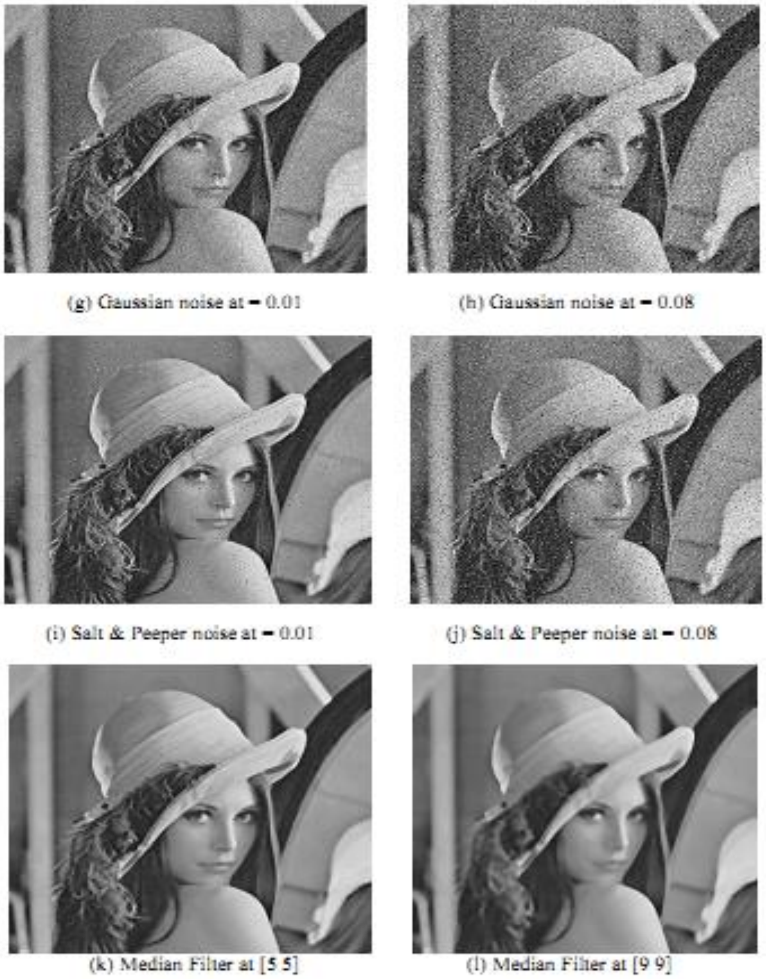
(b) Original Binary JUIT logo

(c) Watermarked Image

(d) JPEG Compression (60%)

(e) Rotation (30°)

(f) Rotation (60°)



(g) Gaussian noise at = 0.01

(h) Gaussian noise at = 0.08

(i) Salt & Peeper noise at = 0.01

(j) Salt & Peeper noise at = 0.08

(k) Median Filter at [5 5]

(l) Median Filter at [9 9]

***Figure 3.5.3*** *Images with various types of attacks.*

The watermarks extracted from the images above are shown correspondingly in Figure 3.5.4.

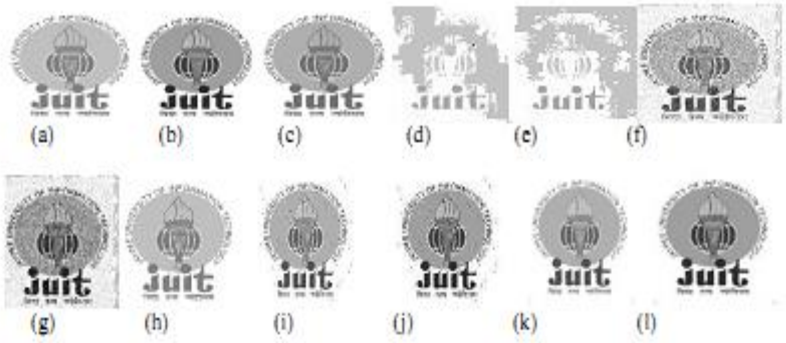
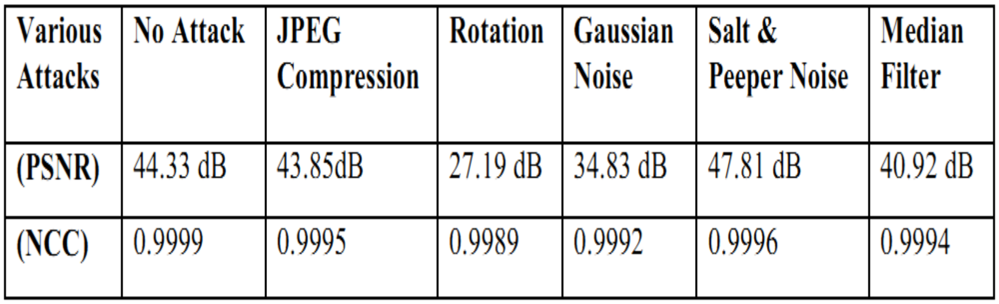


***Figure 3.5.4*** *Watermarks extracted from the attacked Images.*

Table 3.5.2 shows the corresponding PSNR and NCC measurement of wavelet-based modified buyer-seller watermarking protocol.

**Table 3.5.2 The corresponding PSNR and NCC values of the algorithms.**



| Various Attacks | No Attack | JPEG Compression | Rotation | Gaussian Noise | Salt & Peeper Noise | Median Filter |
|---|---|---|---|---|---|---|
| (PSNR) | 44.33 dB | 43.85dB | 27.19 dB | 34.83 dB | 47.81 dB | 40.92 dB |
| (NCC) | 0.9999 | 0.9995 | 0.9989 | 0.9992 | 0.9996 | 0.9994 |

**Table 3.5.2**

The Table 3.5.2 shows that the algorithm has great robustness against the various types of attacks. Figure 3.5.5 to 3.4.10 shows the detector's response to the watermarked Lena image under several types of attacks, which is very similar to Cox [42] and C. Nafornita [40] results. Author has compared [40, 42] with his buyer seller watermarking protocol (BSWP) on the same set of test data. If he set the threshold value in the detection process at 0.5 he has the followings.

**Median filter attack:** For Lena watermarked images, the attack by median filtering with filter size larger than M=5 leads to a correlation smaller than 0.7. When author increases filter size M=9 leads a correlation smaller than 0.6. In fact only the detector C. Nafornita allows filtering with filter size M=5.

**Gaussian Noise:** For Lena watermarked images, the attack by Gaussian noise at=.01. The correlation coefficient is smaller than 0.7 when compared to detector response C. Nafornita and Cox. When he applies Gaussian noise attack at=.08 leads correlation coefficient is smaller than 0.5.

**Salt & Peeper Noise:** For Lena watermarked images, the attack by salt & peeper noise at=.01. The detector response in the BSWP method is above 0.5, having a considerably better performance than the detectors C. Nafornita and Cox et al. method. When he apply salt & peeper noise attack at=.08 the performance of his method is less than 0.5 but better when compared to other two methods.

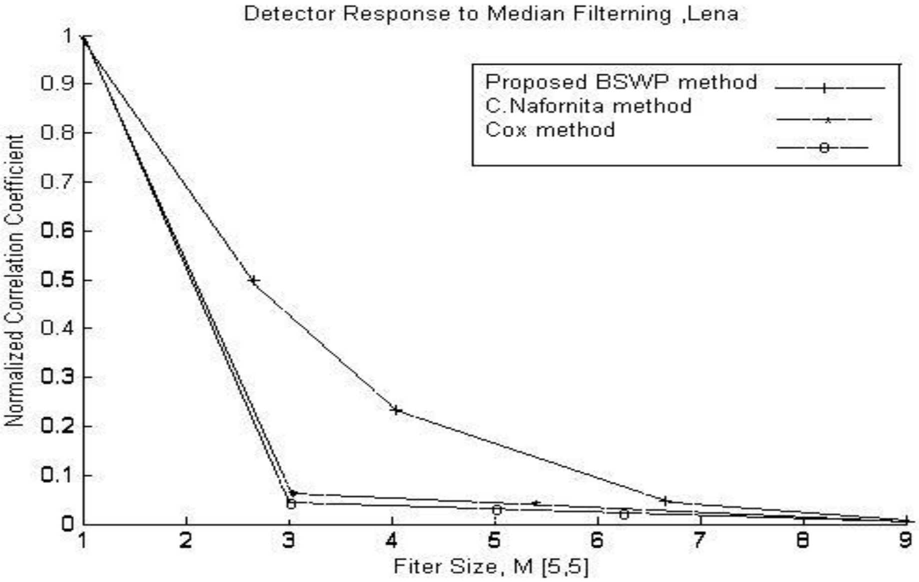


***Figure 3.5.5*** *The detector response's to the watermarked Lena image under median filtering attack when filter size m=5.*

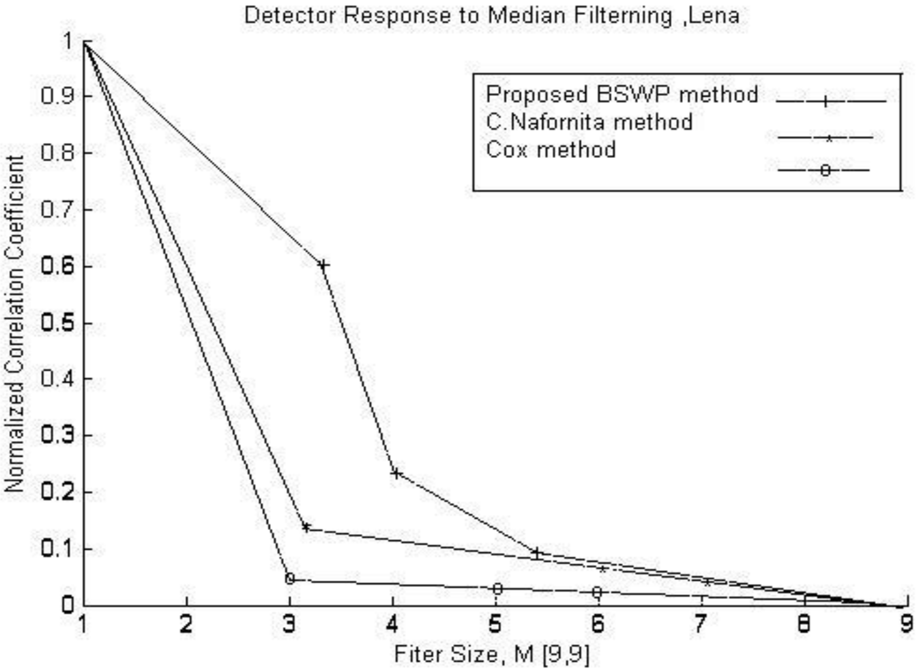


***Figure 3.5.6*** *The detector response's to the watermarked Lena image under median filtering attack when filter size m=9.*

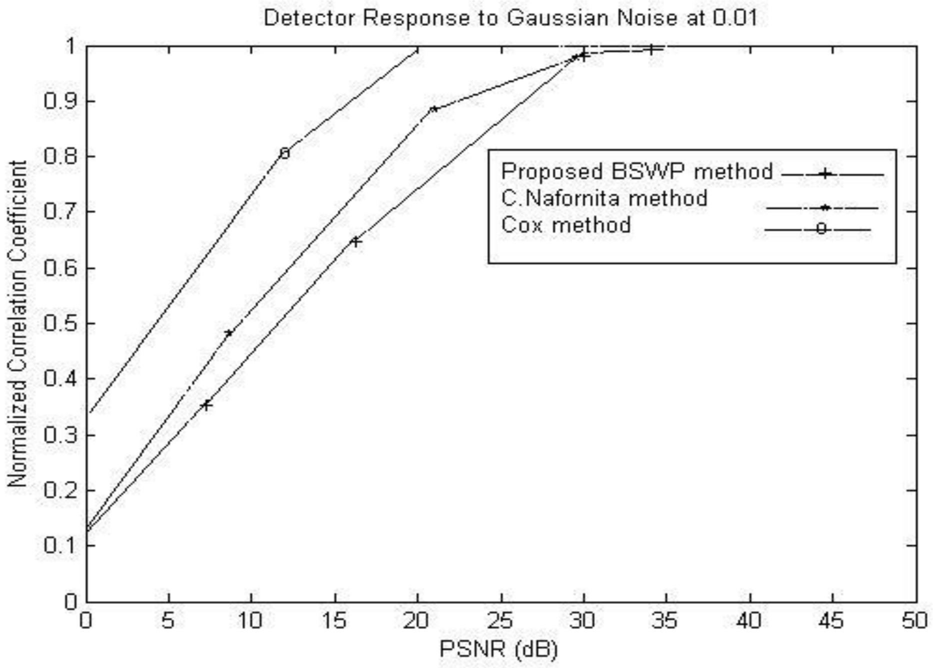


***Figure 3.5.7*** *The detector response's to the watermarked Lena image under Gaussian noise at=0.01.*

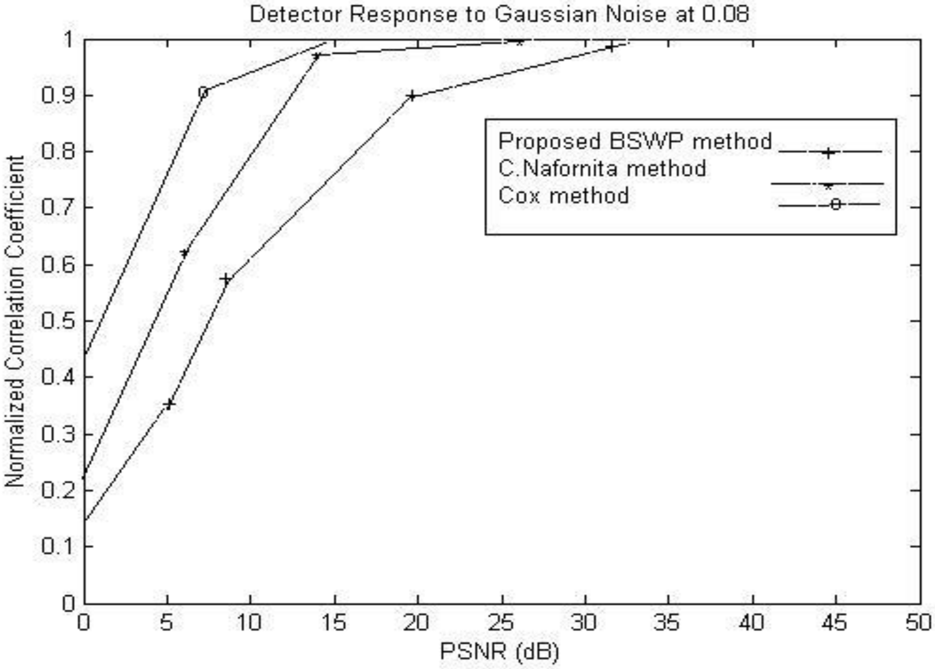


***Figure 3.5.8*** *The detector response's to the watermarked Lena image under Gaussian noise at=0.08.*

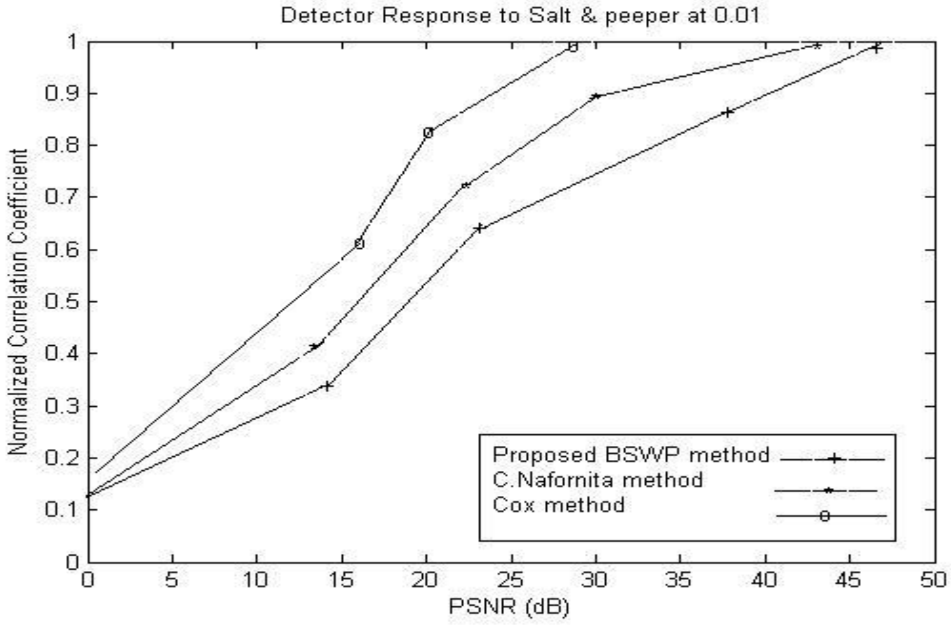


***Figure 3.5.9*** *The detector response's to the watermarked Lena image under Salt & peeper noise at=0.01.*

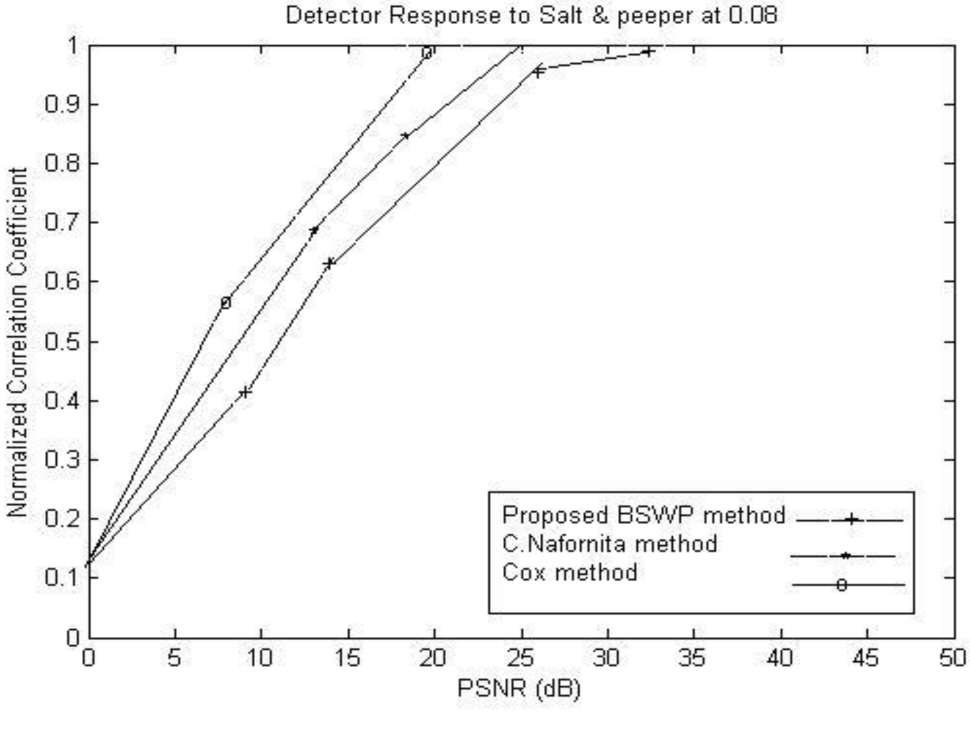


***Figure 3.5.10*** *The detector response's to the watermarked Lena image under Salt & peeper noise at=0.08.*

## 3.6 Conclusion

In this chapter, a wavelet-based modified buyer-seller watermarking protocol (BSWP) is implemented. DWT may have a positive impact on the performance of the watermarking system. The protocol focuses on managing the watermarks he does not design new method but simply use wavelets for embedding the watermarks. In this watermarking is done by embedding the watermark in the special high frequency selective sub-bands of 3-levels DWT transformed of an original image. The security of this protocol is depending upon the embedding and extraction of watermark.

The contribution toward this research is published and is as follows:

**[1]** Ashwani Kumar, S.P. Ghrera, and Vipin Tyagi, "Implementation of Wavelet-Based Modified Buyer-Seller Watermarking Protocol," WSEAS Transactions on Signal Processing, Vol. 10, pp. 212-220, April 2014. [SCOPUS indexed]. http://www.wseas.org/multimedia/journals/signal/2014/a025714-226.pdf

# CHAPTER # 4

## MODIFIED BUYER-SELLER WATERMARKING PROTOCOL (MBSWP) BASED ON DISCRE WAVELET TRAFORM (DWT) AND PRINCIPAL COMPONENT ANALYSIS (PCA)

### 4.1 Introduction

The speedy development of internet and e-commerce needs a copyright protection mechanism for multimedia data. Straight off a day's digital watermarking becomes an important technique for protecting the digital rights [44]. This hidden data can later be extracted to prove the ownership of the digital content [2, 3]. With the increasing role of the internet, there is always a need to protect the multimedia data over the web. Information hiding in still images has two main applications such as fingerprinting and copyright protection. But important aspects of digital watermarking systems include imperceptibility, robustness, capacity, and security of the embedding and extracting process. Digital watermarking [4, 11, 34, 36, 42] techniques use encrypted domain for embedding and extracting the watermarks. The rapidly growing of the internet encourages some bad usage too, like operations such as transformation, duplication, and redistribution of digital content. With the avail of some software tools, one can easily identify these bad users and redistribution of digital content can be placed. In the proposed protocol seller is responsible to embed a watermark [32] that identifies the buyer into a digital content.

The first PCA domain was introduced to gray-scale image watermarking [45]. Lai et al. [46] suggested a hybrid DWT-SVD watermarking procedure in which two halves of the watermark image is embedded into the two singular value matrices of intermediate frequency sub-bands obtained while taking one level DWT of host image. After embedding the watermark, the two halves are combined to get the watermarked image. Principal Component Analysis (PCA) [9, 10, 47] is often applied to subdue a large number of variables to a smaller set of their linear combinations that adequately identify the arrangement. The primary advantage of using PCA transform is to choose the suitable significant components into which one can embed the watermark.

In this chapter, author presents a modified buyer seller watermarking protocol, which uses DWT and PCA. Proposed protocol focuses on managing the watermark.

## 4.2 Related Work

One of the solutions for distribution of digital rights is based on a unique watermark for every transaction between vendor and purchaser. PCA [44] based watermarking algorithms, the early researching work conducted by Wang [47] who embedded watermarks into the PCA coefficients of the static image without degrading their visual quality. Most of the PCA based watermarking methods were done in projection space.

In this chapter, author has demonstrated a modified buyer-seller watermarking protocol based on DWT and PCA with vector quantization to fulfill the design requirements, unlike from the predecessors, his approach makes improvements in the many aspects such as anonymous communication between buyer and vendor. The watermarking scheme for embedding and extracting the watermarks is more robust and imperceptible because it uses a hybrid technique.

## 4.3 DWT and PCA Transform

In this section, authors have discussed Discrete Wavelet Transform and Principal Component Analysis for images.

### 4.3.1 Discrete Wavelet Transform

Discrete wavelet transforms (DWT) [32] is a signal analytic theory that can localize the signal in spatiotemporal. This theory has already been widely used. The basic thought of applying DWT [37, 38, and 48] to the image processing is that by using discrete wavelet transform, the host image can be decomposed into lower frequency sub-band and higher frequency sub-bands. Especially, higher frequency portions of the images hold the self similarity between each frequency component, horizontally, vertically and diagonally. This self-similarity can be derived from the correlation coefficients between lower frequency components and their similar high frequency components.

The main advantage of the wavelet transforms [49] is its compatibility with a human vision system model as compared to the fast fourier transform (FFT) or discrete cosine transform (DCT) transform. This permits to use higher energy watermark in those areas in which the HVS is known to be less sensitive such as high resolution detail sub-bands. Inserting the watermarks bit in these regions allow us to increase the robustness of the watermark without any visible effect on the image quality.

### 4.3.2 Principal Component Analysis (PCA)

Principal Component Analysis (PCA) is likewise known as Karhunen Loeve (KL) Transform in pattern recognition & as factor or principal component analysis in the literature. Principal component analysis has been called one of the valuable results from applied linear algebra. PCA provides a roadmap in order to explain how to bring down complex data sets to a lower dimension to reveal the sometimes hidden simplified structure that often underlie it. In Yavuz [50] a reference image is generated from the cover image using PCA [51] and the watermark is embedded according to the difference between the image and its reference image.

PCA is an orthogonal transformation of the coordinate system in which one can describe the datasets. The new coordinate values by which one can represent out dataset are called principal components or simply PCs.

## 4.4 Modified buyer-seller watermarking protocol based on DWT and PCA

The proposed protocol uses wavelets and PCs for embedding and extracting watermark from the original digital content. Author has used the same trust model as it is used by [10, 11]. The approach inserted watermark information into the maximum coefficient of the PCA block this leads in great robustness. In the algorithm a watermark image i.e. a baby image is inserted into selected high frequency bands of discrete wavelet transform. After that, he has applied Principal Component Analysis (PCA) [52] on these high frequency wavelet coefficients and stored the mean (Ai) and covariance (Ci) of the data onto the first principal component called PCs. After applying principal component analysis (PCA) transformation author has chosen blocks for embedding the watermark. Now he select only those blocks which contain maximum energy. Then the watermark bits is inserting only into the maximum coefficient of the PCA block. The extraction procedure of the watermark is same as embed the watermark.

**Algorithm 1: Watermark embedding scheme**

**Input :** The original color image I of size 512 × 512 and the watermark image W of 128 × 128.

**Output:** Watermarked color image I' of size 128 × 128.

**Step 1:** Apply DWT to the original color image I. This results in four multi-resolution sub-bands: $HH_1$,$HL_1$,$LH_1$,$LL_1$. For every sub-band apply DWT again to get 16 sub-bands.

**Step 2:** Select $HL_3$,$LH_3$ high frequency sub-bands of the original color image I.

**Step 3:** Compute the energy of each sub-band using the following equation no. (4.4.1):

$$E_r = \frac{1}{n \times n} \sum_{i=1}^{n} \sum_{j=1}^{n} C^2(i, j) \qquad \textbf{(4.4.1)}$$

Where $E_r$ denotes the energy, n × n is the size of sub-band, and *C* is the wavelet coefficient.

**Step 4:** Select only maximum energy blocks, which are the edges and texture blocks of the image. Then author has apply PCA to each selected block as described.

1. When author gets the block zero mean Zi as below:

$$Z_i = E(B_{si} - M_i) \qquad \textbf{(4.4.2)}$$

2. He calculate the covariance matrix Ci by equation no. (4.4.3) of the zero mean blocks $Z_i$ as:

$$C_i = Z_i \times Z_i^T \qquad \textbf{(4.4.3)}$$

Where *T* denotes the transpose matrix

3. Then he has calculated the PCA transformation of every block by using equation no. (4.4.4):

$$X_i = \phi^T Z_i \qquad \textbf{(4.4.4)}$$

Where $X_i$ is the principal component PCs of the blocks and ф is the matrix of eigenvectors.

**Step 5:** The watermark bits are embedded with strength α into maximum coefficient Mi of each principal component PCs block Xi. For embedding the watermark author uses equation no. (4.4.5):

$$M_i = M'_i \pm \alpha W \qquad \textbf{(4.4.5)}$$

Where α is the watermark strength factor.

**Step 6:** Apply inverse PCA on the modified PCs blocks for obtaining the modified wavelet block by using equation no. (4.4.6):

$$Z_i = \phi \; X_i \qquad \textbf{(4.4.6)}$$

**Step 7:** Apply the IDWT to get the new watermarked coefficient. Finally reconstruct the watermarked color image from these new coefficients.

**Algorithm 2: Watermark extracting scheme**

**Input :** The watermark color image I' of size 512 × 512 and watermark W of 128 × 128.

**Output :** The extracted watermarked color image W′ of size 128 × 128.

**Step 1:** Apply DWT on the watermarked image I' to decompose it into four non-overlapping multi-resolution coefficient sets: LL3, HL3, LH3 and HH3.

**Step 2:** Select $HL_3$,$LH_3$ high frequency sub-bands of the watermarked image I'.

**Step 3:** For each block compute the energy Er then select only the maximum energy blocks.

**Step 4:** Then extract the watermark W′ by applying the equation no. (4.4.7):

$$W^{'} = \frac{M^{'}_{i} - M_{i}}{\alpha} \qquad \textbf{(4.4.7)}$$

**Step 5:** Then the detected watermark is compared with the original watermark by calculating the similarity measure between them by equation no. (4.4.8):

$$NC = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} W(i,j).W^{'}(i,j)}{\sum_{i=1}^{m} \sum_{j=1}^{n} W(i,j)^{2}} \qquad \textbf{(4.4.8)}$$

Where NC is the normalized correlation coefficient.

## 4.5 Results and Security Analysis

These parameters are PSNR, MSE and NC measurements.

### 4.5.1 Peak Signal-To-Noise Ratio (PSNR)

PSNR is used to calculate the distortion between the watermarked image and original image. For that, author has used equation no. (4.5.1) and (4.5.2).

$$\mathrm{PSNR} = 10 * \log \frac{255^2}{\mathrm{MSE}} \qquad \textbf{(4.5.1)}$$

### 4.5.2 Mean Square Error (MSE)

The MSE represents the cumulative squared error between the compressed image and the original image. To calculate the PSNR, first calculates the mean-squared error (MSE) using the next equation:

$$\text{MSE} = \sum_{i=1}^{x} \sum_{j=1}^{y} \frac{(|A_{i,j}-B_{i,j}|)^{2}}{x*y} \qquad \textbf{(4.5.2)}$$

Where x and y is the width, height of the image and $x * y$ is the no. of pixels.

### 4.5.3 Normalized Correlation Coefficient (NCC)

NCC is used to calculating the robustness of the embedding scheme. NCC is defined by equation no. (4.4.8).

## 4.6 Result Analysis

In this section, author has demonstrated the results of the proposed protocol based on DWT and PCA. Most of the details of the image [40] such as edges and textures are found into the high frequency bands of the DWT of the image. First, author decomposed the image up to 3 levels, select only HL3 and LH3 sub-bands of the DWT image, then watermark is embedded in the principal components of the high frequency wavelet coefficients. The test set comprises images from standard color image dataset [http://graphics.cs.williams.edu/data/images.xml], as well as well-known images such as Lena, peppers, Baboon and fruit. Author has calculated PSNR and NCC values for that. Author has used standard test images database of Lena, Peppers, Baboon, and Fruits of size 512 × 512 each are shown in Figure 4.6.1 (a-d) and corresponding watermark image are shown in Figure 4.6.1 (e-h). The color watermark was a baby image of different sizes.

Author has taken the gray-scale watermark of size 256 × 256. This watermark is embedded into Lena, Peppers, Baboon, and Fruits images respectively. The presented method is implemented using MATLAB. Form 4.6.1 (e-h) shows the resultant watermarked images and corresponding PSNR values are presented in Table 4.6.1. Author has compared his results with Run et al. [53], Lai et al. [46], Bhatnagar et al. [54], and Ahahmad et al. [55].

In Figure 4.6.1, one can see no perceptual degradation is observed between the original and watermarked images according to HVS [44]. Figure 4.6.2 shows the original watermark, extracted watermark and binary watermark. For every quaternion PCA coefficient there is real and imaginary components so the color watermark image can also be embedded into the original images.

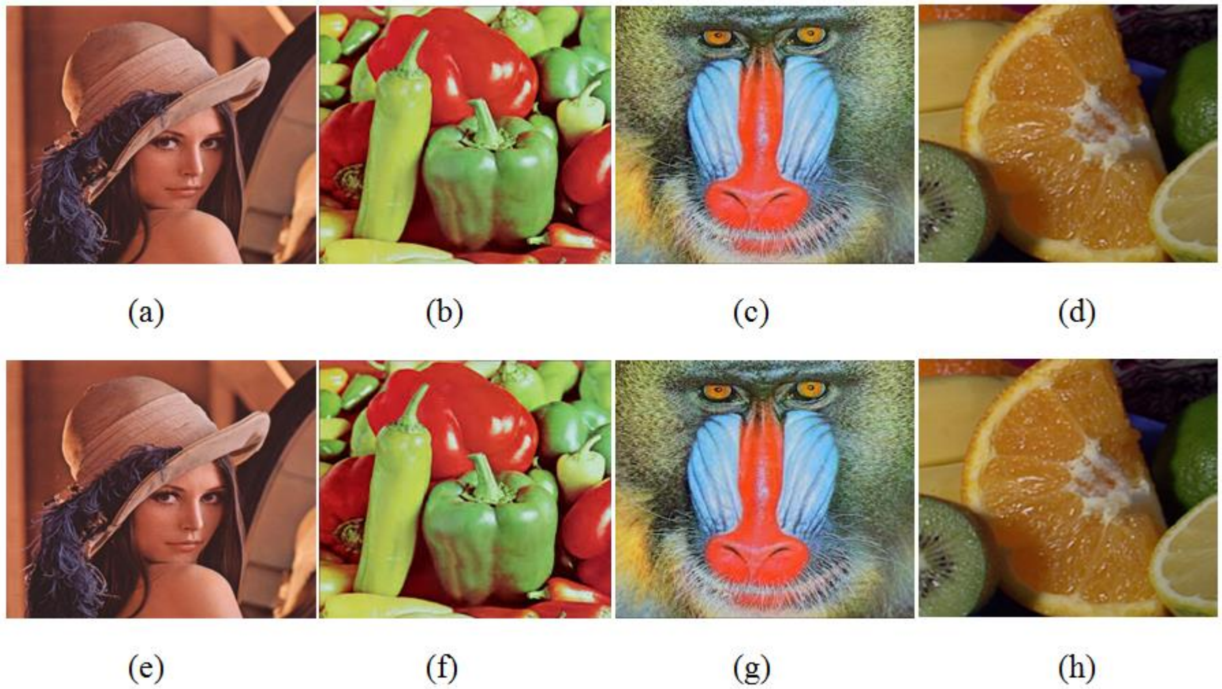


***Figure 4.6.1*** *(a) Lena (b) Peppers (c) Baboon (d) Fruits (e) Watermarked Lena (f) Watermarked Peppers (g) Watermarked Baboon (h) Watermarked Fruits*

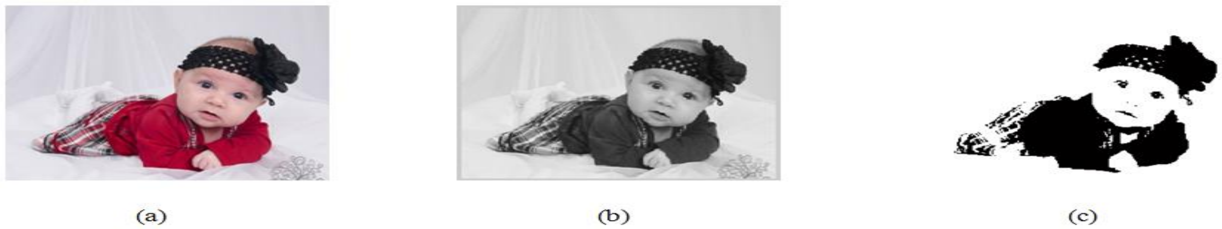


***Figure 4.6.2*** *(a) Original watermark (b) Extracted watermark (c) Binary watermark*

**Table 4.6.1 Peak signal to noise ratio (PSNR) dB for each original color image.**

| Test color images | Lena | Peppers | Baboon | Fruits |
|---|---|---|---|---|
| PSNR | 43.59 | 41.68 | 39.25 | 38.57 |

However, in this author has only use the gray-scale watermarks image to present the validity of the watermark embedding and extracting scheme. Figure 4.6.3 shows the extracted watermark from all images, i.e., (Figure 4.6.3 (a-d)) when no attacks were applied.

***Figure 4.6.3*** *(a-d) Extracted watermark when no attacks were applied.*

To assess the validity of embedding algorithm watermarked image was affected by different type of attacks such as Salt & Pepper Noise, Compression, Median Filter, Rotation, and Gaussian Noise. Figure 4.6.4 represents the attacked image by JPEG compression at different values. Author has taken Lena test images for compression and he selects the compression ratio 50% and 30% for extracting the watermark. It is shown that using the approach, the watermarks can be easily extracted.

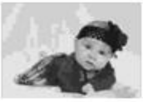
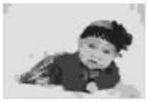
| Attack | JPEG Compression (50%) | JPEG Compression (40%) | JPEG Compression (30%) |
|---|---|---|---|
| Attacked Image | <br>PSNR = 43.59dB | <br>PSNR = 39.62dB | <br>PSNR = 34.28dB |
| Extracted Watermark | <br>NC= 0.9645 | <br>NC= 0.8625 | <br>NC= 0.7129 |

***Figure 4.6.4*** *JPEG compression attacks at quality factor 50, 40, and 30*

Figure 4.6.5 & 4.6.6 shows the test images of Lena, and fruits against rotation attacks. For rotation three different angles are used, i.e., 50°, 65°, and 75°, then author has extracted the watermark from the watermarked images. These watermarks are shown in figure 4.6.5 & 4.6.5 and can be easily recognized by human eyes or by human vision system (HVS).

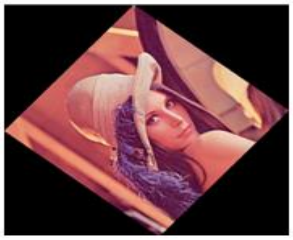
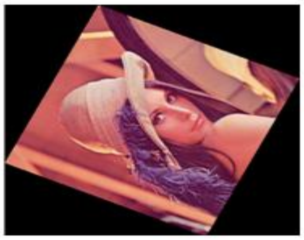
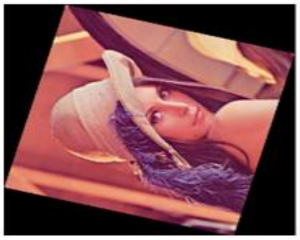
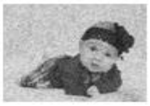
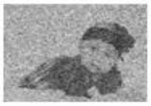
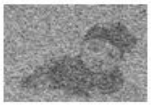
| Attack | Rotation Transform with Rotation Angel 50° | Rotation Transform with Rotation Angel 65° | Rotation Transform with Rotation Angel 75° |
|---|---|---|---|
| Attacked Image | <br>PSNR = 35.11dB | <br>PSNR = 33.71dB | <br>PSNR = 31.34dB |
| Extracted Watermark | <br>NC= 0.8325 | <br>NC=0.6129 | <br>NC= 0.4876 |

***Figure 4.6.5*** *Rotation Transform attack with rotation angle* 50°, 65°, and 75° *for Lena.*

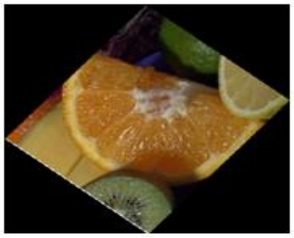
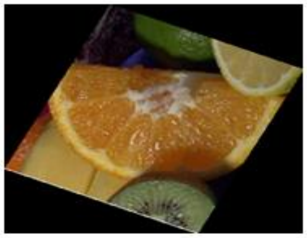
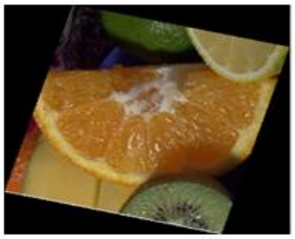
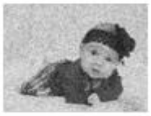
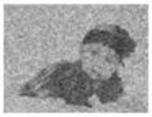
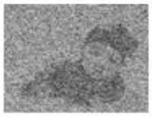
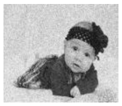
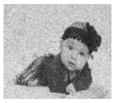
| Attack | Rotation Transform with Rotation Angel 50° | Rotation Transform with Rotation Angel 65° | Rotation Transform with Rotation Angel 75° |
|---|---|---|---|
| Attacked Image | <br>PSNR = 33.57dB | <br>PSNR = 31.12dB | <br>PSNR = 29.32dB |
| Extracted Watermark | <br>NC= 0.7334 | <br>NC=0.5129 | <br>NC= 0.3876 |

***Figure 4.6.6*** *Rotation Transform attack with rotation angle* 50°, 65°, and 75° *for fruits.*

In case of Gaussian noise, he select Lena image for generating the results. For that, author set mean to zero and covariance to 0.002 to the watermarked image, extracted watermark are shown in Figure 4.6.7. The figure shows that the watermark is still recovering after high density of Gaussian noise.

| Attack | Gaussian Noise at 0.02 | Gaussian Noise at 0.08 |
|---|---|---|
| Attacked Image | PSNR = 40.63dB | PSNR = 38.48dB |
| Extracted Watermark |  NC= 0.8172 |  NC= 0.6338 |

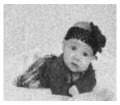
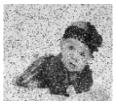
| Attack | Salt & Pepper Noise at 0.02 | Salt & Pepper Noise at 0.08 |
|---|---|---|
| Attacked Image | PSNR = 43.59dB | PSNR = 40.12dB |
| Extracted Watermark |  NC= 0.9741 |  NC= 0.7137 |

***Figure 4.6.7*** *Gaussian Noise of density 0.02 & 0.08 and Salt & pepper noise of density 0.02 & 0.08.*

Then author has indicated the effect of watermark embedding scheme against the salt & pepper noise attack. For that Lena test image is taken and zero mean and the value of covariance 0.002 is used. Figure 4.6.7 shows the result of the scheme against salt & pepper noise.

Author has shown some more result of the proposed scheme against geometric distortion. In this, the correctness of the watermark extraction depends on the feature points of the image [44]. If one can detect the feature points of the watermarked image which are the same as the original image, author can easily extract the watermark without any error. In Figure 4.6.8 the first image is the original image, the second one is the carrier watermark image, and the third one is the extracted watermark image. In the case of salt & pepper noise, the scheme has better extraction effect than other image processing attacks. Author has successfully extracted the watermark from JEPG compression, rotation, Gaussian noise, salt & pepper noise, and Median filter attacks. The correlation coefficients for all extracted watermarks after all attacks are presented in Table 4.6.2.

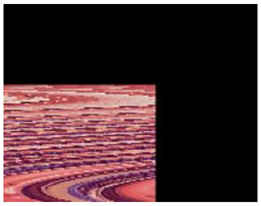
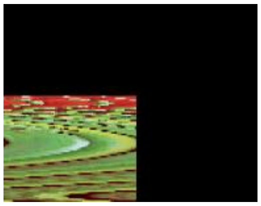
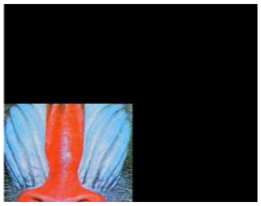
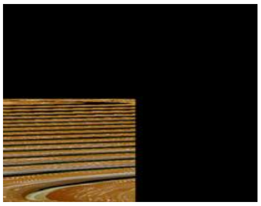
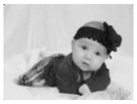
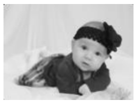
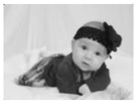
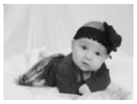
| Attack | Lena image (512×512) | Peeper image (512×512) | Baboon image (512×512) | Fruit image (512 ×512) |
|---|---|---|---|---|
| Original Images | | | | |
| Carrier watermarked Images |  |  |  |  |
| Extracted Watermarks |  |  |  |  |

***Figure 4.6.8*** *Watermark extraction result against Geometric distortion on test images*

**Table 4.6.2 Comparison of normalized correlation coefficient with existing methods.**

| Attacks | Proposed method | Ahahmad et.al | Run et. al. | Lai et.al. | Bhatnagar et.al |
|---|---|---|---|---|---|
| JEPG Compression | 0.9645 | 0.5156 | 0.9512 | 0.5376 | 0.9637 |
| Rotation | 0.8324 | 0.4972 | Not reported | 0.4972 | 0.9025 |
| Gaussian Noise | 0.8172 | 0.5376 | 0.7566 | 0.4279 | 0.3603 |
| Salt & pepper | 0.9741 | 0.3537 | Not reported | 0.4255 | 0.4635 |
| Median Filter | 0.9564 | Not reported | 0.9564 | Not reported | 0.4624 |
| Speckle Noise | 0.9163 | Not reported | 0.9827 | 0.9202 | Not reported |

## 4.7 Comparative Analysis

In this section, author has compared the watermarking embedding method with the existing methods [46, 53, and 54]. The comparative analysis is provided through the Table 4.7.1. By adding a noise into the host image [56] is responsible for the degradation and distortion of the image. The watermark data are also affected by adding the noise that makes difficult for watermark extraction. It is well-defined from the table 4.7.1 the performance of the scheme shows better resolution than existing methods. Table 4.7.1 shows very good performance against JPEG compression and salt & pepper noise attack. For Median filtering, the scheme extracts the watermark upto 8× 8 and in case of Rotation and Median filter, the method shows excellent results. The performance of the scheme against the JPEG compression attack is very close to [53, 54] and better than the watermarking algorithm reported by [46] and [55] From the comparative analysis table it may be figured out that the scheme is very robust against salt & pepper noise, and Median filter attack, and shows better performance over the methods proposed by [46] and [55]. Tables 4.7.2 have been used for comparing the PSNR values of the watermarking embedding scheme and the other method reported by [53, 54]. It is very clear from table 4.7.2 that the watermarking embedding scheme gives better results compared to existing methods. Table 4.7.2 shows that the watermarking embedding scheme gives good result in case of all attacks when compared to [46, 53, and 54]. The performance of the watermarking scheme against the all attacks is very close to [54] and the [46] and far better than the watermarking algorithm reported by [53]. The imperceptibility of the watermarking scheme has also been compared with the other existing algorithms [46, 53] and [54] shown in Table 4.7.2.

**Table 4.7.1 Comparison of method with Run et al. Lai et al. and Bhatnagar et al.**

| Attacks | Proposed method | Run et al. | Lai et al. | Bhatnagar et al |
|---|---|---|---|---|
| Extraction technique | Semi-blinb | Non-blind | Semi-blind | Non-blind |
| Embedding domain | DWT+PCA | DWT+SVD | FRFT+SVD | DWT+SVD |
| Size of watermark | 256×256 | 256×256 | 256×256 | 128×128 |
| Size of original image | 512×512 | 512×512 | 512×512 | 256×256 |
| JEPG compression | QF=1 to 80 | QF=1 to 75 | QF=1 to 100 | QF=1 to 100 |
| Rotation | 50° | Not reported | 50° | 50° |
| Gaussian Noise | Up to 50 % | Up to 10 % | Up to 100 % | Up to 10 % |
| Salt & pepper Noise | Up to 50 % | Not reported | Up to 100 % | Not reported |
| Median filter | 3×3 | Not reported | 11×11 | Not reported |
| Speckle Noise | Tested | Tested | Tested | Not reported |

**Table 4.7.2 Comparisons of peak signal to noise ratio (PSNR) dB with existing methods.**

| Test color images | Proposed method | Run et al. | Lai et al. | Bhatnagar et al. |
|---|---|---|---|---|
| Lena | 43.59 | 32.54 | 36.11 | 39.25 |
| Peppers | 41.68 | 31.47 | 36.24 | 37.96 |
| Baboon | 39.25 | 33.93 | 32.18 | 37.57 |
| Fruits | 38.57 | 31.72 | 35.86 | 37.32 |

Figure 4.7.1 shows the comparison of the embedding scheme with other existing techniques [46, 53, and 54]. This comparison is reported in terms of watermark payload and imperceptibility in case of Lena image. It is observed that the scheme achieves better results as compared to other existing techniques.

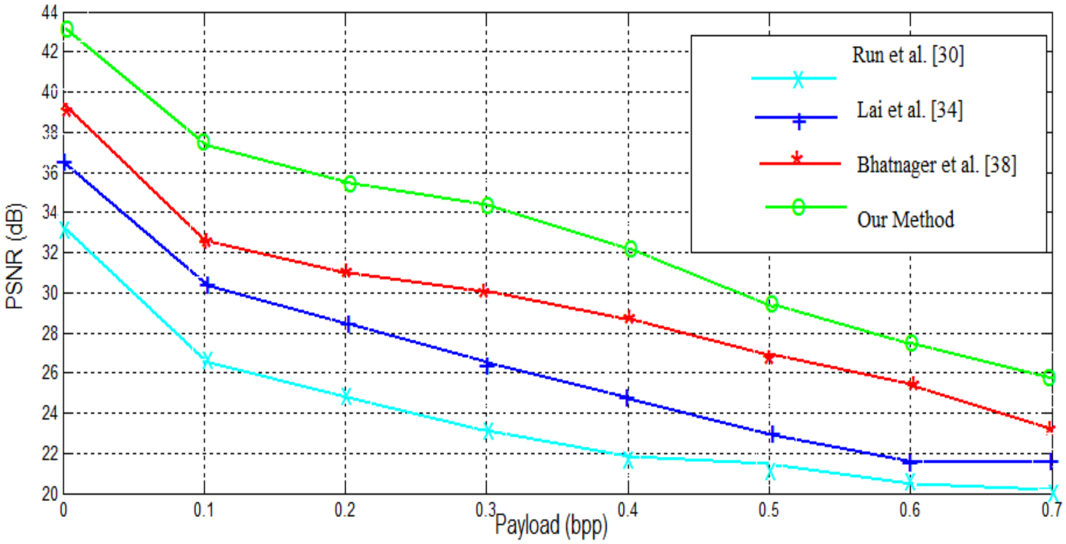


***Figure 4.7.1*** *Performance comparison the proposed watermarking scheme with existing approaches for Lena image*

In Figure, 4.7.1 author has compared his embedding algorithm with Salt & Pepper noise attack with existing method of [46, 53, and 54]. The proposed scheme produces very impressive results against salt & pepper noise and JPEG compression. Hence, author has graphically presented and compared his result with these two attacks in Figure 4.7.2 & 4.7.3. These two figures provide a performance comparison of proposed method for salt & pepper noise by adjusting the value of noise variance. The performance of the scheme against the salt & pepper noise attack is in close proximity of the Bhatnager et al., and far better than the watermarking algorithm reported by Run et al., and Lai et al.

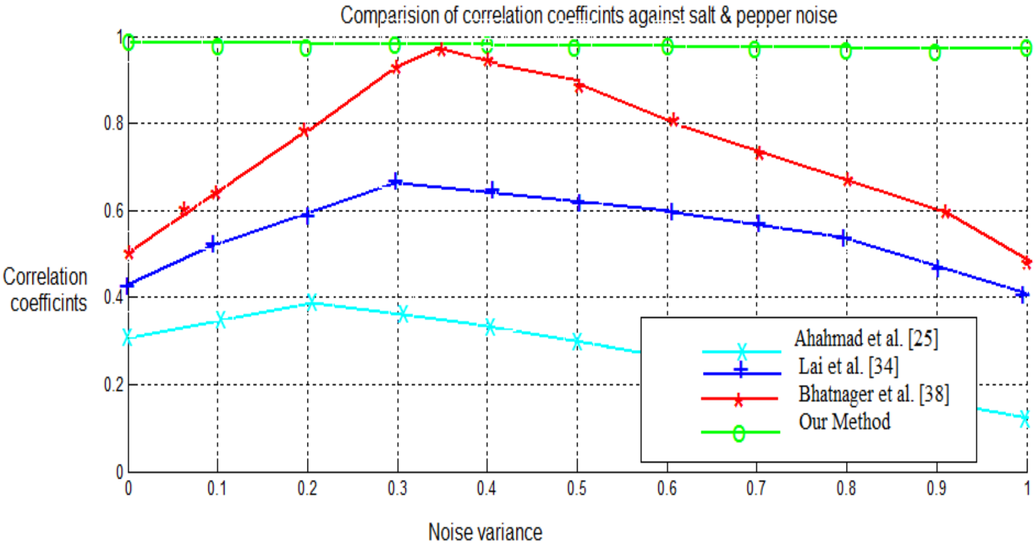


***Figure 4.7.2** Performance of proposed watermarking scheme for different salt & pepper noise attack*

In Figure 4.7.3, author has provided a performance comparison of his method for JPEG compression attack by varying the quality factor. For assuring the robustness, of watermarked image the value of quality factor has been carried from 10 to 100. It has been concluded that the performance of the proposed embedding scheme is very close to the algorithm proposed by Bhatnager et al. and Lai et al. The scheme is superior over the algorithm proposed by Ahahmad et al.

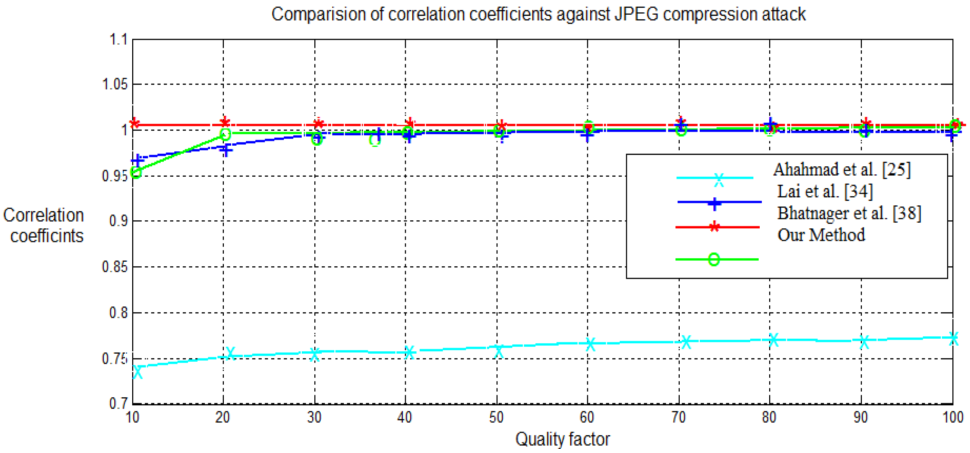


***Figure 4.7.3** Performance of proposed watermarking scheme by varying the value of quality factor*

## 4.8 Conclusion

In this chapter, author has proposed a modified buyer seller watermarking protocol, which uses wavelets, and PCA transform. The method is implemented using 3-level DWT with PCA transform. The method is also image dependant and able to survive under geometric distortion and image processing attacks. PCA transform help us for reducing correlation coefficient among the wavelet coefficients. He has decomposed the original image up to 3 levels, then he select only HL3 and LH3 bands of the DWT image, then watermark bits are inserted into the principal components PCs. A gray-scale watermark image has been embedded only the maximum energy blocks were chosen for the embedding procedure. The scheme performs better when compared with existing reporting methods (Run et al. [53], Lai et al. [46], Ahahmad et al. [55] and Bhatnager et al. [54]). The results prove that the scheme gives better result against Median Filter, Salt & Pepper Noise, JPEG Compression, Rotation and Gaussian Noise.

The contribution toward this research is published and is as follows:

**[1]** Ashwani Kumar, S.P. Ghrera, and Vipin Tyagi, "Modified Buyer Seller Watermarking Protocol based on Discrete Wavelet Transform and Principal Component Analysis," Indian Journal of Science and Technology, Vol. 8, no. 35, pp. 1-9, 2015. [SCOPUS indexed].

# CHAPTER # 5

## A COMPARISON OF BUYER-SELLER WATERMARKING PROTOCOL (BSWP) BASED ON DISCRETE COSINE TRANSFORM (DCT) AND DISCRETE WAVELET TRANSFORM (DWT)

### 5.1 Introduction

Buyer-Seller watermarking protocol (BSWT) [57] is used to preserve the rights for the buyer and the seller. Frequency domain watermarking embedding that is DCT and DWT can affect the robustness and imperceptibility of watermarking algorithm. This chapter studies the comparison of both domain which is DCT and DWT and concludes which one is better on the bases of some parameters. Digital watermarking is a key technology to embed information as unperceivable signals in digital contents. Buyer-seller watermarking protocols based on Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) integrate digital watermarking algorithm and cryptography techniques for copyright protection. In this chapter, author has shown the comparison of these two, buyer-seller watermarking protocol based on Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). These two protocols use Public Key Infrastructure (PKI), arbitrator and watermarking certificate authority (WCA) for better security. This chapter also shows results of watermark image quality based on peak signal-to-noise ratio (PSNR) mean square error (MSE) and similarity factor (SF).
Digital watermarking techniques can also be used to detect a document or image is illegally distributed or modified [58, 59].

Digital watermarking [42] and copyright marking [4] have been proposed, complementing encryption techniques, to establish and prove ownership rights by embedding the seller’s information in the redistributed content. There are number of watermarking protocols proposed in [5] to identify the illegal distribution of digital content.

The classical methods modify the least significant bits (LSB) of specific pixels of the host image based on the watermark bits [60]. For frequency domain, the main concept is to insert a watermark into frequency coefficients of the transformed image using the discrete cosine transform (DCT), the discrete wavelet transform (DWT) [61] or other kind of transforms techniques [60, 62].

## 5.2 Related Work

There are many watermarking protocols that have been proposed using cryptography and digital watermarking techniques. Memon and Wong proposed a buyer-seller watermarking protocol in [15] to deal with the customer's right problem, but also introduced a new issue, the unbinding problem, in their solution. The proposed work compares buyer-seller watermarking protocol based on discrete cosine transform (DCT) and discrete wavelet transform (DWT) to fulfill the design requirements, different from the predecessors, proposed approach makes improvements on the many aspects such as anonymous communication between buyer and seller [31] it support multi-transaction and dispute resolution and avoids double watermark insertion. Using the concept of discrete wavelet transform [32] it results that it may increase the security of the protocol hence the efficiency will increase.

## 5.3 Comparison of DWT and DCT Buyer-Seller Watermarking Protocol

In this section, author has shown the comparison of two protocols i.e. buyer seller watermarking using DCT and DWT transform to provide more security for the buyer and the seller during the transmission of digital content over the network. He first defines the role and notations, which are given in table 5.4.1. He has also defined the wavelet decomposition and determination of watermarking location.

The buyer-seller watermarking protocol based on DWT uses robust watermark technique proposed by L Qiao [23] with the RSA cryptosystem [63]. For that, author assumes following.

- Every seller in transaction has unique watermarking embedded function algorithm in the software.
- He also assumes that all messages are transferred in a secure manner.
- Digital content is a still image.
- WCA is honest, trust worthy and every transaction is atomic.
- Single unique watermark may be generated for each digital content.

## 5.4 Buyer-Seller Watermarking Protocol (BSWP) Using DWT

Wavelet based transform are gaining more popularity because it has a number of advantages over other transforms. It contains progressive low bit-rate transmission and quality scalability. The buyer seller watermarking protocol based on DWT uses robust watermark technique proposed by L Qiao with the RSA cryptosystem.

### 5.4.1 Watermark Generation and Extraction Protocol with Discrete Wavelet Transform (DWT)

The watermark generation and extraction protocol using discrete wavelet transform (DWT) [32] as depicted in figure 5.4.1 [a & b]. In this process the original image is decomposed by using 2-dimension discrete wavelet transformation (DWT) and coefficients of each sub-band from which the features are extracted. Coefficients that meet some specific conditions are selected for watermarking embedding. Then watermarking is embedded by changing these coefficients according to specific regulation. Finally, the modified coefficients are reconstructed with other coefficients to watermarked image by using inverse 2D-DWT (IDWT). After wavelet decomposition of watermarked image, features that meet specific requirements are extracted and watermarking are embedded in these locations.

### Watermark Insertion using DWT

In this, author has inserted the watermark into the original image with the help o f equation (5.4.2).

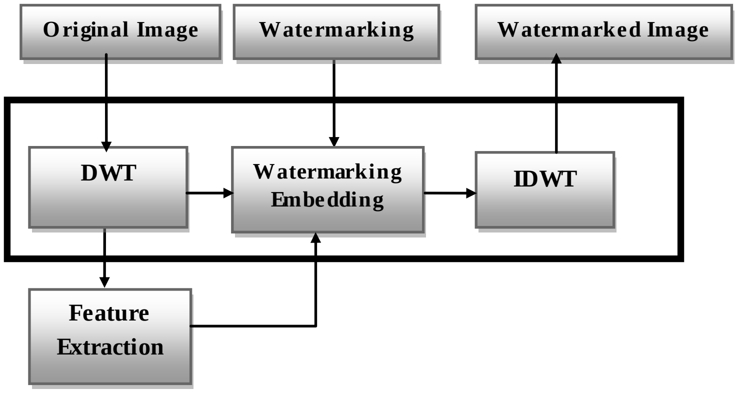


***Figure 5.4.1(a)*** *DWT Based Encoder*

### Watermark Extraction using DWT

In this, author extracts the watermark from the original image with the help of equation (5.4.3).

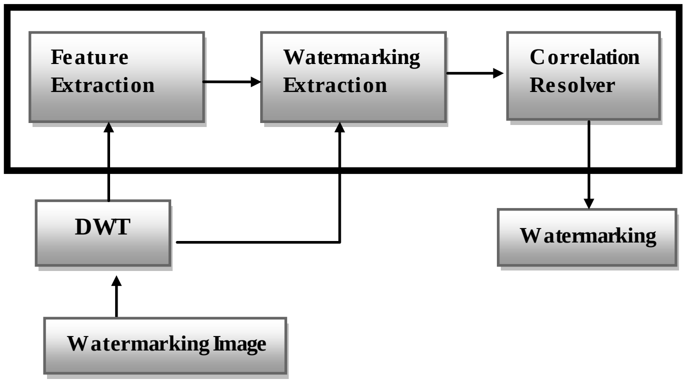


***Figure 5.4.1(b)*** *DWT Based Decoder*

Discrete wavelet transforms (DWT) is a signal analytic theory that can localize the signal in spatiotemporal. This theory has already been widely used. The basic idea of applying DWT on the image processing is that, the original image can be decomposed into lower frequency sub-band and higher frequency sub-band. Especially, higher frequency components of images have the self similarity between each frequency components, horizontally, vertically and diagonally. Wavelets are obtained from a signal prototype wavelet y(t) called mother wavelet by dilations and shifting. Equation (5.4.1) shows the general form of a discrete wavelet transform.

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}}\psi(\frac{t-b}{a}) \qquad \textbf{(5.4.1)}$$

Where a is scaling parameter and b is shifting parameter.

The 1D discrete wavelet transform is given by the equation no. (5.4.2).

$$\mathrm{W}_{\mathrm{f}}(\mathrm{a,b}) = \int_{-\infty}^{\infty} \mathrm{x(t)}\varphi_{\mathrm{a,b}}(\mathrm{t})\mathrm{dt} \qquad \textbf{(5.4.2)}$$

The inverse 1D discrete wavelet transform is given by the equation no. (5.4.3).

$$\mathrm{x(t)} = \frac{1}{\mathrm{C}}\int_{0}^{\infty}\int_{-\infty}^{\infty} \mathrm{W}_{\mathrm{f}}(\mathrm{a,b})\varphi_{\mathrm{a,b}}(\mathrm{t})\mathrm{db}\frac{\mathrm{da}}{\mathrm{a}^{2}} \qquad \textbf{(5.4.3)}$$

Where

$$\mathrm{C} = \int_{-\infty}^{\infty} \frac{(|\varphi\omega|)^{2}}{\omega}$$

Figure 5.4.2 shows the buyer-seller watermarking protocol based on DWT [32] which is secure than its predecessors. The buyer-seller watermarking protocol based on DWT uses public key cryptosystem and has five different roles.

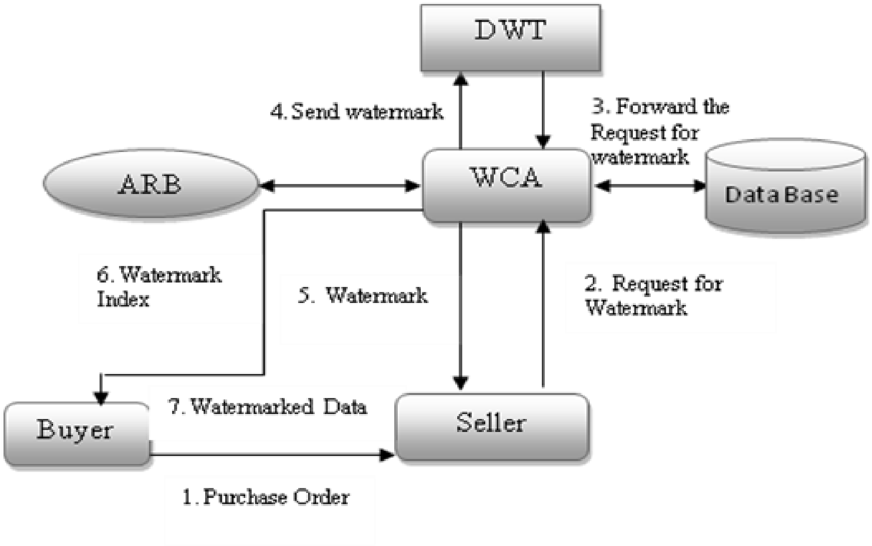


***Figure 5.4.2*** *Buyer-Seller Watermarking protocol with DWT*

The Figure 5.4.3 shows the details of possible transactions in the buyer-seller watermarking protocol with DWT.

**Table-5.4.1The notations used in the buyer-seller watermarking protocol based on DWT are defined below.**

| NOTATION | DESCRIPTION |
|---|---|
| **X** | Original copy of digital content. |
| **W** | Watermark information to be embedded, generated based on public keys of buyer and seller. |
| **X'** | Watermarked digital content. |
| **WID** | Identity number, which is to be embedded in Generated watermark information's Index the digital content. |
| **DWTWID** | Generated watermark information's Index Identity number using Discrete Wavelet Transform (DWT). |
| **ɸ** | Insertion of Watermark information into the original copy of digital content. |
| **$(P_{B,}S_B)$** | A public-secret key pair, where PB is buyer's (or B's) public key and SB is B's secret key. |

| | |
|---|---|
| **$DS_{SB}$(M)** | The message M is digitally signed by B’s private key. |
| **$E_{PB}$(M)** | The message M is encrypted using B’s public key. |
| **$E_{SB}$(M)** | The message M is encrypted using B’s private key. |
| **$D_{PB}$(C)** | The cipher text C is decrypted using B’s public key. |
| **$D_{SB}$(C)** | The cipher text C is decrypted using B’s private key. |

**Table-5.4.1**

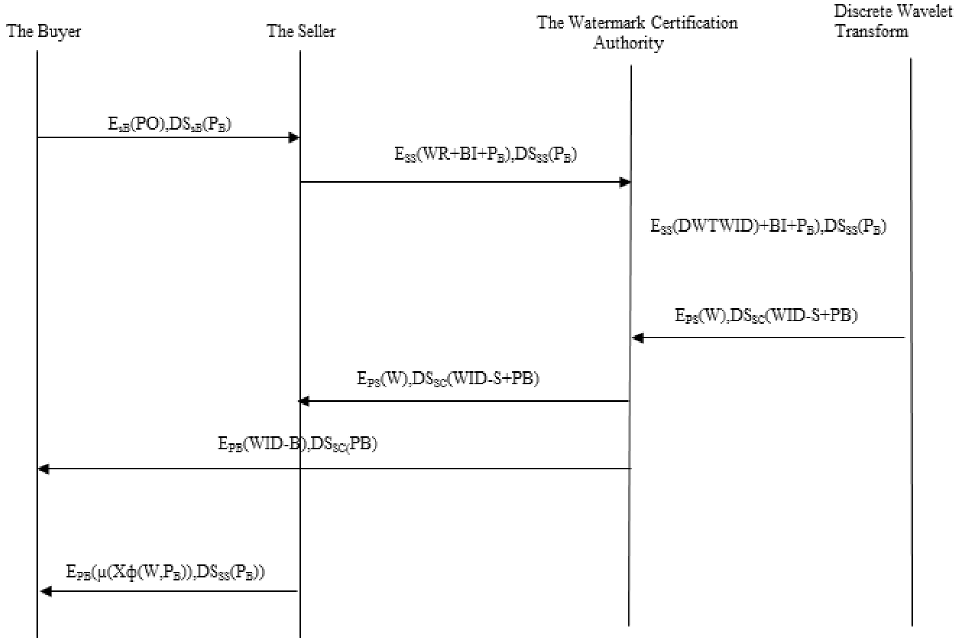

The Buyer
The Seller
The Watermark Certification Authority
Discrete Wavelet Transform
$E_{sB}(PO),DS_{sB}(P_B)$
$E_{SS}(WR+BI+P_B),DS_{SS}(P_B)$
$E_{SS}(DWTWID)+BI+P_B),DS_{SS}(P_B)$
$E_{PS}(W),DS_{SC}(WID\text{-}S+PB)$
$E_{PS}(W),DS_{SC}(WID\text{-}S+PB)$
$E_{PB}(WID\text{-}B),DS_{SC(}PB)$
$E_{PB}(\mu(X\phi(W,P_B)),DS_{SS}(P_B))$

***Figure 5.4.3** Transaction in the watermarking protocol using DWT*

## 5.5 Buyer-Seller Watermarking Protocol (BSWP) Using DCT

In this section, author has used DCT to provide more security for the buyer and the seller during the transmission of digital content same as author did with DWT. In this section, author has defined the role and notations which are given in table 5.5.1.

In this, there are four roles i.e. one is buyer, second is a seller, third is WCA device and fourth is DCT. The seller provides the watermark embedding operation and sells the watermarked product to the buyer. The WCA device is integrated into the seller’s computer system and it will generate the watermark with the help of DCT for the buyer. He assumes that every seller in transaction has unique water marking embedded function algorithm in their software. In this protocol, author use watermarking embedding with discrete cosine transform (DCT), and arbiter (ARB) and watermarking certificate authority (WCA).

### 5.5.1 Watermark Generation and Extraction Protocol with Discrete Cosine Transform (DCT)

The watermark generation and extraction protocol using discrete cosine transform (DCT), as depicted in figure 5.5.1 [a & b]. The protocol can be executed multiple times for multi-transactions between the seller A and the buyer B, as depicted in Figure 5.5.2. S and B first need to negotiate a purchase agreement ARG on rights and obligations as well as the specification of the digital content X. Figure 5.5.1 shows the watermarking generation and extraction protocol.

*Watermark Insertion using DCT*

In this, he inserts the watermark into the original image with the help of equation **(5.5.1)**.

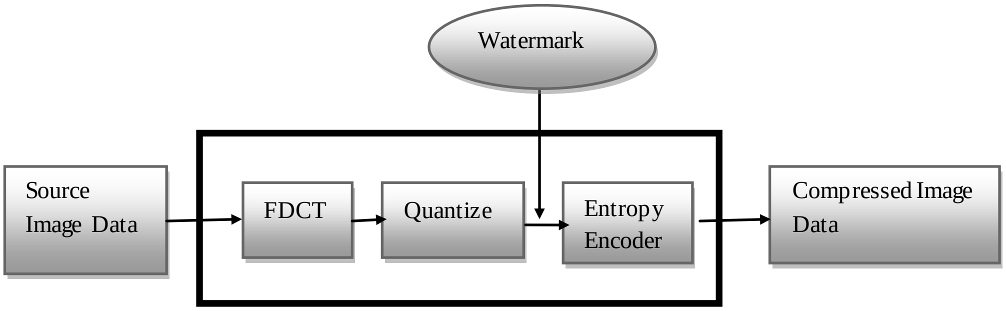


***Figure 5.5.1****(a) DCT Based Encoder*

### *Watermark Extraction using DCT*

In this, he extracts the watermark from the original image with the help of equation (5.5.2).

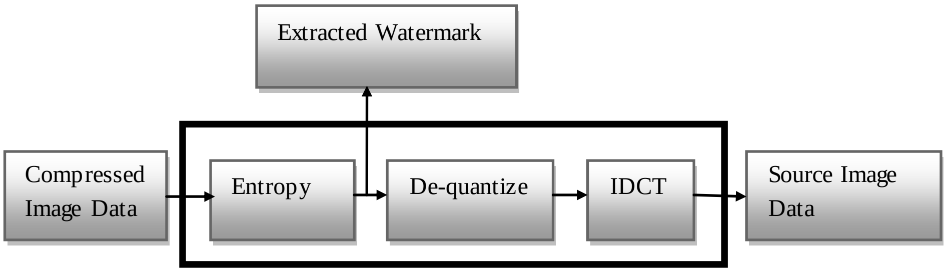


***Figure 5.5.1****(b) DCT Based Decoder*

The discrete cosine transform (DCT) is a technique for converting a signal into elementary frequency components. It uses a transformation function which transforms the representation of data from space domain to frequency domain. The general equation for a 2D DCT is defined by the following eq. no. (5.5.1).

$$f(u,v) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} c\,(u)\;c\,(v) f\;(i,j)\cos\,[\frac{\pi(2i+1)u}{2N}]\cos\,[\frac{\pi(2j+1)u}{2N}] \qquad \textbf{(5.5.1)}$$

The inverse transform is defined as

$$f(x,y) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} c\,(u)\;c\,(v) f\;(i,j)\cos\,[\frac{\pi(2i+1)u}{2N}]\cos\,[\frac{\pi(2j+1)u}{2N}] \qquad \textbf{(5.5.2)}$$

Figure 5.5.2 shows the buyer-seller watermarking protocol with discrete cosine transform (DCT) [31]. The protocol is based on public key cryptosystem and has five different roles.

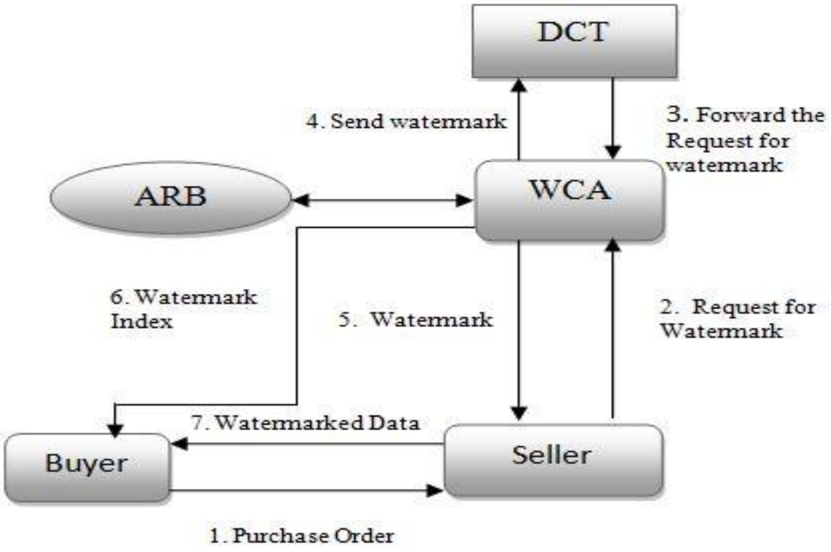


***Figure 5.5.2*** *Buyer-Seller Watermarking protocol with DCT*

The Figure 5.5.3 shows the details of possible transactions in the buyer-seller watermarking protocol with DCT.

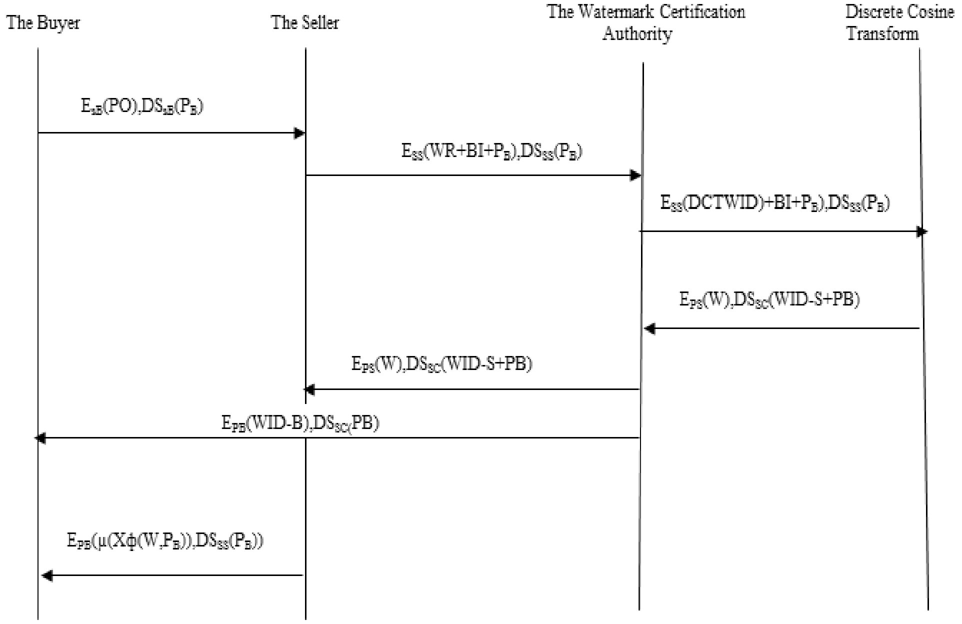

The Buyer
The Seller
The Watermark Certification Authority
Discrete Cosine Transform
$E_{sB}(PO),DS_{sB}(P_B)$
$E_{SS}(WR+BI+P_B),DS_{SS}(P_B)$
$E_{SS}(DCTWID)+BI+P_B),DS_{SS}(P_B)$
$E_{PS}(W),DS_{SC}(WID\text{-}S+PB)$
$E_{PS}(W),DS_{SC}(WID\text{-}S+PB)$
$E_{PB}(WID\text{-}B),DS_{SC(}PB)$
$E_{PB}(\mu(X\phi(W,P_B)),DS_{SS}(P_B))$

***Figure 5.5.3*** *Transactions in the watermarking protocol using DCT*

**Table-5.5.1 The notations used in the buyer-seller watermarking protocol based on DCT are defined below.**

| NOTATION | DESCRIPTION |
|---|---|
| X | Original copy of digital content. |
| W | Watermark information to be embedded, generated based on public keys of buyer and seller. |
| X' | Watermarked digital content. |
| WID | Identity number, which is to be embedded in Generated watermark information's Index the digital content. |
| DCTWID | Generated watermark information's Index Identity number using Discrete Cosine Transform (DCT). |
| ϕ | Insertion of Watermark information into the original copy of digital content. |
| (PB,SB) | A public-secret key pair, where PB is buyer's (or B's) public key and SB is B's secret key. |
| DSSB(M) | The message M is digitally signed by B's private key. |
| EPB(M) | The message M is encrypted using B's public key. |
| ESB(M) | The message M is encrypted using B's private key. |
| DPB(C) | The cipher text C is decrypted using B's public key. |
| DSB(C) | The cipher text C is decrypted using B's private key. |

**Table-5.5.1**

## 5.6 Result Analysis of These Two Protocols

In this section, author has studied the effect of DWT and DCT upon the buyer-seller watermarking protocol. Buyer-seller watermarking protocol based on DWT is better and gives more secure watermark insertion.

Many researchers have used Lena image as the original image. He has also uses Lena image of size 256×256 as a test image. The researcher has applied some types of attacks on the Lena image after watermark embedding to prove the quality of their proposed work. He chooses some previous work [9, 64, 65, and 66] to obtain robustness results. For that, he first defined some parameter to measure the quality of image.

### 5.6.1 Parameter Used

For analysis the comparison of DWT & DCT domain author has used PSNR, MSE and Similarity factor (SF) measurements.

1. PSNR (Peak signal-to-noise ratio) is generally used to analyze quality of image.

$$\mathrm{PSNR} = 10 * \log \frac{255^2}{\mathrm{MSE}} \qquad \textbf{(5.6.1)}$$

2. The MSE (Mean Square Error) represents the cumulative squared error between the compressed image and the original image.

$$\mathrm{MSE} = \sum_{\mathrm{i}=1}^{\mathrm{x}} \sum_{\mathrm{j}=1}^{\mathrm{y}} \frac{(|\mathrm{A}_{\mathrm{i,j}} - \mathrm{B}_{\mathrm{i,j}}|)^2}{\mathrm{x} * \mathrm{y}} \qquad \textbf{(5.6.2)}$$

Where *x* is width of image and *y* is height and *x*y* is the no. of pixels.

3. Similarity Factor (SF):- Similarity Factor is measure by the similarity of pixel acuteness between the original image and the watermarked image. This helps to measure the changes in the perceptual quality of the image. The equation (5.6.3) shows the formula to calculate similarity factor.

$$SF = \frac{\sum_i \sum_j I(i,j) * I_{\,w}(i,j)}{\sum_i \sum_j I_{\,w}(i,j)^{\,2}} \qquad \textbf{(5.6.3)}$$

Where I (i,j) is the original image and Iw (i,j) is the watermarked image. The similarity factor should always be equal to 1.

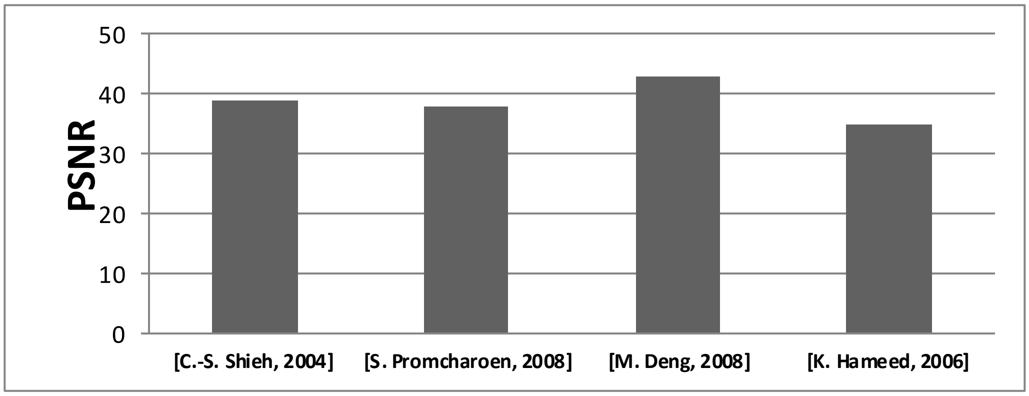


***Figure 5.6.1*** *PSNR value of image in DCT domain*

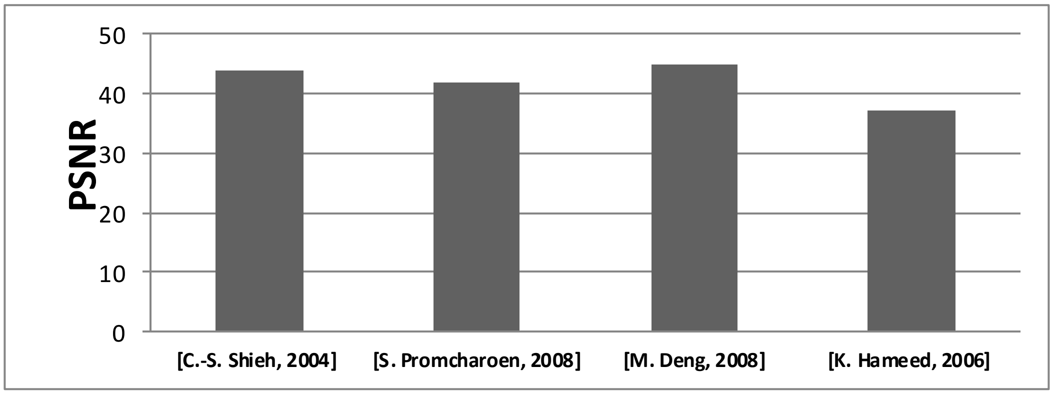


***Figure 5.6.2*** *PSNR value of image in DWT domain*

It is concluded to compare the obtained results from previous work by calculating the difference between the original image and watermark image using PSNR measurement. The above figures show robustness, imperceptible results for both embedded domains. The figure 5.6.1 shows PSNR values according DCT embedding domain. The figure 5.6.2 shows the PSNR values according DWT embedding domain. The results of DWT were found to be higher than 42, whereas most DCT result were found less than that. Hence, it clearly shows that the DWT embedding domain is better in terms of imperceptible, robustness and capacity than DCT embedding domain.

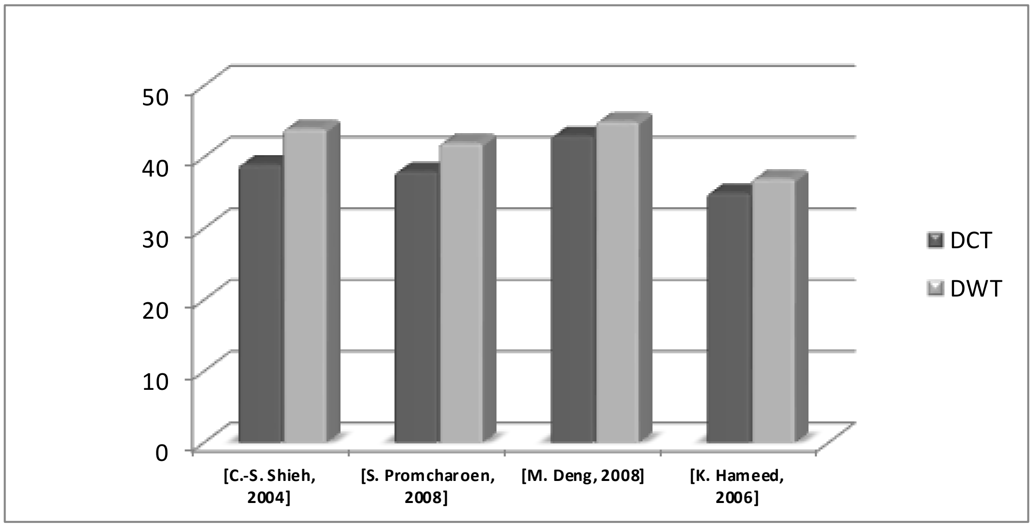


***Figure 5.6.3*** *Comparison of PSNR value in DCT & DWT domain*

Figure 5.6.3 shows the comparison of PSNR value in DCT & DWT domain. The DWT embedding domain is more robust than DCT embedding domain and it also contain high capacity. In the brief DWT based watermarking is better than the DCT domain watermarking for embedding the watermark into the buyer seller watermarking protocol.

**Table 5.6.1: The value of PSNR, MSE & SF is given.**

| Previous Work | Discrete Cosine Transform(DCT) | | | Discrete Wavelet Transform(DWT) | | |
|---|---|---|---|---|---|---|
| | **PSNR** | **MSE** | **SF** | **PSNR** | **MSE** | **SF** |
| [C.-S. Shieh, 2004] | 39.393 | 227.748 | 0.423 | 44.876 | 221.999 | 0.323 |
| [S. Promcharoen, 2008] | 38.765 | 228.180 | 0.499 | 42.675 | 225.093 | 0.423 |
| [M. Deng, 2008] | 43.897 | 223.139 | 0.325 | 45.987 | 219.368 | 0.291 |
| [K. Hameed, 2006] | 37.675 | 229.113 | 0.538 | 37.654 | 229.748 | 0.536 |

**Table 5.6.1**

## 5.7 Conclusion

This chapter compares (BSWP) based on Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). It is clear that the DWT is better than DCT in terms of imperceptibility, robustness and capacity. DCT and DWT based buyer seller watermarking protocol is used to fulfill the design requirements, different from the previous, these approach makes huge change on the many aspects such as anonymous communication between buyer and seller. It supports multi-transaction and dispute resolution and avoids double watermark insertion. This chapter has shown the various results which are obtained by calculating PSNR, MSE and SF measurement.

The contribution toward this research is published and is as follows:

[1] Ashwani Kumar, S.P. Ghrera, and Vipin Tyagi, "A Comparison of Buyer-Seller Watermarking Protocol (BSWP) Based On Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT)," Computer Society of India (CSI) Vol. 1. pp. 401-408, Springer International Publishing, 2015. [SCOPUS indexed].

# CHAPTER # 6

## AN ID-BASED SECURE AND FLEXIBLE BUYER-SELLER WATERMARKING PROTOCOL (BSWP) FOR COPYRIGHT PROTECTION

### 6.1 Introduction

Digital watermarking protocols are the ones which combine fingerprinting technique with watermarking, for embedding digital signal or watermark into an original multimedia object. BSWP is fundamentally applied to continue the digital rights of both the purchase and vendor. In this chapter, author has proposed an identity-based BSWP that encountered various weaknesses of Zhang et al. watermarking protocol. He ensures that by pointing out these weaknesses, inaccuracy can be minimized for further implementing of buyer-seller watermarking protocol. The suggested protocol uses ID-based public key cryptography and digital watermarking scheme to place the ownership of digital content. Hence, copyright protection is attained. Author claimed that his suggested protocol is efficient and has adequate security as compared to traditional proposed protocols and suitable for any practical buyer-seller watermarking scheme.

The speedy development of internet and e-commerce needs a copyright protection mechanism for multimedia data. Digital watermarking becomes an important technique for protecting the digital rights. The principal object of digital watermarking technique [4] is to retain digital copyright or watermark, embedded into the cover object. The desirable secure digital watermarking scheme is one, which integrates public key cryptosystem and digital watermarking technique for protecting the buyer and seller in a digital content transaction. Digital watermarking [5] techniques use encrypted domain for embedding and extracting the watermarks. The rapidly growing of the internet encourages some bad usage too, like operations such as transformation, duplication, and redistribution of digital content. With the avail of some software tools, one can easily identify these bad users and redistribution of digital content can also be placed.

Memon et al. [10] proposed the very first buyer-seller watermarking protocol in 2001 and Ju et al. [15] modified this protocol with various advances. Digital watermarking [13] algorithm is divided into two parts, first non blind watermarking schemes and second, blind watermarking schemes, non blind watermarking scheme needs original cover object as well as watermark and watermark key for extracting the watermark while blind watermarking scheme does not require cover object, watermark key and watermark for detection or extraction the watermark. The buyer-seller watermarking protocol [31] is a three-party protocol among a service provider, a customer and a trusted watermark certificate authority. This protocol combines fingerprinting and encryption techniques for protecting the participants into any transaction. In the history, Hwang et al. [67] introduced a time stamping protocol in 2005. In their protocol, a TTP (trusted third party) was introduced for checking the verification and signing phase. Ju et al. [15] proposed an anonymous buyer-seller watermarking protocol with anonymity control in 2002. In this paper, the author has identified the anonymity problem. They have discussed that a buyer can purchase digital content anonymously, but the anonymity can be controlled. Zhang et al. [68] proposed a secure buyer–seller watermarking protocol in 2006. In his paper, no assistance is needed, so that it avoids the conspiracy problem, piracy tracing problem and customer’s right problem. There are only two participants, a seller and a buyer. The protocol can simultaneously resolve many problems. However, there is a drawback in the Zhang et al.’s protocol, i.e. the buyer’s assistance is needed to solve the piracy dispute. Therefore, dispute resolution and unbinding problems exist in Zhang et al. protocol.

Author propose an identity-based buyer-seller watermarking protocol and encountered various existing weaknesses of Zhang et al. (2006)’s protocol such as dispute resolution and unbinding problem. Here, he proposes a new identity-based BSWP for proving the ownership of digital content. His proposed protocol enables the seller to produce the watermark content with their private key. The watermark certificate authority (WCA) is responsible for issuing the digital signature corresponds to ID of the seller, timestamp [67] used for watermark content, watermark and cover object. WCA is maintaining, its own table and keeping the requested IDs of both buyer and seller. Suppose if dispute occurs the buyer can communicate or confirm to the WCA to checkout that whether he/she is the original buyer or not. If any dispute occurs at a later stage, with the help of arbiter it can also be resolved to check the correctness of information used by the seller. Timestamps are compared by the arbiter to identify the appropriate seller of digital content and with the help of timestamps, unbinding problem is also solved. Some key details of his proposed watermarking protocol are identified below:

1. In the proposed protocol, author adopts wavelet and principal component analysis based techniques [69] with identity-based public key cryptography.

2. This watermarking protocol must be autonomous of all watermarking schemes.

3. The proposed protocol makes use of a tamper resistance device, which is embedded into seller's computer and reduces the overhead on WCA as TTP.

## 6.2 Reviewing the scheme of Zhang et al.

Zhang et al. [68] proposed a secure BSWP in 2006. The authors proposed a secure BSWP without the assistance of a TTP in which there are only two participants, seller and buyer. Zhang et al.'s paper is based on the Lei et al. [11] and in this no third party is brought in; therefore, the proposed protocol is more childlike and more dependable than the existing watermarking protocol. Zhang et al.'s protocol resolves the conspiracy problem, piracy tracing problem and customer's right problem. However, there is a drawback in the Zhang et al.'s protocol, i.e. the buyer's assistance is needed to solve the piracy dispute problem. Here, he shows the notations of Zhang et al.'s protocol.

$E_{pk*}(X')$ = encrypted watermark image

$E_{pk*}(X'')$ = second round encrypted watermark image

$E_{pk*}(W)$ = encrypted watermark

$Cert_{CA}(pk_B)$ = digital certificate of CA

$pk_B, sk_B$ = random key pair

ARB = Arbiter

$SEC_B$ = secret key of buyer

$SEC_S$ = secret key of seller

$E_{pk^*}(SEC_B)$ = encrypted secret key

$Sign_{sk^*}(E_{pk^*}(SEC_B))$ = sign encrypted secret key

$Cert_{pk_B}(pk^*)$ = anonymous certificate

In the Zhang et al.'s protocol, seller randomly generates a secret $SEC_S$ key. In the encrypted domain, seller obtains the encrypted watermark $E_{pk*}(W)$ as follows.

$E_{pk*}(W) = E_{pk*}(SEC_S) \otimes E_{pk*}(SEC_B)$

$E_{pk*}(SEC_S \oplus SEC_B)$ **(6.2.1)**

Seller S then inserts the second round watermark through the following formula:

$E_{pk*}(X'') = E_{pk*}(X') \otimes E_{pk*}(W)$

$E_{pk*}(X' \oplus W)$ **(6.2.2)**

Zhang et al.'s et al. claimed that their proposed secure buyer-seller watermarking protocol provides solution for conspiracy problem, piracy-tracing problem and customer’s right problem. Author has identified that the protocol is unable to solve the dispute resolution problem and unbinding problem. Figure 6.2.1 shows a simplified trading model which is based on the Lei et al. protocol.

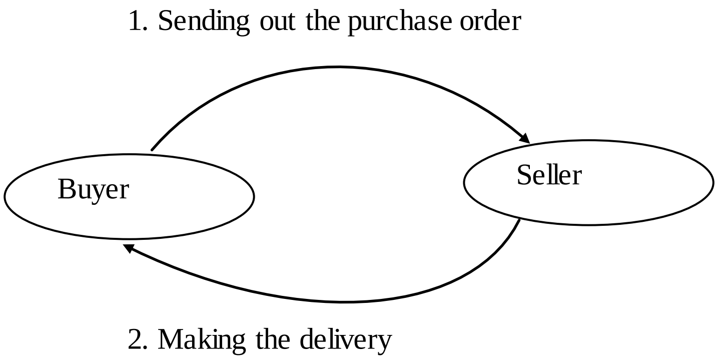


***Figure 6.2.1*** *A simplified trading model*

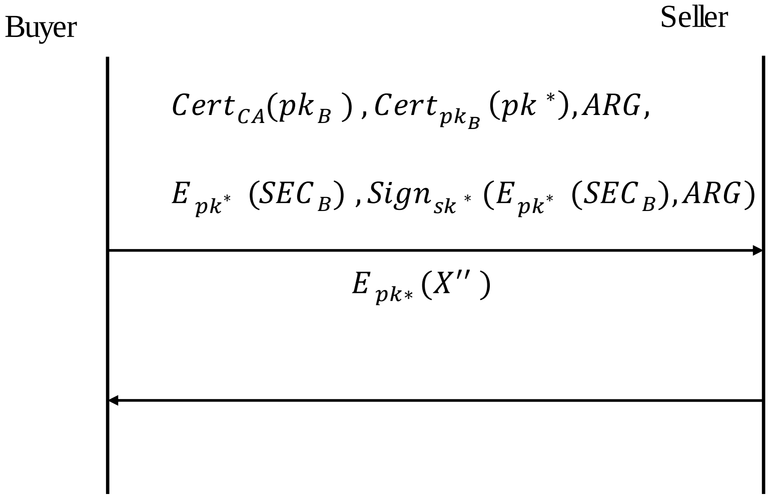

Buyer
Seller
$Cert_{CA}(pk_B),Cert_{pk_B}(pk^*),ARG,$
$E_{pk^*}(SEC_B),Sign_{sk^*}(E_{pk^*}(SEC_B),ARG)$
$E_{pk*}(X'')$

***Figure 6.2.2*** *The encryption phase of J. Zhang secure buyer-seller watermarking protocol [11].*

To level out these topics, author has proposed identity-based cryptographic scheme [6] into the watermarking algorithm. ID-based techniques were introduced by Shamir in 1984 [70].

## 6.3 An Id-Based Secure and Flexible Buyer-Seller Watermarking Protocol for Copyright Protection

This research work is as an extension of author's previous work [31]. In his suggested protocol, he uses same trust model uses by Memon et al. [10] and Lei et al. [11]. The proposed protocol is based on public key infrastructure, arbiter, ID based public key cryptography [42, 71] and digital watermarking scheme. The watermarking scheme involved secret key and digital signature certificate issued by WCA. WCA maintains its own table and keeping the requested IDs of both buyer and seller because it contains a database. The proposed protocol is flexible because it makes use of tamper resistance device which is used to reduce the overhead on WCA and also solves problems listed in section 1. Now, in the digital signature verification phase someone else can use the WCA public keys to validate that the watermark content that was embedded at a certain time into the digital content. The proposed digital watermarking protocol consists of three sub-protocols: the watermark embedding and signing protocol; watermark detecting and verifying protocol; and registration protocol as presented in Figure 6.3.2. He first determines the roles and notations for various participants in his proposed protocol as presented in Figure 6.3.1.

**Seller:** The owner of the digital content or from where the buyer wants to purchase the digital content.

**Spurious buyer:** Who wants to learn the rightful side of the digital capacity that does not belong to him?

**WCA:** Public, private, and shared secret key is issued by this authority. The valid watermark and digital signature are also generated by WCA.

**ARB:** ARB stands for an arbiter, if any dispute occurs between the buyer and seller, that dispute is resolved by arbitration. ARB also verifies the correctness of the digital certificates.

**Tamper-resistant device:** This device is detached into seller's computer and used to produce necessary watermarks and digital signature.

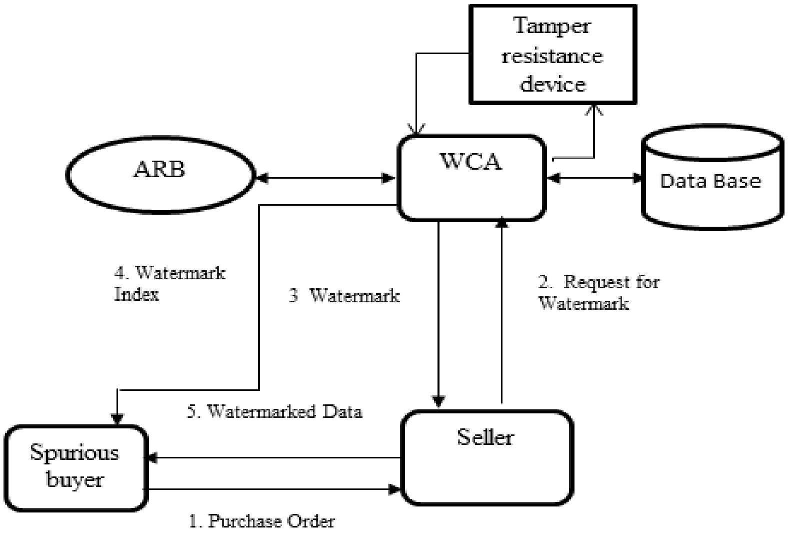


***Figure 6.3.1*** *ID-based buyer-seller watermarking protocol.*

Author has shown assumptions of his suggested protocol.

1. Buyer seller and WCA contain a matched clock. This clock is held securely.
2. The cover object is an image in which the watermark is applied.
3. WCA is assumed to be trustworthy.
4. The buyer seller communicates through a secure channel.
5. The valid watermark is generated by the seller and WCA.

The goals of the proposed watermarking scheme are described below:-

1. The proposed protocol solves the unbinding problem, the dispute resolution problem. In addition, it identifies the spurious seller who claims of ownership of digital content.
2. The buyer interacts with the seller but one time.
3. The buyer does not possess any knowledge of cryptosystem and the embedded watermark.

4. The proposed protocol avoids the double watermark insertion and WCA is responsible for the generation of the watermark.

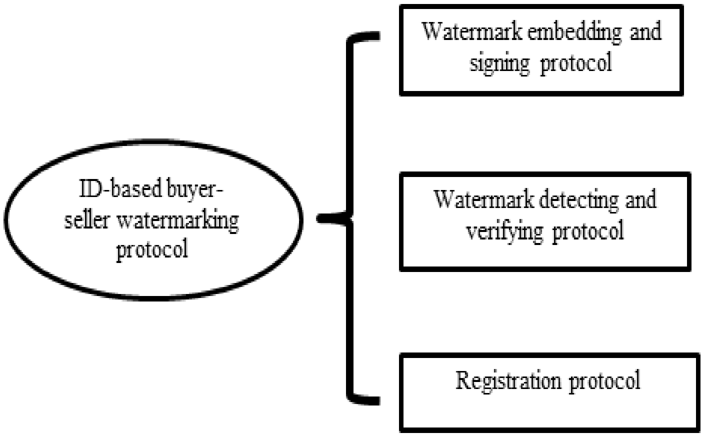

ID-based buyer-seller watermarking protocol
Watermark embedding and signing protocol
Watermark detecting and verifying protocol
Registration protocol

***Figure 6.3.2*** *Three sub-protocols of ID-based buyer-seller watermarking protocol.*

Author has shown the roles and notations of his proposed ID-based secure and flexible buyer-seller watermarking protocol.

X= original image

W = watermark

W' = forge watermark

Z= forged digital content

$X_W$ = watermarked image or data

$E_{H(w_k)}$= encrypted watermark key

$D_{H(w_k)}$= decrypted watermark key

C= cipher text

t= timestamp

$SE_{PC_{wca}}$ = seller performs encryption using WCA public key

ARG = arbiter

$ID_S$= seller credential

$SD_{K_{wca}}$ = seller performs decryption using WCA public key

$Ver_{PC_{wca}}$ (Ds) = verification of digital signature

Ds($Sig_{K_{wca}}$) = digital signature Ds generated by WCA using its private-key.

### 6.3.1 Watermark embedding and signing protocol:-

The watermark embedding and signing protocol is described in Figure 6.3.1. The protocol is being executed multiple times for authentication of a buyer between the seller and WCA. If seller wants to establish the lawful ownership of their digital content, i.e. image X, then the seller can carry out the embedding and signing a protocol with WCA as given in Figure 6.3.1.

The dealings between the seller and *WCA* is given below.

1. The seller selects a random and robust watermark W.
2. The seller embeds the watermark W into digital content X to obtain watermarked data Xw.

$$X_W = E_{H(w_k)}(X,W) \qquad \textbf{(6.3.1.1)}$$

where E is the watermark embedding algorithm and $H(w_k)$ is the watermark key.

3. Then the seller converts plaintext P into ciphertext C using the public-key cryptosystem, PCwca.

$$C = SE_{PC_{wca}}(ID_S, t, X, W, X_W) \qquad \textbf{(6.3.1.2)}$$

where $X_W$ provided by the seller and t is the creation of time of the watermarked content e.i. $X_W$.

4. The seller sends the cipher text C to the WCA.
5. After receiving C, WCA perform some decrypt operation.

$$(ID_S, t, X, W, X_W) = SD_{K_{wca}}(C) \qquad \textbf{(6.3.1.3)}$$

where $K_{wca}$ is the private key of WCA and D is the decryption.

6. WCA checks whether $ID_S$ is legitimate or not. If not WCA aborts the sub-protocol.

7. If the time t is accepted, then WCA checks to confirm that the watermarked content $X_W$ has been constructed by embedding the watermark W in X.
8. If watermark content $X_W$ is valid then WCA generates the digital signature Ds using WCA private key $K_{wca}$.

   $\mathrm{Ds} = \mathrm{Sig}_{K_{wca}}(\mathrm{ID}_S, t, W, H(w_k))$ **(6.3.1.4)**
9. WCA sends this digital signature to the seller.
10. After receiving the digital signature Ds seller verifies it using the public key of the WCA

    $\mathrm{Ver}_{PC_{wca}}(\mathrm{Ds}) = (\mathrm{ID}_S, t, W, H(w_k))$ **(6.3.1.5)**
11. If the digital signature is valid, then the seller keeps Ds, t, and W in their local database. After successfully completion of watermark embedding and signing protocol, the Seller can publicize the digital watermarked content $X_W$.

### 6.3.2 Watermark detecting and verifying protocol:-

The watermark detecting and verifying protocol is described in Figure 6.3.2. This protocol takes place between the buyer and the arbiter (ARB). If the arbiter receives a forge digital content, let, say Z and seller consist $K_S$, t, Ds, W, X. Then seller can claim the rightful ownership of Z by executing the watermark detecting and verifying protocol.

1. The seller sends $\mathrm{ID}_S, t, W, H(w_k)$, Ds and X to arbiter.

2. After getting all information from the seller, arbiter uses the watermark detection algorithm:-

$D_{H(w_k)}(Z, X, W)$ **(6.3.2.1)**

Where D belongs to watermark detecting scheme. If he received the result of the above equation, equal to 1, then *Z* consist watermark *W* and if the effect of above equation equal to 0 then *Z* does not contain watermark *W* and arbiter performs next step.

3. After step 2, arbiter verifies the validity of the digital signature Ds using the equation given below:-

$$\mathrm{Ver}_{\mathrm{PC_{wca}}}(\mathrm{Ds}) = (\mathrm{ID_S}, \mathrm{t}, \mathrm{W}, \mathrm{H}(\mathrm{w_k})) \qquad \textbf{(6.3.2.2)}$$

where PCwca is the public-key cryptosystem of WCA. If Eq. (6.3.2.2) is true then arbiter returns their own key $\mathrm{ID_S}$, t, otherwise arbiter returns 0.

### 6.3.3 Registration protocol:-

The registration protocol takes place between the customer and the WCA, If a buyer wants to hide his identity into a transaction of digital content then buyer randomly selects a pair of key $\mathrm{Rpk_B}$, $\mathrm{Rsk_B}$ and sends $\mathrm{Rpk_B}$ to a trustworthy WCA [68]. After receiving $\mathrm{Rpk_B}$, WCA generates an anonymous digital certificate $\mathrm{Cert_{WCA}}(\mathrm{Rpk_B})$ and sends it to the buyer. If buyer does not require anonymity, the entire registration process can be skipped and normal digital certificate can be practiced by the buyer.

| **Seller** | | **WCA** |
|---|---|---|
| 1. Seller select watermark $W$<br>2. $X_W = E_{H(w_k)}(X, W)$<br>3. $C = SE_{PC_{wca}}(ID_S, t, X, W, X_W)$ | | 5. $(ID_S, t, X, W, X_W) = SD_{K_{wca}}(C)$<br>6. $WCA$ checks $ID_S$, $t$<br>7. Checks $X, X_W$ |
| 10. $Ver_{PC_{wca}}(s) = (ID_S, t, W, H(w_k))$ | 4. $C$ → | 8. $Ds = Sig_{K_{wca}}(ID_S, t, W, H(w_k))$ |
| 11. Stores $Ds$, $t$, $W$ into the database | ← 9. $Ds$ | |

***Figure 6.3.1.1*** *Watermark embedding and signing protocol*

| Seller | | Arbiter (ARB) |
|---|---|---|
| 1. Seller sends<br>$(ID_S, t, W, H(w_k)), D$s,X) | | 2. Perform decryption $D_{H(w_k)}(Z, X, W)$ |
| | | 3. Arbiter verifies $Ver_{PC_{wca}}(s) = (ID_S, t, W, H(w_k))$ |

***Figure 6.3.1.2** Watermark detecting and verifying protocol*

**Table 6.3. 1 Comparison of the proposed scheme with existing protocols.**

| | **[J. Zhang, 2006]** | **[J.G Choi, 2003]** | **[N.D. Memon, 2001]** | **[C. L. Lei, 2004]** | **[Proposed Scheme]** |
|---|---|---|---|---|---|
| The customer's rights problem | Solved | Solved | solved | solved | solved |
| The piracy-tracing problem | Solved | Solved | not tested | solved | solved |
| The unbinding problem | Solved | not solved | not solved | solved | Solved |
| The anonymity problem | partially solved | Solved | not solved | partially solved | Solved |
| The dispute resolution problem | Solved | not solved | not solved | solved | Solved |
| Tamper-resistant WCA device With Database | No | No | No | No | Yes |

## 6.4 Security Analysis of Proposed Scheme

In this section, the security of the proposed ID-based secure and flexible buyer-seller watermarking protocol is analyzed. Author has examined the security of his protocol and compare with scheme of [10, 11, 14, and 68]. The proposed watermarking protocol is secure and flexible for the reason that buyer has no idea about the original digital content X hence, is unable to remove the watermark. Since seller gets no access to the watermarked copy of the digital content X hence, the seller cannot distribute illegal replicas of digital content X. The proposed protocol solved the problems identified in Zhang et al. protocol and problems, which are listed in section 1. The security of proposed protocol is examined and compared with previously published work [10, 11, 14, and 68] in tabular form.

**Table 6.4.1 Comparison of computation cost with existing protocol.**

| | [J. Zhang] | [J.G Choi] | [N.D. Memon] | [C. L. Lei] | [Proposed] |
|---|---|---|---|---|---|
| Encryption Operation | 3 | 2k+1 | 2 | 3 | 1 |
| Decryption Operation | 1 | 4 | 1 | 1 | 1 |
| ⊕ operation | 2 | 2 | 2 | 2 | 2 |
| Signing Operation | 1 | k | 2 | 2 | 1 |

k: is the number of watermark

Table 6.4.1 and Table 6.4.2 show the comparison of various results. In table 6.4.1, seller uses a tamper resistant device, which produces necessary watermarks and digital signature. Table 6.4.1 shows that the protocol can withstand all of the known problems, which are listed above and identify the true owner of digital content. Table 6.4.2 shows the various encryptions and decryption operation used in the proposed protocol author has used three sub-protocols watermark embedding and signing protocol, watermark detecting and verifying protocol and registration protocol. In this scheme, the number of communication rounds takes one encryption, one decryption, 2 watermark embedding, and one signing operation respectively which minimizes the pass time and also reduces overhead on WCA hence better when compare to others like [10, 11, 14, and 68] in tabular form. Furthermore, if buyer sent a request to purchase a product with anonymity then seller publishes the encrypted product to the buyer and seller is not able to trace the identity of the buyer. Hence, during the entire transaction the privacy of buyer is protected against the seller. In the case of WCA, it only has the credentials of buyer, but WCA is not aware about the product or digital content which buyer has bought hence buyer is also protected against WCA.

### 6.4.1 Dispute resolution problem

In the dispute resolution problem, if the seller takes evidence to the judge i.e. arbiter that the buyer is responsible for copyright violation. The seller does not exactly know where the watermark is embedded into the digital content X. The seller is unable to frame the buyer. When the arbiter asks to the buyer for the watermark W, the buyer can send some random watermark W′ instead of original W. The seller has presented the Judge with a signed and encrypted copy of the watermark W, and this watermark W will not match the watermark W′ presented by the buyer. Then the buyer would be considered as spurious buyer. For that, WCA finds value of watermark W in place of watermark W′ with the help of equation no. 6.3.1.3. WCA takes the final decision based on this equation.

$$(ID_S, t, X, W, X_W) = SD_{K_{wca}}(C)$$

### 6.4.2 Unbinding problem

Unbinding problem is solved because in this, first the seller does not know the buyer's watermark $W_B$, because the watermark is embedded by a trusted third party, i.e. WCA under encryption algorithm. The buyer's signature binds to the ARG that uniquely identify a particular digital content X. These aspects make it impossible for the seller to transplant the watermark into another copy of the forged digital content.

When, both buyer and seller argue to prove ownership of the similar media $Z$, then arbiter executes the watermark detecting and verifying protocol to specify whom the lawful possessor of the digital content $Z$ is. For determining the robustness of the underlying watermarking algorithm he check the result of equation no. (6.3.2.1). If the digital signature, i.e. is $Ds$ is generated by the $WCA$ then the equation no. (6.3.2.2) should be reliable.

$$\mathrm{D}_{\mathrm{H}(\mathrm{w}_\mathrm{k})}(\mathrm{Z}, \mathrm{X}, \mathrm{W})$$

$$\mathrm{Ver}_{\mathrm{PC}_{\mathrm{wca}}}(\mathrm{Ds}) = (\mathrm{ID}_\mathrm{S}, \mathrm{t}, \mathrm{W}, \mathrm{H}(\mathrm{w}_\mathrm{k}))$$

In the case of watermark embedding and signing protocol cipher text C and digital signature Ds are transmitted between the WCA and seller. Because ciphertext C is encrypted using the public key of PCwca of WCA, an unauthorized person cannot obtain the digital content X and $X_W$ from the ciphertext C and digital signature Ds because the original digital content X and watermarked data $X_W$ are kept secret in watermark embedding and signing protocol. Hence, the buyer can obtain $X_W$ only if after seller publicizes the watermarked data, then arbiter can determine that the seller is the rightful owner or not.

From the above analysis, the proposed protocol can solve the common problems, which are presented in Section 1 and design goals are also achieved which are given in Section 3. The protocol has come at some modification based on the previous publish protocol like it he did not embed second watermark into the original digital content, the buyer need to interact with the seller, arbiter and the WCA in the transaction process and the seller and WCA are used for issuing the valid watermark. Hence, the seller is unable to bind a watermark for framing the innocent buyer i.e. the unbinding problem is resolved and if any disputed occurs between buyer and seller then WCA and arbiter solved that issue using time-stamp based technique to establish use of timestamp at what time the digital content or signal was created, signed or verified i.e. dispute resolution problem is resolved.

## 6.5 Experimental Result

All previously proposed buyer-seller watermarking protocol uses Cox [20] method to gain robust watermarking. However, in this proposed protocol, author adopts wavelet and principal component analysis based techniques [69] with identity-based public key cryptography for achieving high robustness. Hence, author claimed the novelty of his proposed scheme as his protocol is more robust and imperceptibility is very high. The test set comprises images from standard color image dataset [http://graphics.cs.williams.edu/data/images.xml], as well as well-known images such as Lena, peppers, fruit and Baboon. He has presented various parameters for analyzing performance of the proposed protocol.

**6.5.1 Peak Signal-To-Noise Ratio (PSNR): -** Peak Signal-To-Noise Ratio is generally applied to analyze quality of picture.

$$\mathrm{PSNR} = 10 * \log \frac{255^2}{\mathrm{MSE}} \qquad \textbf{(6.5.1)}$$

**6.5.2 Mean Square Error (MSE):-** It represents the cumulative squared error between the watermarked image and the original image.

$$\mathrm{MSE} = \sum_{i=1}^{x} \sum_{j=1}^{y} \frac{(|A_{i,j} - B_{i,j}|)^2}{x * y} \qquad \textbf{(6.5.2)}$$

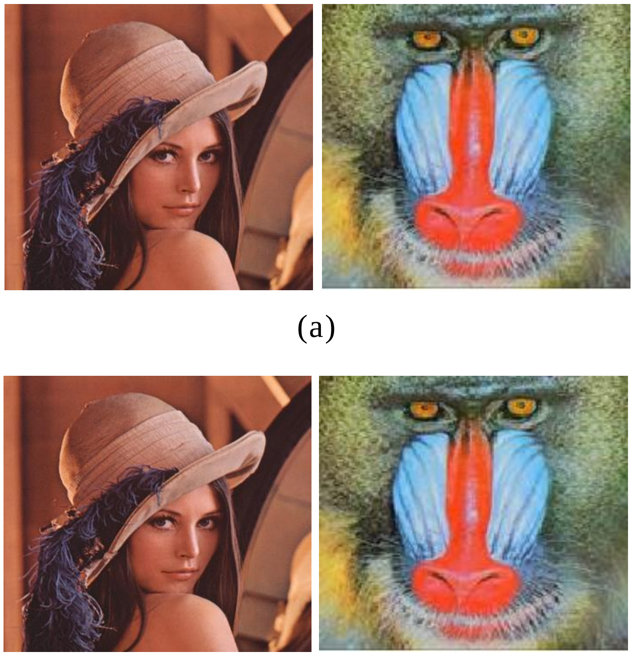
Where x is width of the image and y is height and $x * y$ is the no. of pixels.

**6.5.3 Normalized Correlation Coefficient (NCC):-** It is used for calculating the robustness of the algorithm.

$$\mathrm{NC} = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} A_{i,j} B_{i,j}}{\sum_{i=1}^{m} \sum_{j=1}^{n} A_{ij}^{2}} \qquad \textbf{(6.5.3)}$$

Where $A_{i,j}$ and $B_{i,j}$ denote the pixel values in row i and line j of the original watermark and the exacted watermark respectively.

The correctness of the proposed approach depends upon the robustness of watermarking embedding and extracting scheme. In his scheme, he set α =0.01 i.e. watermark embedding coefficient factor. For instant, he has chosen Lena and Baboon images for producing his result. Figure 6.5.1 shows the original test images and watermarked test images. The various watermark logos i.e. JNU logo and copyright logo are shown in figure 6.5.2. These watermark logo are embedded into the original images for proving the owner of the digital content. Some attacks are applied to the watermarked images for checking the robustness of the proposed scheme. The primary objective of the protocol is to solve the entire problem, which is solved by Zhang el al. and as well dispute resolution problem, and unbinding problem. The embedding method uses wavelets and principal component analysis technique [69] with identity based public cryptography for getting the watermark while the existing protocol uses Cox’s embedding method [20] which is based on DCT transform.



(a)

(b)

***Figure 6.5.1 a)*** *Original Test Image b) Watermark Test Images*

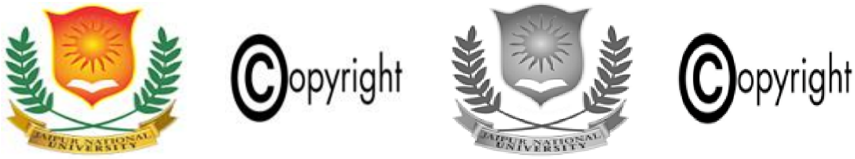
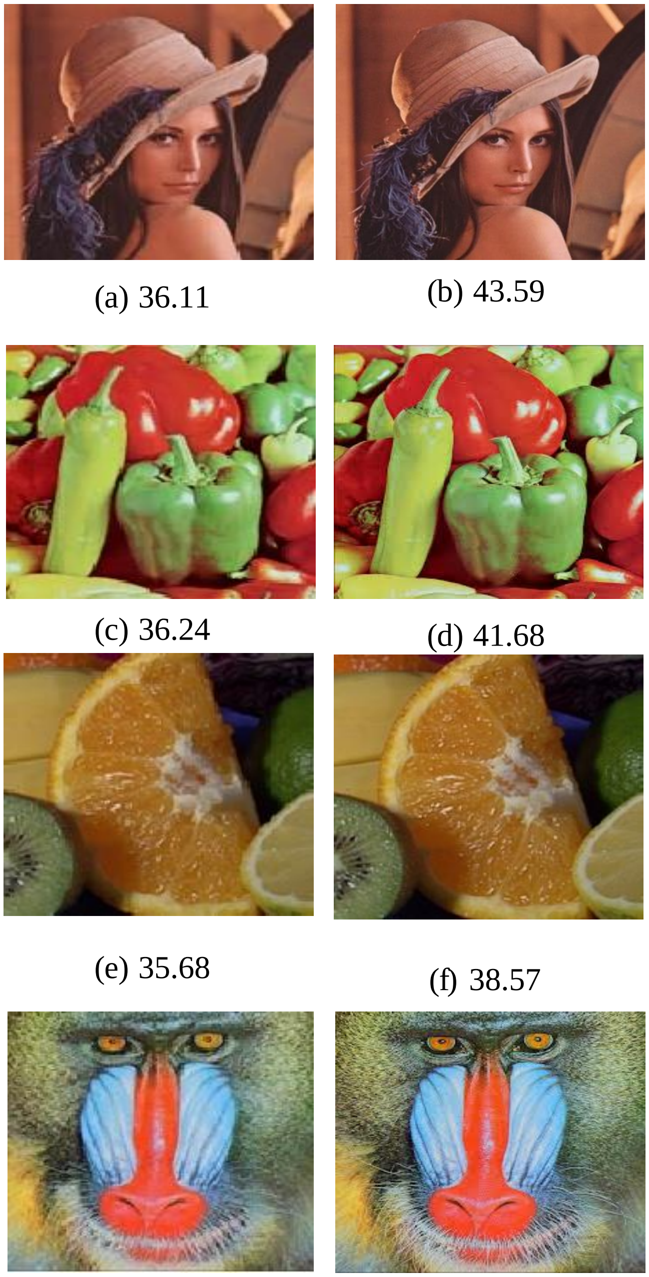


***Figure 6.5.2*** *Watermarks logos (a) JNU (b) Copyright (c) gray scale JNU (d) gray scale Copyright*



(a) 36.11

(b) 43.59

(c) 36.24

(d) 41.68

(e) 35.68

(f) 38.57

(g) 32.18

(h) 39.25

***Figure 6.5.3*** *The watermarked images on left side are created by the buyer and right sides are created by the seller.*

In the watermarking process, WCA generates the valid watermark images seller uses wavelet and principal component analysis transform for creating correlation coefficient and buyer executes these correlation coefficients for generating the watermarked image. Figure 6.5.3 shows the watermarked images created by both buyer and seller. It is clear that the PSNR value of Figure 6.5.3 left side is lower than the right side. The left side of the Figure 6.5.3 shows the watermarked images generated by the buyer and the right side of the figure show watermarked images generated by the seller. Table 6.5.1 shows the PSNR values corresponding to seller and buyer. Here, for calculating the robustness of the watermark embedding scheme author has applied several types of attacks to the watermarked images.

**Table 6.5.1 Peak signal to noise ratio (PSNR) dB created by both buyer and seller for each original color image.**

| PSNR(dB) | Lena | Pepper | Fruit | Baboon |
|---|---|---|---|---|
| **Buyer** | 36.11 | 36.24 | 35.68 | 32.18 |
| **Seller** | 43.59 | 41.68 | 38.57 | 39.25 |

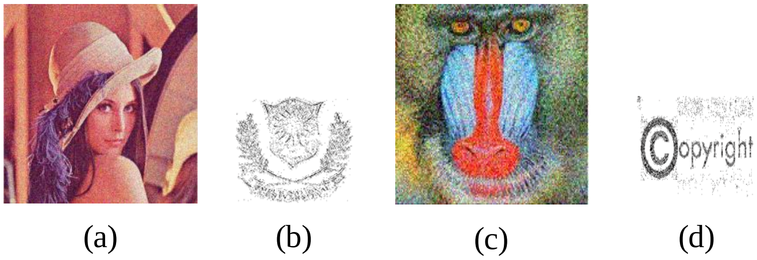


***Figure 6.5.4 a)*** *Watermarked Lena Image after Gaussian Noise at 0.02 b) Extracted Watermark c) Watermarked Baboon Image after Gaussian Noise at 0.02 d) Extracted Watermark.*

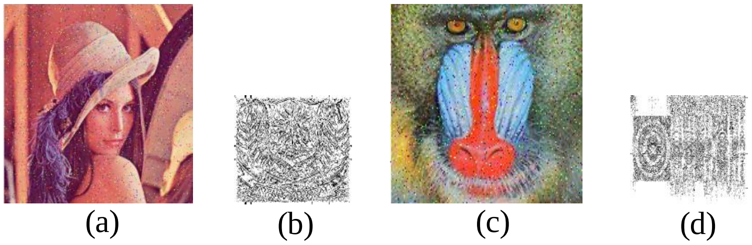


***Figure 6.5.5*** *a) Watermarked Lena Image after Salt & Pepper Noise at 0.02 b) Extracted Watermark c) Watermarked Baboon Image after Salt & Pepper Noise at 0.02 d) Extracted Watermark.*

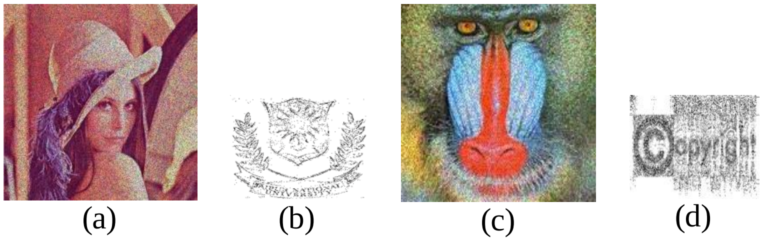


***Figure 6.5.6*** *a) Watermarked Lena Image after Speckle Noise at 0.03 b) Extracted Watermark c) Watermarked Baboon Image after Speckle Noise at 0.03 d) Extracted Watermark.*

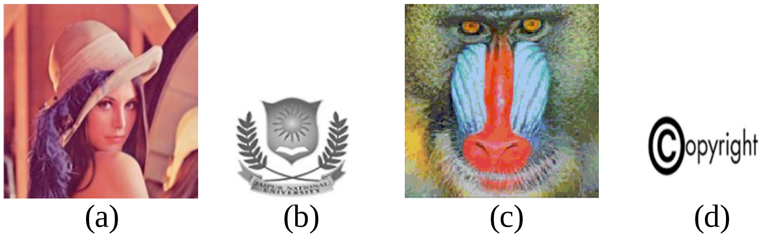


***Figure 6.5.7*** *a) Watermarked Lena Image after Median Filter at [5 5] b) Extracted Watermark c) Watermarked Baboon Image after Median Filter at [5 5] d) Extracted Watermark.*

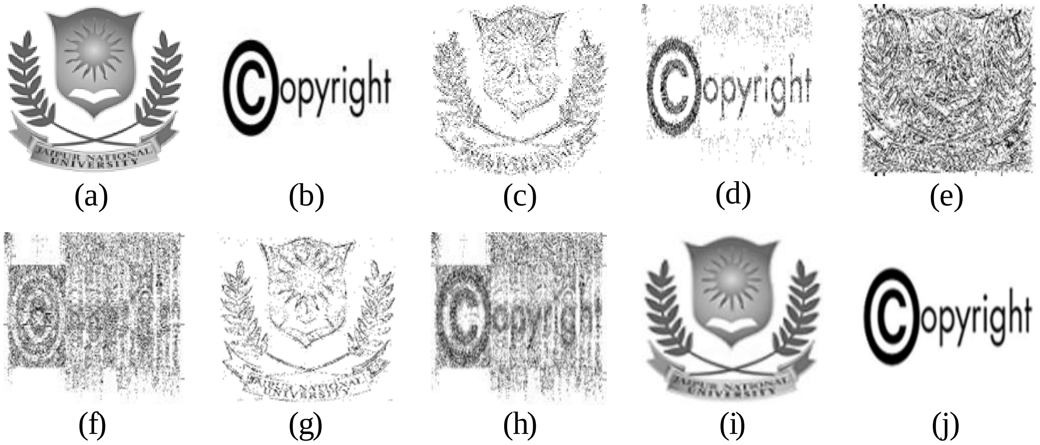


***Figure 6.5.8*** *Extracted Watermark Images*

In Figure, 6.5.4 author has applied Gaussian noise with density of 0.02 to the watermarked Lena and Baboon image, the JNU watermark logo and copyright logo are embedded respectively. The quality of the extracted watermark logos is good with the presence of attacks. To check the quality of these watermarks he has calculated correlation coefficient by using equation no. (6.5.3). The corresponding correlation coefficients are shown in Table 6.5.2.

Figure 6.5.5 shows the performance of the scheme against the salt & pepper noise author has applied this noise with density of 0.02 on the Lena and baboon watermarked images then he has extracted the corresponding watermarks.

In Figure 6.5.6 author has applied speckle noise with 0.03 density on Lena and Baboon watermarked images then corresponding watermark are extracted. In this he got good result and watermarks are still extracted.

Filtering is the most common attacks on digital images. So author has applied median filter to both watermarked images with filter size M=5 in figure 6.5.7. The results show that watermarks are easily recognized. If he will increase the filter, size normalized correlation will decreases. Figure 6.5.8 (a,b) shows the original watermarks and (c,d,e,f,g,h,i,j) shows the extracted watermarks from Lena, and Baboon images. To measure the quality of watermarked images he has PSNR by equation no. (6.5.1). Figure 6.5.8 shows the watermarked images and corresponding PSNR values are shown in Table 6.5.2.

**Table 6.5.2 PSNR Values of all test images.**

| Images | Lena | Pepper | Fruit | Baboon |
|---|---|---|---|---|
| PSNR | 43.59 | 41.68 | 38.57 | 39.25 |

Table 6.5.3 shows the various result of the proposed scheme. Author has successfully extracted the watermark from Gaussian noise, salt & pepper noise, Speckle noise and Median filter attacks. It is noticeable that in the case of Median filter and Gaussian noise the performance of his scheme is quite impressive. Hence, the scheme is very robust against Salt & pepper noise and Median filter attack and shows better performance. Table 6.5.2 shows that the corelation coefficient values for the extracted watermark and PSNR values for the attacked watermark images. The imperceptibility and robustness the watermark embedding scheme is very high.

## 6.6 Conclusion

In this chapter, author presents an identity-based buyer-seller watermarking protocol which can solve the various problems of the previously published protocol and free from all know attacks. In addition, he makes use of a tamper resistance device, which is embedded into seller’s computer and reduces the overhead on WCA. WCA maintains its own table and keeping the requested IDs of both buyer and seller. Hence, it is not required for WCA to participate in each transaction of the digital content between buyer and seller. Author also adopts wavelet and principal component analysis based techniques [69] to increase the robustness and imperceptibility of his embedding scheme. The watermark certificate authority will be responsible for issuing the digital signature corresponds to ID of the seller. If the problem of multiple ownership occurs, then it is the duty of an arbiter to decide it. The arbiter checks the correctness of data used by the seller, and then the arbiter compares the timestamps for determining the true possessor of the digital content. These changes enable the proposed protocol is really secure, feasible and efficient.

The contribution toward this research is published and is as follows:

[1] Ashwani Kumar, S.P Ghrera, and Vipin Tyagi, An ID-based Secure and Flexible Buyer-seller Watermarking Protocol for Copyright Protection, Science & Technology, Pertanika J. Sci. & Technol. Vol. 25, no. 1, pp. 57 – 76, January 2017.

# CHAPTER # 7

## A LIGHTWEIGHT BUYER-SELLER WATERMARKING PROTOCOL BASED ON COMPOSITE SIGNAL REPRESENTATION AND TIME-STAMPING TECHNIQUE

### 7.1 Introduction

The protocol allows a content provider to detect duplicate copy of a digital content and restrict the content provider who blame the innocent customer. This chapter, proposed a lightweight protocol, which uses composite signal representation and time-stamping for watermark embedding and extraction. Author make uses of time-stamp (at what time the digital content or signal was created, signed or verified) to digital watermarking algorithms and uses the composite signal representation for minimizing the overhead and bandwidth due to the use of composite signals. The suggested protocol uses composite signal representations and time-stamp based methods with digital watermarking schemes for content authentication. The proposed watermark embedding and detection algorithm achieves a balance between robustness and image visual quality. Simulation results demonstrate that the algorithm used by proposed protocol has a increase robustness and good quality of watermark images as well and withstand against various image processing attacks.

Increased growth of internet requires a digital copyright-based method to control the flow of multimedia data over internet. Digital watermarking [4, 5] is an effective method to protect the rights for the participant involving in e-commerce. These concepts are used by different watermarking scheme for protecting the intellectual property law and digital right for audios, pictures, and other multimedia content [11]. Time-stamp based methods [67, 72] are used to identify on which time a certain digital content was created, signed or verified. However, digital content can be very easily reproduced by the owner of the digital contens because he knows where the exact watermark is inserted into the digital content. Time-stamp based scheme is used to protect copyright with the help of time-stamp. The possibility of processing encrypted signals directly receiving an increasing attention from applications by non-trusted party.

In this chapter, author focuses on techniques based on homomorphism encryption, since they constitute the basis for any practical implementation of signal processing in encrypted domain theory. Digital watermarking schemes can broadly categorized into public key watermarking schemes and private key watermarking schemes [67, 73].

The proposed protocol allows the content provider to insert the watermarked content with their private watermark key. The content provider uses watermark certificate authority that is trusted third party that issues a valid signature contains the credentials of content provider and uses a time-stamp i.e. at that time the digital content was created, signed or verified. Here, author proposes a lightweight buyer seller watermarking protocol (BSWP) based on composite signal representation and time-stamp for copyright protection, which allows the seller to generate the watermarked content with their private watermark key. The watermark certificate authority will then generate a digital signature associated with the identity of the seller and time-stamp [68] of the watermarked content, watermark and original content. If any dispute occurs between buyer and seller at a later stage, with the help of arbiter one can resolve that issue arbiter first verify the validity of information provided by each claimer (seller). The arbiter to determine the appropriate seller of digital content compares time-stamps. With the help of time-stamps, the problems described in chapter one are also solved. Some key points of the proposed watermarking protocol are described below:

1. The watermark certificate authority *WCA* is not required to store any messages relating to the signed verification between the buyer and seller.

2. This watermarking protocol must be independent of all watermarking schemes.

## 7.2 Related Work

In this section, author has shown the related work of this field. There are many digital watermarking protocols proposed in history, they use cryptography techniques for embedding and extracting watermark. The digital watermarking scheme focuses to improve the robustness of the watermark and imperceptibility of the watermarked image and it reduces the complexity of the underlying scheme. Signal representation allowing us to bind together a number of signal samples and process them as a unique sample. The representation permits us to speedup linear operation on encrypted signals via parallel processing and reduce the size of encrypted signal. Signal processing tools work directly on encrypted data could provide an efficient solution to application scenario where sensitive signals must be protected from non-secure communication channels. Haber and Stornetta [73] proposed a time-stamp based protocol with watermark certificate authority.

$$S = sig_{TSS}(n, t_n, ID_n, X_n, L_n) \qquad \textbf{(7.2.1)}$$

Signal processing in the encrypted domain is a field of research, which aims for developing different tools for processing encrypted data [74]. Composite representation of signals [75] enables to group multiple signal samples into a single unit and to perform basic linear operations on them.

This chapter presents, a new buyer-seller watermarking protocol based on composite signal representation and time-stamp, which is secure and flexible to solve the various problems defined above.

## 7.3 Requirements for the Proposed Protocol

In this section, author has shown the various requirements of proposed protocol.

### 7.3.1 Requirement for cryptographic operation

A efficient and secure BSWP [69] should solve the problems which exist in buyer-seller watermarking protocol.

- *Certification authority obligation*- The problem is to provide a digital certificate for both purchaser and vendor. A vendor may fabricate piracy to frame the purchaser.
- *Customer's rights problem*- This problem indicates that after legally purchasing the digital content still the seller attempt to frame an innocent buyer, because the seller may make and distributed a copy of digital content which the buyer has purchased.
- *Copy detection problem*- Pirated copy of content or data must be detectable and traceable back to the owner of the original copy.
- *Piracy tracing* - The protocol should be able to trace the pirated copy when it found. The seller should be able to trace and identify the copyright violator.
- *The unbinding* - Unable to bind a watermark for a particular digital content or transaction. The seller may distribute pirated by transplanting the buyer's watermark into other contents.

### 7.3.2 Image Processing Requirements

In general, secure digital watermarking [6] scheme should satisfy the following requirements.

- *Kerckhoffs principle:* The digital watermarking algorithm should be secure enough for the system because the watermark key is public and known by all participants.
- *Robustness:* The capability of watermark to resist various image processing attacks such as rotation, scaling, clipping etc.

- *Imperceptibility:* The optical distortion of the watermarked image should not have on the quality of the original painting.
- *Effectiveness:* The algorithms for embedding and extracting the watermark into the digital content should be effective.

### 7.3.3 Composite signal representation

Signal representation is a technique, which enables us to increase the speed of linear operations on encrypted domain. Due to the nature of composite signal representation, the size of the encrypted signals can be reduced as well. It allows us to increase the speed for linear operations on encrypted domain. Due to the nature of composite signal representation, the size of the encrypted signals can be reduced as well. Most of image processing operations can be applied on composite signals. General composite signal representation allows combining no. of signals and processing them as a unique sample. Image processing operations can work directly on encrypted data and provide us an efficient solution for the application which are very sensitive and must be protected during the exchange of secret information.

### 7.3.4 Time-stamping technique

Time-stamping [67] based methods are applicable to identify when a digital signature was created, signed or verified at what time. Time-stamping [76, 77] is a technique that is used to identify on which time a certain digital content was created, signed or verified. However, digital content can very easily reproduced the owner of the digital media can use this scheme to protect his/her copyright through verification with the help of time-stamp. Digital content such as images have a unique characteristic i.e. they allow some sort of distortion. A duplicate seller can utilize this characteristic by slightly modifying the digital content. Now a day's digital content are reproduced very easily, so there is a problem to identify real owner of digital content. To overcome this issue the rightful owner can use this technique to protect his copyright or watermark through verification of the time-stamp.

## 7.4 Proposed Lightweight Buyer-Seller Watermarking Protocol (BSWP) Based on Composite Signal Representation and Time-Stamping Technique

In this proposed protocol, author has used same trust model used by [5] and [11]. This paper is an extension of his previous work [31, 69]. Here author proposed a lightweight BSWP which uses signal representation and time-stamp for secure distribution of digital content. Author proposed a hybrid and effective embedding technique in the encrypted domain. The proposed protocol is based on public key cryptosystem, arbiter, trusted third party, and time-stamping services [24, 78, 79, 80, and 81]. In history a secure protocol is one, which consists of three sub-protocols i.e. the registration protocol, watermark generation and insertion protocol, and identification and arbitration protocol. In this chapter, author has focussed only in watermark generation and insertion protocol for generating and extracting watermark other two protocols are remain same as previous proposed protocol. Author has used tamper resistance device and time-stamp based technique to make his approach better for enhancing the security to the buyer and seller. Tamper resistance device is used to reduce the overhead on WCA and time-stamp are used keep the records of transaction done by customer and content provider. Figure 7.4.1 shows the proposed protocol.

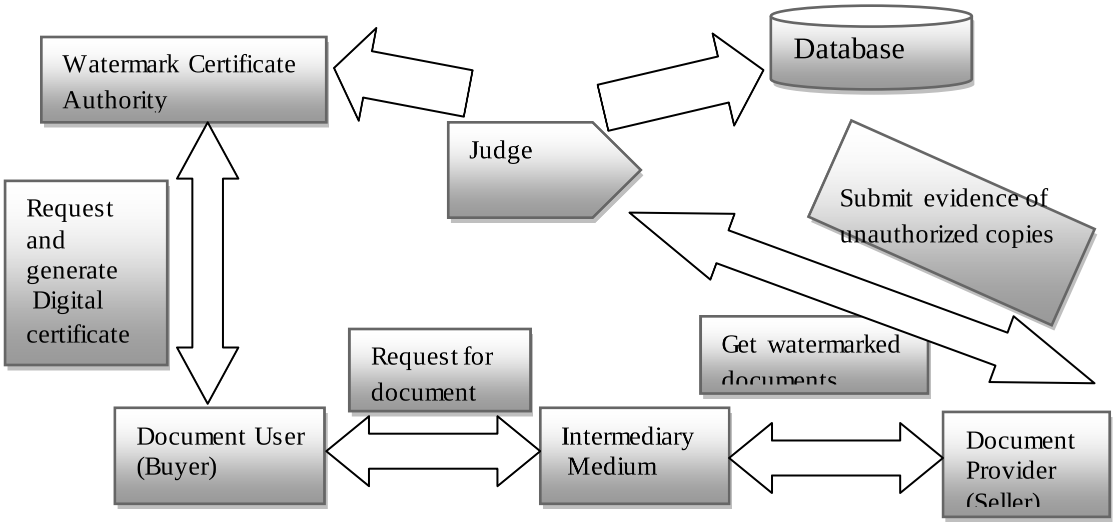

Watermark Certificate Authority
Database
Judge
Submit evidence of unauthorized copies
Request and generate Digital certificate
Request for document
Get watermarked documents
Document User (Buyer)
Intermediary Medium
Document Provider (Seller)

***Figure 7.4.1*** *Proposed lightweight BSWP protocol*

The proposed protocol consists of two sub-protocols, i.e. registration protocol and watermark insertion and detection protocol. Here, author has used time-stamp based public key cryptosystem and has five different roles i.e. buyer, seller, watermarking certificate authority, judge and intermediary.

**Seller:** The owner of the digital content or from where the buyer wants to purchase the digital content.

**Buyer:** Who wants to take the true possession of the digital content that does not go to him.

**WCA:** Watermark certification authority, responsible for issuing public and secret key for the buyer and seller. *WCA* also issues the digital signature based on the private key.

**ARB:** *ARB* stands for an arbiter, who adjudicates lawsuits against the infringement of copyright and intellectual property.

**Time-stamping service:** Time-stamping service (TSS), who signs the current time for the submitted digital document by the submitter.

**7.4.1 Registration protocol:-** This protocol [78] takes place between the customer and the WCA. If a buyer wants to hide his identity into a transaction of digital content, then buyer randomly selects a pair of key and sends it to a trustworthy WCA.

**7.4.2 Watermark generation and extraction protocol:-** This protocol uses secure and robust digital watermarking scheme to generate and extract the watermark. He has used wavelets and principal component analysis [78] methods for doing this.

## 7.5 Security Analysis and Discussion

Underlying security of the protocol relays on the watermarking embedding and detecting scheme and cryptosystem, which author has used for secure communication between buyer and seller. Table 7.5.1 shows the security of the proposed protocol is examined and compared with previously published work [5, 11, 14, and 68]. Table 7.5.1 shows encryption, decryption, homomorphism and signing operation used by cryptosystem which author has used in proposed protocols.

**Table 7.5.1 Comparison of computation cost with existing protocol.**

| | [J. Zhang] | [J.G Choi] | [N.D. Memon] | [C. L. Lei] | [Proposed] |
|---|---|---|---|---|---|
| Encryption Operation | 3 | 2k+1 | 2 | 3 | 1 |
| Decryption Operation | 1 | 4 | 1 | 1 | 1 |
| $\oplus$operation | 2 | 2 | 2 | 2 | 2 |
| Signing Operation | 1 | k | 2 | 2 | 1 |

k: is the number of watermark

The proposed protocol solves all the problems which exist in previously published buyer-seller watermarking protocol. Anonymity is resolved because author has used registration protocol, which contains credentials of all buyers. Unlinkability problem is solved because underlying time-stamp and composite signal representation based method give the purchase information and there is one time interaction between buyer and seller.

## 7.6 Experimental Result

Previously proposed buyer seller watermarking protocol uses Cox method to gain robust watermarking. However, in this author has adopted wavelet and principal component analysis based techniques [69] with time-stamp based public key cryptography for achieving high robustness. In his scheme, he sets α =0.01 i.e. watermark embedding coefficient factor. The test set comprises of various test images in which some images have been taken from the standard grayscale image dataset [http://decsai.ugr.es/cvg/CG/base.htm] and well-known images Lena, Cameraman, Barbara and Man respectively. Figure 7.6.1 shows the original test images and watermarked test images. The watermark logos i.e. JNU logo and copyright logo are embedded into the original test images. He has used

PSNR and NCC parameters for analyzing the quality of watermark and watermarked images. The presented method is implemented in MATLAB 10.

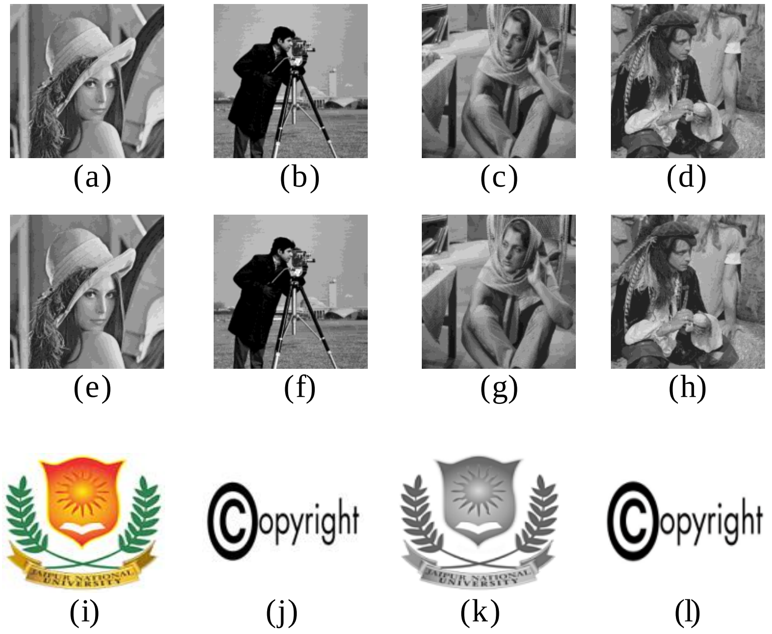


***Figure 7.6.1*** *Original images (a-d) watermarked images (e-h) and watermark images(i-j).*

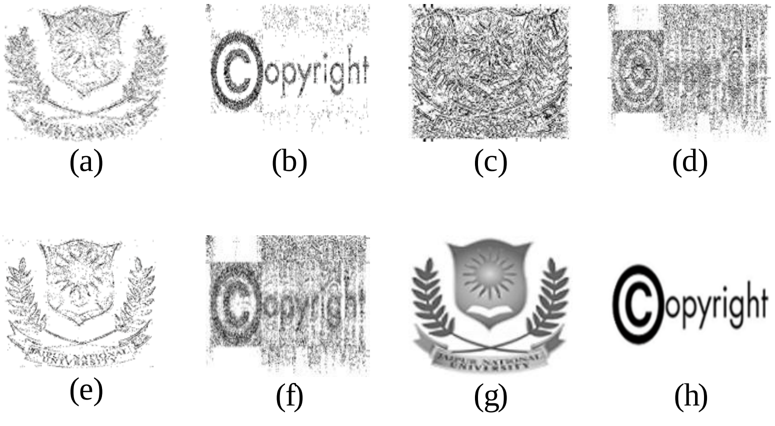


***Figure 7.6.2*** *Extracted watermark logo from watermarked images.*

For calculating the performance of the proposed scheme, author has applied various types of noises to the watermarked images. In Figure 7.6.2 he has shown the various extracted watermarks. For an instance, he only takes Lena and

Barbara image for producing the result. The scheme performs well when tested against various types of attacks the value of Peak Signal-To-Noise Ratio (PSNR) and Normalized Correlation Coefficient (NCC) are given in table 7.6.1 respectively.

**Table 7.6.1 PSNR values and Normalized correlation coefficient of all watermarked images and extracted logos after attacks.**

| **Images** | **Lena** | | **Cameraman** | |
|---|---|---|---|---|
| **Attacks** | **PSNR** | **NC** | **PSNR** | **NC** |
| Gaussian Noise | 40.59 | 0.8463 | 39.25 | 0.8131 |
| Salt & pepper Noise | 39.63 | 0.6338 | 35.10 | 0.5321 |
| Speckle Noise | 39.72 | 0.7842 | 37.61 | 0.6541 |
| Median Filter | 41.01 | 0.9762 | 40.49 | 0.9153 |

## 7.7 Conclusion

The author has proposed a lightweight protocol based on composite signal representation and time-stamping for multimedia data distribution. In addition, he makes use of a time-stamp based techniques which is used to store the information about at what time the digital content or signal was created, signed or verified. His proposed protocol uses digital watermarking algorithms with composite signal based methods for minimizing the overhead. His protocol uses a robust watermark embedding and extracting schemes this lead to higher demand for multimedia data like images with high visual quality. These aspects make proposed protocol really secure, feasible and efficient.

The contribution toward this research is published and is as follows:
[1] A. Kumar, S.P. Ghrera, and V. Tyagi, “A lightweight buyer-seller watermarking protocol based on composite signal representation and time-stamping for multimedia data distribution.” in International Conference on Engineering and Material Sciences (ICEMS-2016). [Indexed in Scopus, and published in SCIENCE DIRECT].

# CHAPTER # 8

## CONCLUSION AND FUTURE WORK

### 8.1 CONCLUSION

This thesis emphasizes on watermarking embedding and extraction scheme into the buyer-seller watermarking protocol. Firstly, author has emphasized on watermark generation protocol and watermark insertion protocol. Secondly, author has worked on cryptosystem with digital watermarking scheme, which uses id-based public key cryptography for providing more security to the buyer and seller. In this, he also makes use of a tamper resistance device to reduce the overhead on WCA as TTP. The last section of the thesis concludes the research work and addresses the scope for future enhancements.

In chapter 3, a robust and efficient watermarking embedding and extraction scheme based on discrete wavelet transform to improve the robustness and imperceptibility of the watermark has been proposed. Unlike existing buyer-seller watermarking protocol, this approach uses wavelet based methods for watermark embedding and extraction these methods are more robust.

In chapter 4, the author proposed a watermarking embedding and extraction scheme as an improved variation of the above scheme, which makes use of principle component analysis with wavelets together for further increasing the robustness of the watermark. The method is implemented using 3-level discrete wavelet transform (DWT) with principal component analysis (PCA) transform. The method is also image dependant and able to survive under geometric distortion and image processing attacks. PCA transform help us for reducing correlation coefficient among the wavelet coefficients. Author has decomposed the original image up to 3 levels, then he select only HL3 and LH3 bands of the DWT image, then watermark bits are inserted into the principal components PCs. PCA is a powerful tool for analyzing data and finding patterns in it. PCA gives a high compression rate and performance is good when noise is present. It is also used for removing the correlation coefficients amongst the dataset. These aspects make proposed protocol more efficient and robust.

Chapter 5 studies the comparison of both domains i.e. discrete cosine transform and discrete wavelet transform and concludes which one is better on the bases of robustness and imperceptibility.

Chapter 6 proposed a cryptosystem with digital watermarking scheme which uses id-based public key cryptography for providing more security to the buyer and seller. The suggested protocol uses Id-based public key cryptography and digital watermarking scheme to place the ownership of digital content. Hence, copyright protection is attained. WCA maintains its own table and keeping the requested IDs of both buyer and seller. Hence, it is not required for WCA to participate in each transaction of the digital content between buyer and seller. The watermark certificate authority will responsible for issuing the digital signature corresponds to ID of the seller. If the problem of multiple ownership occurs, then it is the duty of an arbiter to decide it. The arbiter checks the correctness of data used by the seller, and then the arbiter compares the timestamps for determining the true possessor of the digital content. The suggested protocol is efficient and have adequate security from traditional proposed protocols and suitable for any practical buyer seller watermarking scheme.

Chapter 7 has presented a scheme in which time stamp based technique can be used by TTP to keep accountability of digital signature based on composite signal representation to provide a secure communication between buyer and seller.

This thesis proposed new methods for embedding and extracting the watermark and increase the robustness and imperceptibility. Results show that the proposed embedding approaches are better than the previously proposed scheme in case of robustness and imperceptibility.

## 8.2 Future Work

In future, the work can be done to provide more effective solutions for the identified problems. In addition, the presented methods for embedding and extracting the watermark can be tested on other gray-scale image datasets for further establishing their efficacy. The research can further be expanded by studying the effect of other optimization techniques.

# REFERENCES

[1] F.N. Lang, et al, “A self-adaptive image normalization and quaternion PCA based color image watermarking algorithm,” *Expert Systems with Applications*, vol. 39, no. 15, pp. 12046–12060, 2012.

[2] V. Santhi, N. Rekha, and S. Tharini, “A hybrid block based watermarking algorithm using DWT-DCT-SVD techniques for color images,” *Int. Conf on Computing, Communication and Networking*, pp. 1–7, 2008.

[3] C.Q. Yin, and L. Li, “A color image watermarking algorithm based on DWT-SVD,” *IEEE Int. Conf. on Automation and Logistics, Jinan*, pp. 2607–2611, 2007.

[4] F. Mintzer, and G. W. Braudaway, “If one watermark is good, are more better?,” *In Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP ’99)*, vol. 4, Phoenix, Ariz, USA, pp. 2067–2069, 1999.

[5] P. W. Wong, and N. Memon, “Secret and public key image watermarking schemes for image authentication and ownership verification,” *IEEE Transactions on Image Processing*, vol. 10, no. 10, pp. 1593–1601, 2001.

[6] P. Zeng, Z. Cao, and K.R Choo, “An ID-based digital watermarking protocol for copyright protection,” *Computers and Electrical Engineering*, vol. 37 pp. 526–531, 2011.

[7] A. Rial, J. Balasch, and B. Preneel, “A privacy-preserving buyer-seller watermarking protocol based on priced oblivious transfer,” *IEEE Transactions on Information Forensics and Security*, pp. 202–212, 2011.

[8] X. Cui, G. Sheng, F. Li, and X. Liu, “An Efficient and Impartial Buyer-Seller Watermarking Protocol,” *Journal of Communications,* vol. 10, pp. 339-344, 2015.

[9] M. Deng, and B. Preneel, “On Secure and Anonymous Buyer-Seller Watermarking Protocol,” *Third International Conference on Internet and Web Applications and Services,* pp. 524-529, 2008.

[10] N. D. Memon, and P. W. Wong, “A Buyer-Seller Watermarking Protocol,” *IEEE Transactions on Image Processing,* vol. 10, no. 4, pp. 643–649, 2001.

[11] C. L. Lei, P. L. Yu, P. L. Tsai, and M. H. Chan, “An Efficient and Anonymous Buyer–Seller Watermarking Protocol,” *IEEE Trans. Image Process.,* vol. 13, no. 12, pp. 1618-1626, 2004.

[12] C. de Carvalho J, and Sequeira L, “Buyer-seller conflict and cooperation in marketing channels: port wine distribution,” *International Journal of Wine Research,* 2013.

[13] P. Zeng, Z. Cao, K.R. Choo, “An ID-based digital watermarking protocol for copyright protection,” *Computers and Electrical Engineering,* Vol. 37, pp. 526-531, 2011.

[14] J.G. Choi, K. Sakurai, and J.H. Park, “Does it need trusted third party? Design of buyer-seller watermarking protocol without trusted third party,” *In: Zhou, J., Yung, M., Han, Y.(eds.) ACNS 2003. LNCS,* vol. 2846, pp. 265–279, 2003.

[15] H.S. Ju, H.J. Kim, D.H. Lee, and J.I Lim, “An anonymous buyer-seller watermarking protocol with anonymity control,” *In: Lee, P.J., Lim, C.H. (eds.) ICISC, LNCS,* vol. 2587, pp. 421–432, 2002.

[16] P. Tay, and J. Havlicek, “Image watermarking using wavelets,” *in Proc. of the IEEE Midwest Symposium on Circuits and Systems,* pp. 258-261, 2002.

[17] R. Wolfgang, C. Podilchuk and E. Delp, “Perceptual watermarks for digital images and video,” *Proc. of the IEEE,* vol. 87, no. 7, pp. 1108-1126, 1999.

[18] R. Eslami, and H. Radha, “Wavelet based contourlet transform and its application to image coding,” *in Proceedings of the IEEE International Conference on Image Processing (ICIP’04), IEEE Signal Processing Society,* pp. 3189–3192, 2004.

[19] P. Kumhom, and K. Chamnongthail, “Image watermarking based on wavelet packet transform with best tree,” *Ecti. Transactions on Electrical-eng, Electronics, and Communications,* vol. 2, no. 1, pp. 23-35, 2004.

[20] I.J. Cox, M.L. Miller, and J.A Bloom, “Digital Watermarking,” *Morgan Kaufmann Publishers, San Francisco*, 2002.

[21] M. Kutter, F. Hartung, and S.C. Katzenbeisser, “Introduction to Watermarking Techniques,” *Information Techniques for Steganography and Digital Watermarking, Eds. Northwood, MA: Artec House,* 1999.

[22] N. F. Johnson and S. C. Katezenbeisser, “A Survey of Steganographic Techniques,” *Information Techniques for Steganography and Digital Watermarking,* pp. 43-75, 1999.

[23] L. Qiao, and K. Nahrstedt, “Watermarking Schemes and Protocols for Protecting Rightful Ownership and Customer’s Rights,” *Journal of Visual Communication and Image Representation*, vol. 9, no. 3, pp. 194–210, 1998.

[24] B.-M. Goi, R. C.-W. Phan, Y. Yang, F. Bao, R. H. Deng, and M. U. Siddiqi, “Cryptanalysis of Two Anonymous Buyer-Seller Watermarking

Protocols and An Improvement for True Anonymity," *In Applied Cryptography and Network Security, LNCS 2587*, pp. 369–382, 2004.

[25] M. Kuribayashi, and H. Tanaka, "Fingerprinting protocol for images based on additive homomorphic property," *IEEE Transactions on Image Processing,* vol. 14, no. 12, pp. 2129–2139, 2005.

[26] J. Zhang, W. Kou, and K. Fan, "Secure Buyer-Seller Watermarking Protocol," *IEEE Proceedings of Information Security,* vol. 153, no. 3, pp. 15–18, 2006.

[27] F. C. Chen, T. Ming, and S. Wei-Zhe, "Buyer-Seller Watermarking Protocols with Off-line Trusted Parties," *MUE '07. International Conference on Multimedia and Ubiquitous Engineering,* pp. 1035–1040, 2007.

[28] I. M. Ibrahim, S. H. N. El-Din, and A. F. A. Hegazy, "An effective and secure buyer-seller watermarking protocol," *In Third International Symposium on Information Assurance and Security, IAS 2007,* pp. 21–28, 2007.

[29] S. Katzenbeisser, A. Lemma, M. U. Celik, M. van der Veen, and M. Maas, "A buyer-seller watermarking protocol based on secure embedding," IEEE Trans. Inf. Forensics Security, vol. 3, no. 4, pp. 783–786, December 2008.

[30] Y. Hu, and J. Zhang, "A secure and efficient buyer-seller watermarking protocol," *Journal of Multimedia,* vol. 3, no. 4, pp. 161-168, 2009.

[31] A. Kumar, M. D. Ansari, J. Ali, K. Kumar, "A New Buyer-Seller Watermarking Protocol with Discrete Cosine Transform," *in CNC CCIS © Springer-Verlag Berlin Heidelberg,* vol. 142, pp. 468–471, 2011.

[32] A. Kumar, V. Tyagi, M. D. Ansari, and K. Kumar, “A Practical Buyer-Seller Watermarking Protocol based on Discrete Wavelet Transform,” *International Journal of Computer Applications,* vol. 21, no. 8, pp. 46-51, 2011.

[33] C. L. Chena, C.C. Chenb, D. K. Lic, and P.Y. Chend, “A Verifiable and Secret Buyer–Seller Watermarking Protocol,” *IETE Technical Review,* vol. 32, no. 2, pp. 104-113, 2015.

[34] V. Potdar, S. Han, and E. Chang, “A survey of digital image watermarking techniques,” *in Proc. of the IEEE International Conference on Industrial Informatics,* pp. 709-716, 2005.

[35] C. Chan, and L. Cheng, “Hiding data in Images by simple LSB substitution,” *Pattern Recognition,* vol. 37, no. 3, pp. 469-474, 2004.

[36] V. Tyagi, and J. P. Agarwal, “Digital Watermarking, Computer Society of India,” 2008.

[37] X. G. Xia, C. G. Boncelet, and G. R. Arce, “A Multiresolution Watermark for Digital Images,” *Image Processing 1997 Proceedings. International Conference,* vol. 1, pp. 548-551, 1997.

[38] J.C. Liu, C.H. Lin, and L.C Kuo, “A robust full band image watermarking scheme,” *Proceedings on IEEE,* 2006.

[39] A.A. Haj, et. al, “Combined DWT-DCT digital image watermarking,” *Journal of computer science,* vol. 3, no. 9, pp. 740-746, 2007.

[40] C. Nafornita, M. Borda, A. Kane, “A wavelet-based digital watermarking using sub-band adaptive thresholding for still images,” *microCAD,* pp. 87-92, 2004.

[41] D. Kundur, and D. Hatzinakos, “Diversity and attack characterization for improved robust watermarking,” *IEEE Transactions on Signal Processing,* vol. 49, no. 10, pp. 2383-2396, 2001.

[42] I. J. Cox, J. Kilian and T. Shamoon, “Secure spread spectrum watermaking for multimedia,” IEEE Transaction of Image Processing, *IEEE Computer Society,* vol. 6, no. 12, pp. 1673-1687, 1997.

[43] B. Wang, J. Ding, Q. Wen, X. Liao, and C. Liu, “An image watermarking algorithm based on DWT DCT and SVD,” *Proceeding of ICNIDC,* pp. 1034-1038, 2009.

[44] L. Fang-nian, et al, “A self-adaptive image normalization and quaternion PCA based color image watermarking algorithm,” *Expert Systems with Applications,* Vol. 39(15), pp. 12046-12060, 2012.

[45] T. D. Hien, Y.W. Chen, and Z. Nakao, “A Robust Digital Watermarking Technique based on Principal Component Analysis,” *International Journal of Computational Intelligence and Applications,* vol. 4, no. 2, pp. 138-192, 2004.

[46] L, Chih-Chin, and T. Cheng-Chih, “Digital image watermarking using discrete wavelet transform and singular value decomposition,” *IEEE Trans. Instrum. Meas,* vol. 59, no. 11, pp. 3060-3063, 2010.

[47] W. Shuo-zhong, “Watermarking based on principal component analysis,” *Journal of Shanghai University (English Edition),* vol. 4, no. 1, pp. 22-26, 2000.

[48] M. Kutter, S. K. Bhattacharjee, and T. Ebrahimi, “Towards second generation watermarking scheme,” *Image Processing, ICIP 99. Proceedings,* vol. 1, pp. 320-323, 1999.

[49] H. Olkkonen, “Discrete wavelet transforms algorithms and applications,” *InTech*, 2011.

[50] E. Yavuz, and Z. Telatar, “Digital watermarking with PCA based reference Images,” *Lecture Notes in Computer Science*, vol. 4678, pp. 1014-1023, 2007.

[51] S. Sinha, P. Bardhan, S. Pramanick, A. Jagatramka, D. K. Kole, and A. Chakraborty, “Digital video watermarking using discrete wavelet transform and principal component analysis,” *International Journal of Wisdom Based Computing, v*ol. 1, no. 2, 2011.

[52] I.N. Yassin, Nancy M. Salem, and Mohamed I. El Adawy, “Entropy based video watermarking scheme using wavelet transform and Principal Component Analysis,” *Engineering and Technology (ICET), International Conference on. IEEE*, 2012.

[53] R. Ray-Shine, Shi-Jinn H, Jui-Lin L, Kao T-W, Chen R-J, “An improved SVD-based watermarking technique for copyright protection,” *Expert Syst. Appl*. vol. 39, no. 1, pp 673–689, 2012.

[54] G. Bhatnagar, Wu QMJ, and Raman B, “A new robust adjustable logo watermarking scheme,” *Comput & Security*, vol. 31, pp. 40-58, 2012.

[55] A.A Mohammad, Alhaj A, and Sameer S, “An improved SVD-based watermarking scheme for protecting rightful ownership,” *Sig. Process*, vol. 88, pp. 2158-2180, 2008.

[56] P. Pandey, S. Kumar, and S. K. Singh, “A robust logo watermarking technique in divisive normalization transform domain,” *Multimedia Tools and Applications*, pp. 1-25, 2013.

[57] L. S. Hwan, K. S. Geun, and K. K. Ryong, “Mobile 3D Secure Transmission Based on Anonymous Buyer-Seller Watermarking Protocol,”

*Recent Advances in Communications and Networking Technology,* vol. 3, no. 1, pp. 33-43, July 2014.

[58] F. Shih, and Y.-T. Wu, "Information Hiding by Digital Watermarking," *Information Hiding and Applications,* vol. 227, 2009.

[59] I. Hartung, and F. Kuter, "Multimedia Watermarking Techniques," *Proceeding of the IEEE,* vol. 87, no. 7, pp. 1079-1107, 1999.

[60] F.-H. Wang, J.-S. Pan, and L. Jain, "Intelligent Techniques, Innovations in Digital Watermarking Techniques," *Studies in Computational Intelligence, Springer Berlin Heidelberg,* 2009.

[61] M.K. Vetterli, "Wavelets and Subband Coding," *Prentice Hall,* 1995.

[62] S. J. a. N. B. Hingoliwala H.A, "An image compression by using haar wavelet transform," *Advances in Computer Vision and Information Technology,* 2008.

[63] R. L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Communications of ACM,* vol. 21, 1978.

[64] C.-S. Shieh, H.-C. Huang, F.-H. Wang et al, "Genetic watermarking based on transform-domain techniques," *Pattern Recognition,* vol. 37, no. 3, 2004.

[65] S. Promcharoen, and Y. Rangsanseri, "Genetic Watermarking with Block-Based DCT Clustering," *In: ISCIT,* pp. 346-351 2008.

[66] K. Hameed, A. Mumtaz, et al, "Digital Image Watermarking in the Wavelet Transform Domain," *World Academy of Science, Engineering and Technology,* vol. 13, 2006.

[67] M.S. Hwang, K.F. Hwang, C.C Chang, “A time-stamping protocol for digital watermarking,” *Appl. Math Comput.*, vol. 169, no. 2, pp. 1276–1284, 2005.

[68] J. Zhang, W. Kou, and K. Fan, “Secure Buyer-Seller Watermarking Protocol,” *IEEE Proceedings of Information Security,* vol. 153, no. 3, pp. 15–18, 2006.

[69] A. Kumar, S.P Ghrera, and V. Tyagi, “Modified Buyer Seller Watermarking Protocol based on Discrete Wavelet Transform and Principal Component Analysis,” *Indian Journal of Science and Technology,* vol. 8, no. 35, pp. 1-9, 2015.

[70] A. Shamir et al, “Identity-based cryptosystems and signature schemes,” *Crypto’84,* pp. 48–53, 1985.

[71] P. Paillier et al, “Public key cryptosystems based on composite degree residuosity classes,” *In Proc. Eurocrypt’99, Stern, J. (Ed.): LNCS* vol. 1592, pp. 223-238, 1999.

[72] A. Buldas, P. Laud, H. Lipmaa, and J. Villemson, “Time-stamping with binary linking schemes,” *in: Advances in Cryptology-CRYPTO98,* pp. 486-501, 1998.

[73] S. Haber, and W.S. Stornetta, “How to time-stamping,” *Journal of Cryptology,* vol. 3, no. 2, pp. 99–111, 1991.

[74] Z. Erkin, A. Piva, S. Katzenbeisser, R. L. Lagendijk, J. Shokrollahi, G. Neven, and M. Barni, “Protection and retrieval of encrypted multimedia content,” *When cryptography meets signal processing, EURASIP Journal on Information Security,* 2007.

[75] T. Bianchi, A. Piva, and M. Barni, “Efficient point wise and block wise encrypted operations,” *In Proc. of ACM Multimedia & Security Workshop,* pp. 85–90, 2008.

[76] J.S Chou, Y. Chen, and C.J Chan, “Cryptanalysis of Hwang-Chang’s a time-stamp protocol for digital watermarking,” *Preprint,* 2007.

[77] M.S. Hwang, E.J.-L. Lu, I.-C. Lin, “Adding timestamps to the secure electronic auction protocol,” *Data and Knowledge Engineering,* vol. 40, no. 2, pp. 155–162, 2002.

[78] A. Kumar, S.P. Ghrera, and V. Tyagi, “A new and efficient buyer-seller digital watermarking protocol using Identity based technique for copyright protection,” *International Conference on Image Information Processing (ICIIP -2015) proceedings IEEE Computer Society Press in IEEE Explore, pp. 531-535,* pp. 21-24, 2015.

[79] J. Q. Xie, Q. Xie, L. J. Tian, “A Buyer-Seller Digital Watermarking Protocol without Third Party Authorization,” *Advanced Engineering Forum,* vol. 6, no. 7, pp. 452-458, 2012.

[80] S. A. Mostafa, A. S. Tolba, F. M. Abdelkader, and H. M. Elhindy, “Video watermarking scheme based on principal component analysis and wavelet transform,” *International Journal of Computer Science and Network Security,* vol. 9, no. 8, 2009.

[81] D. Kundur and Hatzinakos, “Digital Watermarking for Telltale Tamper Proofing and Authentication,” *Proceedings of the IEEE,* vol. 87, no. 7, pp. 1167-1180, 1999.

# LIST OF PUBLICATIONS

## 1.1 Journal Publications:

[1] A. Kumar, S.P. Ghrera, and V. Tyagi, "An ID-based Secure and Flexible Buyer-seller Watermarking Protocol for Copyright Protection," Science & Technology, Pertanika J. Sci. & Technol. Vol. 25, no. 1, pp. 57 – 76, January 2017. [Indexed in Scopus, ELSEVIER Emerging Sources Citation Index (ESCI)]
http://www.pertanika.upm.edu.my/Pertanika%20PAPERS/JST%20Vol.%2025%20(1)%20Jan.%202017/05%20JST%20Vol%2025%20(1)%20Jan%20%202017_0589-2015_pg57-76.pdf

[2] A. Kumar, S.P. Ghrera, and V. Tyagi, "Modified Buyer Seller Watermarking Protocol based on Discrete Wavelet Transform and Principal Component Analysis," Indian Journal of Science and Technology, Vol. 8, no. 35, pp. 1-9, 2015. [Scopus indexed].
http://dx.doi.org/10.17485/ijst/2015/v8i35/47258

[3] A. Kumar, S.P. Ghrera, and V. Tyagi, "Implementation of Wavelet Based Modified Buyer-Seller Watermarking Protocol," WSEAS Transactions on Signal Processing ,Vol. 10, pp. 212-220, April 2014. [Scopus indexed].
http://www.wseas.org/multimedia/journals/signal/2014/a025714-226.pdf

[4] A. Kumar, S.P. Ghrera, and V. Tyagi, "Survey of Buyer-Seller Watermarking Protocol," International Journal of Technology & Management, vol. 6, pp. 51-65, September 2013.

## 1.2 Conference Proceedings:

**[5]** A. Kumar, S.P. Ghrera, and V. Tyagi, "A Comparison of Buyer-Seller Watermarking Protocol (BSWP) Based On Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT)," Computer Society of India (CSI) Vol. 1. pp. 401-408, Springer, 2015. [Scopus indexed]. http://dx.doi.org/10.1007/978-3-319-13728-5_45

**[6]** A. Kumar, S.P. Ghrera, and V. Tyagi, "A new and efficient buyer-seller digital watermarking protocol using Identity based technique for copyright protection," International Conference on Image Information Processing (ICIIP -2015) proceedings, IEEE Explore, pp. 531-535, 21-24 Dec 2015. [Scopus indexed IEEE Explore]. https://www.computer.org/csdl/proceedings/iciip/2015/0148/00/07414830-abs.html

**[7]** A. Kumar, S.P. Ghrera, and V. Tyagi, "A lightweight buyer-seller watermarking protocol based on composite signal representation and time-stamping for multimedia data distribution." in International Conference on Engineering and Material Sciences (ICEMS-2016). [Indexed in Scopus, and published in SCIENCE DIRECT, Communicated].