STUDIES IN TECHNIQUES FOR IMAGE AND VIDEO SECURITY

By

TOSHANLAL MEENPAL

ENROLLMENT No. ENGG01201004002

BHABHA ATOMIC RESEARCH CENTRE MUMBAI

A thesis submitted to the
Board of Studies in Engineering Sciences

In partial fulfillment of requirements

for the Degree of

DOCTOR OF PHILOSOPHY

of

HOMI BHABHA NATIONAL INSTITUTE

18 September, 2015

HOMI BHABHA NATIONAL INSTITUTE

Recommendations of the Viva Voce Committee

As members of the Viva Voce Committee, we certify that we have read the dissertation prepared by Toshanlal Meenpal entitled "STUDIES IN TECHNIQUES FOR IMAGE AND VIDEO SECURITY" and recommend that it may be accepted as fulfilling the thesis requirement for the award of Degree of Doctor of Philosophy.

Chairman- Dr. Kallol Roy		Date: 18/09/15
Guide- Dr. A.K. Bhattacharjee		Date: 18/09/15
Co-guide- Dr. Subhamoy Maitra		Date:
Member 1- Dr. Archana Sharma		Date: 18-9-2015
Member 2- Dr. Gopika Vinod		Date: 18-9-2015
Member 3- Dr. V. H. Patankar		Date: 18/09/15
Internal Examiner- Dr. S. Mukhopadhyay		Date: 18/09/15
External Examiner- Prof. G. Sivakumar		Date: 18/9/15

Final approval and acceptance of this thesis is contingent upon the candidates submission of the final copies of the thesis to HBNI.

I/We hereby certify that I/we have read this thesis prepared under my/our direction and recommend that it may be accepted as fulfilling the thesis requirement.

Date:

Place:

Co-guide

Guide

PROFFESSOR
APPLIED STATISTICS UNIT
INDIAN STATISTICAL INSTITUTE
203, Barrackpore Trunk Road
Kolkata - 700 108

STATEMENT BY AUTHOR

This dissertation has been submitted in partial fulfillment of requirements for an advanced degree at Homi Bhabha National Institute (HBNI) and is deposited in the Library to be made available to borrowers under rules of the HBNI.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgement of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the Competent Authority of HBNI when in his or her judgment the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

Toshanlal Meenpal

DECLARATION

I, hereby declare that the investigation presented in the thesis has been carried out by me. The work is original and has not been submitted earlier as a whole or in part for a degree / diploma at this or any other Institution / University.

Toshanlal Meenpal

List of Publications arising from the thesis

Journal

1. T. Meenpal, S. Banik and S. Maitra, "A Scheme for Conditional Access based Systems using Index Locations of DCT Coefficients", *Springer Journal of Real-Time Image Processing*, 2014, (DOI) 10.1007/s11554-014-0409-y.

Communicated

1. T. Meenpal, T. K. Das and S. Banik, "An efficient compression compliant JPEG/MPEG encryption scheme", Paper communicated and under review in Springer Journal of Multimedia Tools and Applications (MTAP-S-15-01662).

Conferences

1. T. Meenpal and A. K. Bhattacharjee, "High Capacity Reversible Data Hiding using IWT", *International Symposium on Electronic System Design (ISED), 2011*, pp. 352 - 357, 2011.

2. T. Meenpal and A. K. Bhattacharjee, "Watermark Removal Attack extended to Forgery against Correlation-based Watermarking Schemes", Paper accepted in 11^{th} *International Conference on Information Systems Security (ICISS) 2015* (To be published in Springer Lecture Notes in Computer Science).

Toshanlal Meenpal

Dedicated to

MY BELOVED FAMILY MEMBERS, WIFE, MY DAUGHTER and GOD

Acknowledgments

I would like to express my sincere gratitude to my supervisors, Dr. A. K. Bhattacharjee and Prof. Subhamoy Maitra for their excellent guidance, encouragement and support in every stage of my research. Dr. A. K. Bhattacharjee's faith and support really motivated me to take up the challenge of new inter-disciplinary areas of research. I am greatly indebted to Dr. Maitra for academic as well as non academic support that I have received from him throughout my research period. His ability to instruct, guide, and inspire is truly remarkable and is only surpassed by his knowledge and passion for work.

I would also like to thank my doctoral scrutiny committee members Dr. Kallol Roy, Dr. Archana Sharma, and Dr. Gopika Vinod for many valuable suggestions. I also owe a debt of gratitude to Prof. Bimal Roy, Director of Indian Statistical Institute for allowing me to work at Center of Excellence in Cryptology, ISI Kolkata. I also thank all the lab members of COEC for their fruitful interactions and specially Subhadeep Banik and Sourav Sen Gupta for assisting me in the research.

I feel a deep sense of gratitude to my **parents**, brother and sisters for their tremendous support and motivation. I am very grateful to my beloved wife Ankita for her love and patience during my Ph.D period. Special Thanks to my little princess and my best friend, my daughter*Aarini*. Finally, I would like to give my soul respect to *GOD* for full support in my PhD work.

Place: HBNI, Mumbai
Date: 18 September, 2015.

Toshanlal Meenpal

Contents

Synopsis

The focus of this research work is to study, analyze and develop robust techniques for information hiding, image/video encryption techniques and to design an efficient conditional access based system.

First we develop an improved lossless data hiding scheme for digital images using Integer Wavelet Transform (IWT) and threshold embedding technique. Data are embedded into the least two significant bit-planes of high frequency Cohen-Daubechies-Feauveau (CDF) (2,2) integer wavelet coefficients, whose magnitudes are smaller than a certain predefined threshold. Histogram modification is applied as a preprocessing to prevent overflow/underflow. Experimental results show that this scheme performs better than prior techniques in terms of a higher payload and better image quality.

Next we show that a generic watermark removal attack on a correlation-based watermarking scheme can be extended in general to a forgery attack on the same. In certain cases, even if there exists a weak watermark removal strategy, it may be extended to a strong forgery attack. We prove our case by implementing our strategy against Modified Differential Energy Watermarking (MDEW) [1] which is considered to be one of the robust correlation-based watermarking schemes in the DCT domain.

Then we also develop a Conditional Access based System (CAS) for 'Image On Demand (IOD)' commercial applications, using index locations of

the DCT coefficients. Here we point out the significance of using the index locations of the DCT coefficients as a unique descriptor of any image and propose a novel scheme that can be efficiently adapted for any CAS. The DCT coefficients are sorted by magnitude generating two data sets (a) sorted DCT coefficients and (b) An array which contains their original index locations. We show that the distribution of values (DCT Index locations) in the generated array is significantly different for various images, and we exploit this to design an efficient CAS based scheme. Thus, the index locations play a significant role in representing an image whereas the actual values of the DCT coefficients have lesser effect. We propose a scheme in which we share a low quality version of an image with the customers. We keep secret an optimal number of index locations which are the most significant. These, we share to the customers only on demand, to construct the corresponding high quality image.

Finally we carry out a research work around JPEG and MPEG encryption. Through this research we propose a new format preserving selective encryption scheme for JPEG/MPEG which is compression friendly as well as highly secure. We choose quantized DCT coefficients of the I-frame for encryption. The resultant image/video is completely obscure and is suitable mainly for high end security applications.

List of Tables

List of Figures

List of Notations

Objects

I	Original image / object for watermarking
s	The mark to be introduced on the original image / object
$\tilde{I}$	Marked image / object
$\tilde{I}'$	Potentially (suspected to be) marked image / object
$I^{\$}$	Low quality image / object
$s^{(i)}$	User-specific mark to be introduced on the original image / object for the i^{th} user
$\tilde{I}^{(i)}$	Marked image / object for the i^{th} user
$\tilde{I}^{(i,\#)}$	Forged marked image / object for the i^{th} user
I_d	DCT transformed image for original image I
$\tilde{I}_d^{(i)}$	Modified DCT transformed image after marking for i^{th} user
V	Original video object
V'	Encoded video object
$Z_{10^{16}}$	Ring of integers modulo 10^{16}

Functions

E_A	Energy for lc-subregion A
X_A	Energy for a 8×8 DCT block A
$E(X)$	Expectation of a random variable X
$V(X)$	Variance of a random variable X
X^C	Estimate for the random variable X
$CORR(X, Y)$	Correlation between random variables X and Y
$H(X)$	Entropy of the distribution of random variable X
$Q(I, J)$	PSNR of image I with respect to image J
$\phi(I, J)$	MSE between two images I and J
$X \oplus Y$	Bitwise XOR between variables X and Y

List of Abbreviations

ANNTS	artificial neural network technology for steganography
BPCS	bit-plane complexity segmentation
bpp	bits per pixel
CAS	conditional access based system
CDF	Cohen-Daubechies-Feauveau
CKLS	Cox-Kilian-Leighton-Shamoon
dB	decibel
DE	difference expansion
DCT	discrete cosine transform
DEW	differential energy watermarking
DFT	discrete fourier transform
DRM	digital rights management
DWT	discrete wavelet transform
FPE	format-preserving encryption
g-LSB	generalised LSB
HEVC	high efficiency video coding

HVS	human vision sensitivity
iDFT	inverse discrete fourier transform
IOD	image on demand
IWT	integer wavelet transform
LBG	Linde-Buzo-Gray
LSB	least significance bit
LUT	look up table
MDCT	Modified DCT
MDEW	modified differential energy watermarking
MPEG	moving pictures experts group
MSE	mean square error
PDF	probability density function
PoV	pairs of value
PRNG	pseudorandom number generator
PSNR	peak signal to noise ratio
PVD	pixel value differencing
RDH	reversible data hiding
ROI	regions of interest
SDMCS	secure digital multimedia communication system
SRTP	secure real-time transport protocol
UEP	unequal error protection

Chapter 1

Introduction

There had always been security and digital right management issues since technology was introduced to help creation, distribution, and consumption of media between the "rights holders" (those who manage "rights to content"), intermediaries in the media value-chain, and end-users. There has been significant advancement in the field of digital signal processing, personal computers, and digital networks. In general these fall under the domain of digital technologies. The intermediaries and end-users utilize these techniques or their combination to do more with media than they could ever have imagined before. This new situation has intensified the difference that has always existed between these three classes of "users" in the media value-chain. Rights holders generally try to enforce the rights that have been granted to them by successive legislation. While, intermediaries and end-users always try to stick to rights and exceptions that were traditionally assigned to them, its applicability to the new digital space is often disputed by other affected parties. As a result we are witnessing, the continuous violation of right-holder's assets. This seriously affects their economic viability. On the other hand, the ongoing deployment of media distribution is based on Dig-

ital Rights Management (DRM) technologies. This substantially limits the default rights and usages normally available to media users [2].

These problems are globally accepted as very troublesome and critical for the future of our society. Some temporary solutions have been tried out but those solutions have limitations too. This scenario needs to be handled with great expertise which necessitates that certain essential and vital requirements to be defined clearly before the development and commercialization of the new digital multimedia technologies.

1.1 Basic Structure of Secure Digital Multimedia Communication System

In this section we describe the high-level structure of any Secure Digital Multimedia Communication System (SDMCS). Any SDMCS system compulsorily needs to contain following major features:

- The desired application goal is successfully achieved.
- Ensuring that the digital asset is packaged in a form that will prevent unauthorized copying/usage.
- Appropriately distributing the digital asset to the end-user.
- Making sure the end-user is able to render the digital asset consistently with his/her rights.

  In addition, SDMCS systems increasingly treat packaged content and the rights to access that content as separate entities. This adds a fourth feature that an SDMCS system needs to contain.

- Distribution of usage permissions allowing the user to access the pro-

tected content.

In this direction, we present the problem statement of this thesis by the help of figure (Figure 1.1) accompanied with further details. Figure 1.1 represents various target applications, corresponding to security techniques and the challenges involved in the design and practical realization of such SDMCS systems.

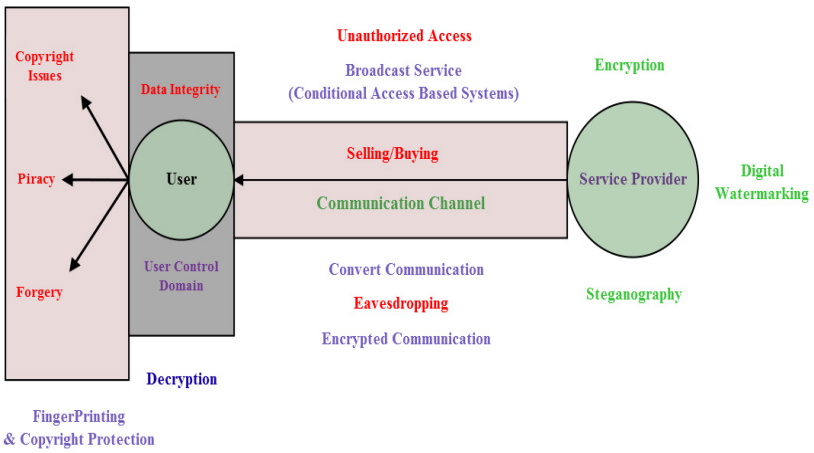


Figure 1.1: SDMCS Challenges and Solutions

Generally in any communication system there are two parties involved, and there is a communication channel in between. Accordingly in Figure 1.1 the two parties are Service Provider/(Party 1) and End-User/(Party 2). Various applications (shown in purple color in Figure 1.1) are our areas of study and the challenges/threats (mentioned in red color in the same figure) associated with the corresponding applications are listed below:

- Covert Communication – *Eavesdropping*
- Fingerprinting and Copyright Protection of Multimedia Data – *Forgery*
- Broadcast Service (CAS) – *Unauthorized Access*
- Encrypted Communication – *Eavesdropping*

Broadly speaking, all of the above listed applications require an establishment of SDMCS. We study and analyze each of these SDMCS based applications separately.

1.2 Major Contributions

The main contribution of this thesis is to study the underlying technologies (for example, Digital Watermarking, Steganography and Encryption) that are deployed to design various SDMCS based applications. We investigate the extent to which the proposed technology had been successful in providing a fool-proof solution for the respective SDMCS. We also propose better/improved system or scheme as a solution to the corresponding identified problem. The underlying goals of this study are broadly:

- To study the existing techniques which have been deployed to design such SDMCS systems.
- To investigate the extent to which the existing relevant techniques have been able to resolve the identified challenges and threats.
- To propose and design new/improved schemes for the above mentioned SDMCS based applications.

Brief description of each of the SDMCS based applications have been given in next four subsections (i.e. 1.2.1, 1.2.2, 1.2.3 and 1.2.4). We also present our contribution towards the underlying technology for each of the individual application scenario in the subsequent subsections.

1.2.1 Covert Communication

In covert communication systems, the goal is to conceal the very fact that some form of communication is being attempted between the two parties. Steganographic techniques are used to design such type of SDMCS and pre-existing channels are utilized. Communication of the covert message does not demand a channel of its own. The cover signal is used as the transmission medium. In our case the cover signal is digital image.

The main challenge faced by modern intelligence agencies in this case is, to attempt to discern if some covert data is being communicated by two parties under suspicion.The problem lies in trying to determine if an uncontroversial transmission, in fact, contains a more conspiratorial message. The extraction of the hidden data from the cover media by an adversary is the secondary goal, and not within the scope of current research.

Problem Definition

The aims of improving this type of SDMCS are two-fold:

- The first aim is to make the embedding capacity as high as possible.
- The second aim is to reduce the visible distortion as low as possible.

However, there is a trade-off between distortion and embedding capacity. If distortion is minimized, then only a small amount of data can be embedded. On the other hand, if the embedding capacity is increased, distortion also increases. So the scope of improving the balance between both of them always exists. Here we consider the question "How much data can be imperceptibly embedded into an image, assuming that the sender and receiver have access to a shared image and that there is no modification in the communicated data during its transmission?"

Contribution

We analyze the problem and propose a Reversible Data Hiding (RDH) algorithm that leads to the enhancement of the data hiding capacity by introducing a novel histogram shifting equation and an embedding mechanism. This modification can greatly improve the embedding capacity with graceful degradation of image quality. The proposed scheme also has the advantage of selecting a smaller difference coefficient as a threshold value to attain a particular payload requirement. Results are provided demonstrating that the scheme outperforms the prior techniques in terms of PSNR and payload.

Details of our analysis and simulations are presented in chapter 3 that had been published in [3].

1.2.2 Fingerprinting and Copyright Protection

Digital Watermarking is the underlying technology which is used to ensure copyright protection and fingerprinting of the multimedia data. Digital Watermarking refers to embedding an imperceptible secret signal (watermark) in the original (cover) data. The embedded watermark needs to be transparent (not detectable by human eyes). The embedded watermark(s), can be used for various purposes, each of which is associated with different robustness, security, and embedding capacity requirements [4]. This implies that the watermark should be robust to most common attacks such as cropping, noise addition, compression, enhancement, filtering etc. Some of the major applications of digital watermarking are as follows.

Copyright Protection: For the protection of intellectual property, the data owner can embed a watermark representing copyright information in his/her data. This watermark can prove his/her ownership in court when someone has infringed on his/her copyrights.

Copy Control and Access Control: The information stored in a watermark can directly control digital recording devices for copy protection purposes [5]. In this case, the watermark represents a copy-prohibit bit and watermark detectors in the recorder determines whether the data offered to the recorder may be stored or not.

Fingerprinting: Some applications require the ability to identify the legal recipient rather than the owner. It is effective where a buyer specific watermark is embedded to identify the source of illegal copies. It is similar to the serial numbers of softwares. This type of application requires that the watermarking scheme should have a very small false positive rate, so that the chance of wrongly implicating an honest buyer is negligible.

Authentication: It is becoming increasingly difficult to identify the malicious changes made to the digital images. Also some of these changes can have serious consequences. Malicious change made to medical images can have a disastrous effect. Thus there is a need for content authentication. This problem can be solved using "fragile watermarks". Fragile watermark(s) may be robust to simple processing. However, any malicious processing would destroy the watermark(s), which may lead to the failure of authentication.

The major challenges or threats tackled by the help of digital watermarking are

Piracy: Making of duplicate copies illegally.
Forgery: Creating an almost valid copy of the multimedia data without owner's permission.
Copyright Issues: Scenario where some one else other than the actual owner tries to claim his/her ownership on the original data.

Problem Definition

Most of the digital watermarking schemes are correlation-based, i.e., the

correlation between recovered and embedded signal acts as the confidence measure in the detection/verification process. It is already known that existing correlation-based watermarking techniques are susceptible to collusion attacks under a generalized framework [6]. But for the attack to be successful, huge number of watermarked copies are required, which may not be practical.

The watermarking strategies should survive some standard image transformations. These are cropping, rotation, resizing, JPEG compression [7], wavelet compression [8], etc. Note that most of the current schemes can easily survive these transformations. Generally the robust watermarking schemes survive most of the attacks related to insertion of random noise in the image, some filtering attacks [9], or nonlinear geometric attacks such as Stirmark [10, 11]. However, there is a need to analyze each of the popular schemes individually to check whether customized attacks can be mounted on them to highlight their weakness. This should be done before deploying any watermarking based copyright protection system, otherwise pirates may find it easy to break the scheme, causing considerable financial loss to the media owner.

We analyze the robustness of the most prevalent correlation-based watermarking scheme by mounting a customized attack model for the same. For correlation-based watermarking schemes, some single-copy attacks are already studied in the literature [12, 1, 13]. It still remains an open question whether there exists a general strategy to cryptanalyse correlation-based watermarking schemes, and mount single-copy forgery attacks on them.

Contribution

We consider this in our current work. We choose Modified Differential Energy Watermarking (MDEW) [1] as our target as it has a conscious design principle that tries to avoid straight-forward but customized single-copy

forgery attacks, as claimed in [1] by the designers of MDEW. However, the conscious design of MDEW [1] scheme, towards having better security, is shown to be vulnerable against our general watermark removal extended to-forgery attack.

Details of our analysis and simulations are presented in chapter 4.

1.2.3 Conditional Access Based Systems

Most of the existing Conditional Access Based Systems (CAS) follow a standard methodology. The service provider shares two copies for single information (specifically image for this work). One copy is a low-resolution version which is shared in the public domain for preview purpose. The other one is a high-resolution version, which is to be provided to the customers through a secure channel on demand (after payment). One major CAS is 'Image On Demand (IOD)', where a user browses a database of multimedia files to retrieve the content of interest. In a typical IOD scenario, a low-resolution image can be quickly downloaded from image database to select the desired content, which can be purchased in a higher resolution version later.

Problem Definition

One drawback of the existing IOD schemes is that the amount of storage is quite high. The reason behind this is that the protocol is to keep at least two copies of a particular image: one for preview purpose and the other is the high-resolution version. High-resolution version is sent separately through secure channel when customer pays for the same. Another drawback is that, the huge amount of data in the form of high-resolution image needs to be sent through the secure channel. It increases the computational and communication overhead at real-time. We try to resolve the drawbacks mentioned above in this research.

One major technique being used to realize CAS is selective encryption. Suitable portion and size of the actual data (image in this case) is scrambled in the process of selective encryption. It is performed in such a way that the image rendered from the rest of the 'in-the-clear portion' (i.e., the segment of the data which is not scrambled) is imperceptible to a significant fraction of the consumers [14].

Contribution

We propose a new scheme that can be efficiently adapted in such a scenario. We analyze the image in the Discrete Cosine Transform (DCT) domain. Polynomials of suitable degree representing the sorted DCT coefficients together with original index locations, can uniquely represent an image. We show that the arrangement of DCT index locations, after the actual coefficients have been sorted by magnitude, is significantly different for various images and we exploit this to design an efficient CAS. The amount of private data, which a service provider needs to transmit through a secure channel to the customers on demand, is reduced significantly by our technique. This reduction in transmitted data makes the system apt for real-time secure applications.

Details of our analysis and simulations are presented in chapter 5 that had been published in [15]

1.2.4 Encrypted Communication

Various organizations are now able to perform real-time audio-conferencing and video-conferencing, even over a non-dedicated channel. However, many multimedia distribution networks are open public channels and, as such, are highly insecure. Any eavesdropper can conveniently intercept and capture the sensitive and valuable multimedia content traveling in a public channel.

In the area of military application, secure multimedia transmission is very crucial to avoid its access from the enemies. Multimedia encryption [16, 17, 18] protects the confidentiality of media as well as the information which is contained inside by converting the media into unintelligible data-stream. Image/video encryption [19] converts the image/video in such a manner that it can not be understood.

Problem Definition

Generally for secure and secret communication in defense, we require that the encrypted image/video should be completely obscure. To achieve this, the existing schemes use naive encryption approach and a dedicated channel is required for secure transmission. While if we use existing selective encryption method for the same, then the resultant data is still viewable although unpleasant. There may be many scenarios where without compromising much on security constraints (similar to naive approach) we may have to transmit image/video through an open public network. An efficient selective encryption scheme which can completely obscure the image/video without degrading the performance of the compression block present in the general multimedia pipeline is required for this case.

Contribution

We present a format preserving selective encryption scheme applied on JPEG/MPEG such that the resultant image/video is completely obscure as well as it retains the original compression factor, which possibly may allow the data to be transmitted successfully within the available channel capacity of the public network. The proposed system ensures content confidentiality during real-time multimedia distribution, archiving, and other delegate processing.

Details of our analysis and simulations are presented in chapter 6.

1.3 Organization of the Thesis

A brief overview of the work carried out in the thesis and organization of the same are summarized below.

Chapter 1 presents the problem definition, motivation and brief contribution of the thesis. A brief introduction to the essential requirements of any SDMCS is discussed. Following which some of the major SDMCS based applications and the challenges/threats associated with the corresponding applications have been explained. Brief introduction to the existing underlying technologies that are used to design SDMCS have been presented. Various research aspects that are identified and our contribution to the corresponding underlying technology is illustrated next.

Chapter 2 gives a brief survey of the existing works related to each of the underlying technology (steganography, attacks on digital watermarking techniques and selective encryption) which are generally deployed to design such SDMCS.

Then we have four contributory chapters (Chapter 3, Chapter 4, Chapter 5 and Chapter 6).

Chapter 3 proposes an improved lossless data hiding scheme for digital images using integer wavelet transform and threshold embedding technique. Data are embedded into the least two significant bit-plane of high frequency CDF (2,2) integer wavelet coefficients whose magnitudes are smaller than a certain predefined threshold. Histogram modification is applied as a preprocessing to prevent overflow/underflow. Experimental results show that this scheme performs better than prior techniques in terms of a higher payload and better image quality.

In Chapter 4 we show that a generic watermark removal attack on a correlation-based watermarking scheme can be extended in general to a

forgery attack on the same. In certain cases, even if there exists a weak watermark removal strategy, it may be extended to a strong forgery attack. We prove our case by implementing our strategy against MDEW [1] which is considered to be one of the robust correlation-based watermarking schemes in the DCT domain.

Chapter 5 presents a conditional access based systems for image on demand commercial application, using index locations of the DCT coefficients. Here we point out the significance of using the index locations of the DCT coefficients as a unique descriptor of any image and propose a novel scheme that can be efficiently adapted for any CAS. We propose a scheme in which we share a low quality version of an image with the customers in the form of polynomials that approximate the sorted DCT coefficients and major portion of index locations. We keep secret an optimal number of index locations which are the most significant. These are shared to the customers only on demand, to construct the corresponding high quality image.

In Chapter 6 we propose a new format preserving selective encryption scheme for JPEG/MPEG which is compression friendly as well as highly secure. We choose quantized DCT coefficients of the I-frame for encryption. The resultant image/video is completely obscure, and is suitable mainly for high end security applications. In addition to this, there is no reduction in the performance of compression algorithms applied later in the standard JPEG/MPEG pipeline.

Finally in the conclusion (Chapter 7), we summarize the work carried out in this thesis. The results are discussed in brief. The advantages and disadvantages of all the proposed methods are also highlighted. We conclude the thesis by suggesting scope for future work.

Chapter 2

Background and Related Works

In this chapter, we present a brief survey of the works relevant to underlying techniques behind SDMCS. We have already explained a few basic issues in the previous chapter. To recapitulate, the techniques are:

- *Steganography*: for Covert Communication systems,
- *Digital Watermarking*: for Fingerprinting and Copyright Protection,
- *Selective Encryption*: for CAS and Secure Encrypted Communication.

These techniques are the backbone of most of the existing SDMCSs.

In the next section we concentrate on steganographic techniques that may be used for covert communication.

2.1 Steganography

The word 'Steganography' is related to hidden communication that literally means "covered writing". The message is out in the open, often for all to

see, but goes undetected because the very existence of the message is secret. Another popular description for steganography is "hidden in plain sight". The basic underlying assumption here is that, if the feature is visible, the point of attack is evident. Thus, the goal here is always to conceal the very existence of the secret communication. Various useful applications of steganography may be found in [20].

The ultimate objectives of steganography, which are undetectability as well as capacity of the hidden data, are the main factors that differentiate it from related techniques such as watermarking and cryptography.

2.1.1 Terminology

Intuitively, this work makes use of some terms commonly used by steganography and watermarking communities.

- *Cover image/Original image:* Used alternatively to describe the image designated to carry the embedded bits.
- *Stego/Watermarked image:* The resultant image after the process of embedding/hiding.
- *Steganalysis/Attacks:* Different kinds of image processing and statistical analysis, that aim to break or attack the steganographic/watermarking schemes.
- *Cryptanalysis:* Cryptologic approach to attack the existing cryptographic algorithm.
- *Payload:* Amount of data which could be embedded or hidden in the cover image. Generally measured in bits per pixel (bpp).
- *Peak Signal to Noise Ratio (PSNR):* A degree of measurement which tells the similarity between two images. It is measured in decibel (dB).

2.1.2 Overview of a Steganographic Process

Figure 2.1 shows a simple representation of the generic embedding and extraction process in steganography. In this example, a secret image is being embedded inside a cover image to produce the stego image.

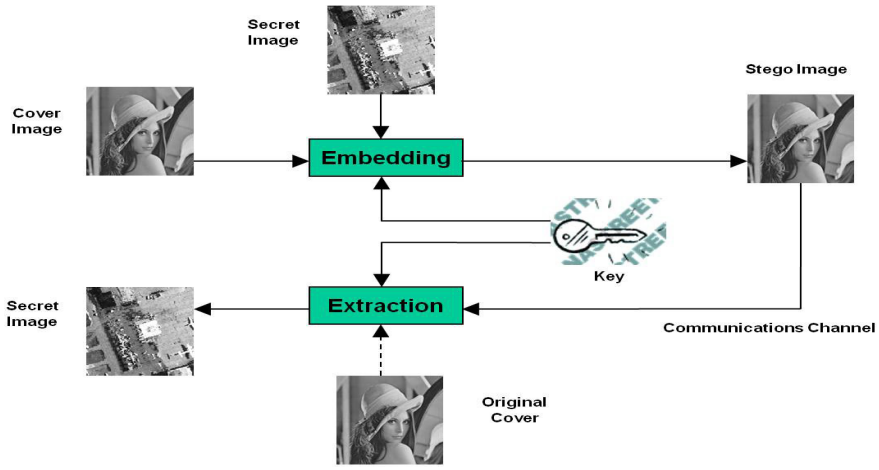


Figure 2.1: Generic Steganography Process of Embedding and Extraction

The first step in embedding and hiding information is to pass both the secret message and the cover message into the embedding stage. In embedding stage, one or several protocols may be implemented to embed the secret information into the cover message. The type of protocol to be applied will depend on: (a) type of information to embed and (b) The cover medium. For example, one will use an image protocol to embed information inside images.

A key is often needed in the embedding process. This can be in the form of a public or private key so that one can encode the secret message with the recipient's public key and the recipient can decode it using his/her private key. In embedding the information this way, one can reduce the chance of a third party attacker getting hold of the stego object and decoding it to find out the secret information.

In general, the embedding process inserts a mark, s, in an object, I. A

key, K, usually produced by a pseudo random number generator is used in the embedding process and the resultant marked object, $\tilde{I}$, is generated by the mapping: $I \times K \times s \rightarrow \tilde{I}$.

Having passed through the embedding stage, a stego object will be produced. A stego object is the original cover object with the secret information embedded inside. Cover image and stego image should be identical in all respect. If both images are identical visually but differ in other aspects or normal image statistics get disturbed during embedding; it is very easy to identify the stego image.

Having produced the stego object, it will then be sent off via some communication channel, such as email, to the intended recipient for decoding/extraction. The recipient must decode the stego object in order for them to view the secret information. The extraction process is simply the reverse of the embedding process. It is the extraction of secret data from a stego object.

In the extraction process, the stego object is fed in to the system. The public or private key that can decode the original key which is used inside the embedding process is also needed so that the secret information can be extracted. Depending on the embedding technique, sometimes the original cover object is also needed in the extraction process.

2.1.3 Image Steganography

Image steganography can be divided into following domains.

Spatial Domain Methods:

There are several schemes of spatial steganography. Most of such schemes, either directly or indirectly, change some bits in the image pixel values for hiding data. Least significance bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values by introducing imperceptible distortions. The major drawback of these technique is the amount of additive noise that creeps in the cover image, having direct impact on the PSNR and the statistical properties of the image. These embedding techniques often can be easily destroyed by compression, filtering or a less than perfect format or size conversion.

Noise of 0.5 bpp on an average is added by this kind of embedding strategy. This kind of embedding also leads to an asymmetry and a grouping in the pixel gray values (0,1);(2,3);. . . (254,255). Many steganalysis techniques use "pairs of value" (PoV) that exist in LSB-based steganography for detection and extraction of hidden message [21]. To defeat this attack, the decision of changing the least significant bit is randomized, i.e., if the message bit does not match the pixel bit, then pixel bit is either increased or decreased by 1. This technique is popularly known as LSB Matching [22, 23, 24].

This kind of embedding also adds a noise of 0.5 bpp on an average. Mielikainen et al. in [24] have suggested the use of a binary function of two cover pixels to embed the data bits to further reduce the noise. A pair of pixel is used for embedding, where the LSB of the first pixel carries one bit of information, and a function of the two pixel values carries another bit of information. This method reduces the embedding noise introduced in the cover image.

A similar kind of scheme by the name of Pixel Value Differencing (PVD) based on Human Vision Sensitivity (HVS) has been proposed in [25]. More amount of data bits are added in the high variance regions of the image,

for example, near "the edges" by calculating the difference values of two neighboring pixels.

Crandall et al. in [26] have introduced the use of an Error Control Coding technique called "Matrix Encoding". In Matrix Encoding, q message bits are embedded in a group of $2^q - 1$ cover pixels while adding a noise of $1 - 2^q$ per group on average. The maximum embedding capacity that can be achieved through this technique is $\frac{q}{2^q-1}$.

LSB-based steganography can be easily extended to hide data in multiple bit-planes. In this kind of approach precaution has to be taken that embedding should be done in low bit-planes, and in case high bit-planes are involved, then local property should be checked so as to improve the perceptual quality of the stego image [27]. A set of binary images according to the Bit-Plane Complexity Segmentation (BPCS) is achieved by decomposing the image. It leads to dividing the bit-plane into consecutive and non-overlapping blocks. Noise-like blocks are identified by checking each of the block for embedding data in it. Higher embedding rate of as high as 4 bpp can be achieved without causing much severe visual artifacts through this kind of technique.

In the next subsection we cover some of the transform domain steganographic algorithms.

Transform Domain Methods:

We have seen that LSB modification techniques are easy ways to embed information, but they are highly vulnerable to even small cover modifications. An attacker can simply apply signal processing techniques in order to destroy the secret information entirely. In many cases even the small changes resulting out of lossy compression systems yields to total information loss.

It has been noted early in the development of steganographic systems that embedding information in the frequency domain of a signal can be much more robust than embedding rules operating in the time domain. Most robust steganographic systems known today actually operate in some sort of transform domain. Transform domain methods hide messages in significant areas of the cover image which makes them more robust to attacks, such as compression, cropping, and some image processing, than the LSB approach. However, while they are more robust to various kinds of signal processing, they remain imperceptible to the human sensory system. Many transform domain variations exist. One method is to use the DCT [28, 29] as a vehicle to embed information in images; another would be the use of wavelet transforms [30]. Transformations can be applied over the entire image [28], to blocks throughout the image [31, 32], or with other variations. However, a trade-off exists between the amount of information added to the image and the robustness obtained [33, 34]. Many transform domain methods are independent to image format and may survive conversion between lossless and lossy formats.

The JSteg algorithm was among the first algorithms to use JPEG images. Although the algorithm stood strongly against visual attacks, it was found that examining the statistical distribution of the DCT coefficients, one can find the existence of hidden data [35]. JSteg is easily detected using the X^2-test. Moreover, since the DCT coefficients need to be treated with sensitive care and intelligence, the JSteg algorithm leaves a significant statistical signature. Wayner [36] stated that the coefficients in JPEG compression normally fall along a bell curve and the hidden information embedded by JSteg distorts this. Manikopoulos et al. [37] discussed an algorithm that utilises the probability density function (PDF) to generate discriminating features that are fed into a neural network system which detects hidden data in this domain.

Few of the Discrete Wavelet Transform (DWT) based steganographic schemes can be found in [38, 39, 40]. Abdulaziz and Pang [41] used vector quantization called Linde-Buzo-Gray (LBG) coupled with BCH code and 1-stage discrete Haar wavelet transforms. They reaffirm that modifying data using a wavelet transformation preserves good quality with little perceptual artifacts. Paulson [42] reports that a group of scientists at Iowa State University are focusing on the development of an innovative application which they call "Artificial Neural Network Technology for Steganography (ANNTS)" aimed at detecting all present steganographic techniques including DCT, DWT and Discrete Fourier Transform (DFT). The inverse DFT (iDFT) encompasses round-off error which renders DFT improper for steganography applications.

In addition to these categories, steganography techniques can also be classified into

- Lossy or Lossless/Reversible.
- Adaptive Embedding in coefficient bits (Difference Expansion, Histogram Modification).

Among the various approaches mentioned above, reversible data hiding techniques have got more attention in recent years because of its lossless nature. Many sensitive applications in the field of military, medical and law enforcement domain require that secret data could be embedded in the cover image and could be extracted completely together with exact recovery of the cover image as well.

In the next section we present a survey of the prior works in the field of reversible data hiding.

2.1.4 Reversible Data Hiding

Reversible data hiding is also known as lossless data hiding. It allows full extraction of the embedded information along with the complete restoration of the cover work. RDH can thus be considered as a special case of data hiding/steganography. Figure 2.2 shows the block diagram of a basic RDH system. The existing RDH schemes are mostly fragile in nature. The two important properties of RDH are imperceptibility and embedding capacity. Roughly speaking, imperceptibility is the measure of similarity between embedded and the cover image. While, embedding capacity is the measure of the maximum number of information bits that can be embedded in the cover image. The performance of a RDH technique is thus evaluated on the basis of these measures.

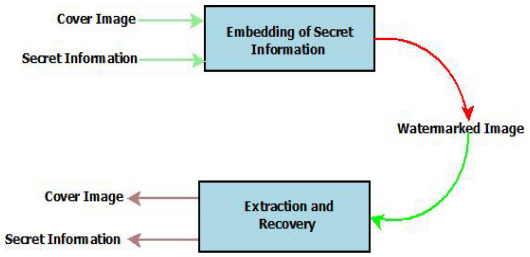


Figure 2.2: Standard Reversible Data Hiding Scheme

Prior Works and Research Aspects

Since Barton [43] proposed the first RDH technique, many lossless data embedding schemes have been developed. Old reversible schemes comprises of techniques such as the modulo-arithmetic additive-based technique [44]; circular interpretation of bijective transformations [45, 46]; compression-based techniques [47, 48]; the generalised LSB (g-LSB) embedding algorithm [49]; and the multiple embedding strategy [50]. All of these schemes, except the last, have low embedding capacity.

Recent reversible schemes are mainly based on two techniques, Difference Expansion (DE) and Histogram Shifting. The DE-based schemes have very high embedding capacities, whereas the histogram shifting schemes have low embedding capacities but can show some good robustness.

The DE method, which was introduced by Tian [51], is a seminal work in this area. DE is based on modifying the difference between a pair of pixel values while keeping their average unchanged. The technique divides the cover image into pair of pixels and then embeds one bit of information into each pair. The technique has received attention because of its high efficiency and simplicity. Since Tian [51] introduced the DE technique, the influence of his work can be easily found in many later works. The extensions of his method by other researchers have yielded many good and more sophisticated algorithms.

The aims of improving the original DE method are two-fold:

1. The first aim is to make the embedding capacity as high as possible.
2. And the second aim is to make the visible distortion as low as possible.

To achieve high embedding capacity, the previously mentioned schemes have adopted three approaches:

1. Simplifying the location map to increase its compressibility.
2. Embedding the payload without a location map.
3. Expanding differences more than once to allow more data to be embedded or using multi-layer embedding.

Meanwhile, the visual quality may be enhanced by the following:

1. Using a predefined threshold T.
2. Selecting smooth areas to embed data.

3. Using sophisticated classification functions

However, there is a trade-off between distortion and embedding capacity. If distortion is minimized, then only a small amount of data can be embedded. On the other hand, if the embedding capacity is increased, visible distortion also increases. Although the previously mentioned schemes can relatively balance the two aims, most of the schemes have a high computational cost, and all of them are time consuming because they scan the host image several times during the embedding process.

2.2 Digital Watermarking

Techniques of embedding a secret imperceptible signal or data called watermark, directly into the transformed image in such a way that it always remains present, is called watermarking. The watermark first made its appearance in handmade paper over 700 years ago. After the invention of the watermark, its use quickly spread through Italy and then all through Europe. It was primarily used to distinguish one paper manufacturer from another.

Watermarking is related to steganography, but is used in a different context and in a different mindset. Both watermarking and steganography are used to hide information or move information in a cover medium, but after this they begin to differ.

Steganography:

- Is not robust or has limited robustness.
- Tries to hide the fact that there is hidden information.

Watermarking:

- Is designed to be robust.

- While not always visible, is designed to carry hidden information.

In our work we mainly focus on the robustness aspect of the existing watermarking techniques, since it is vital enough to analyze the claimed robustness of the watermarking techniques before actually launching them in the commercial domain. Watermarking techniques can be classified into following categories on the basis of their robustness:

- **Fragile:** The fragile watermark is one of the watermarking methods for authentication that has a low robustness toward modifications. Even small changes of the content will destroy embedded information, showing that there has been an attempt of attack. A good example is medical records.
- **Robust:** A robust watermark is almost exactly the opposite of a fragile watermark. A robust watermark can be either visible or invisible, depending on purpose. Robust watermarks are very difficult to remove or damage.

2.2.1 Requirements of a Robust Digital Watermark

Any digital watermarking technique should meet most of the following criterias:

- *Unobtrusive*: Should be invisible or if it is visible, should not interfere with what is being protected.
- *Robust*: The watermark must be difficult, or impossible, to remove.
- *Low False Positive*: It must have a small probability of false detection.
- *Common signal processing*: The watermark should be retrievable if some signal processing (for example. digital-to-analog, analog-to-digital, resampling, and other signal enhancements) is applied.

- *Common geometric distortions*: Watermarks used in images and video should not be affected by scaling, rotation, cropping, or format translation.
- *Collusion attacks*: The watermark should be robust against the technique of combining several copies of the same data set for the purpose of destroying the watermark.
- It should be difficult to create or extract watermark without proper credentials.

In general, most of the above requirements are met by a specific watermarking algorithm. Still there is a need to analyze each of the popular schemes individually and to check whether customized attacks can be mounted to highlight the weakness of the individual scheme itself. This is also similar to the concept of cryptanalysis of the cryptographic schemes.

We mainly target on the following aspects to analyze the robustness of any watermarking scheme.

1. How well the malicious buyer is identified (who has intentionally attacked the watermarked image).
2. How infrequently an honest buyer is wrongly implicated.

Correlation-based watermarking is one of the popular techniques and exists in abundance in the relevant literature [12, 1, 13]. In the next section, we present some of the works related to collusion and other normal benchmark attacks as well as customized single-copy attacks in line of cryptanalysis.

Prior Works and Research Aspects

The watermarking strategies should survive some standard image transformations. These are cropping, rotation, resizing, JPEG compression [7],

wavelet compression [8], etc. Generally most of the robust schemes can easily survive these transformations. The existing methods can also survive the attacks related to insertion of random noise in the image, some filtering attacks [9], or nonlinear geometric attacks such as Stirmark [10, 11]. It is clear that once an attack, based on some image processing technique, is proposed, it is expected that there will be some inverse image processing methodology to resist such kinds of attack. Thus, single-copy attacks, based on image processing techniques, should not survive in the long run.

It is also known that existing correlation-based watermarking techniques are susceptible to collusion attacks under a generalized framework [6]. This requires a sufficient number of watermarked copies. In particular, if the effective document length is n, then $O(\sqrt{\frac{n}{\ln n}})$ copies are required to defeat the watermarking scheme. Note that for an image of size 256×256 or 512×512, for a successful collusion attack, a large number of watermarked images may be required, depending on the size of the key information. This may not be practical. On the other hand, we here concentrate on cryptanalytic attack based on a single watermarked copy.

The existing watermarking models need to be analyzed using cryptanalytic techniques as is done for standard cryptographic schemes. In chapter 4, we look into the watermarking scheme as a cryptographic model and provide an attack that can be considered to be a cipher text only jamming attack, since the proposed attack removes/invalidates the secret watermark using a watermarked copy only. For different kinds of cryptanalytic attacks; see [52]. Brief survey of single-copy attacks is also given in [12].

2.3 Encryption

Encryption is a method or a process for protecting information from undesirable attacks by converting it into a form non recognizable by the attackers. Data encryption is mainly the scrambling of the data, such as text, image, audio, video and so forth to make the data unreadable, invisible or incomprehensible during transmission. The goal is to protect the content of the data against the attackers. The reverse of encryption is decryption, which recovers the original data. Figure 2.3 is the general model of a typical encryption/decryption system.

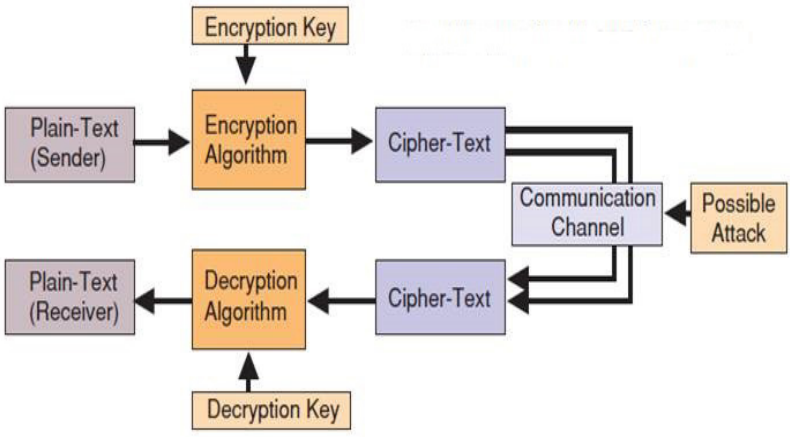


Figure 2.3: Encryption/Decryption System

Prior Works and Research Aspects

Depending on the type of plaintext, data encryption systems are classified as text encryption, audio encryption, image encryption and video encryption. In order to have a generic cryptosystem that can encrypt digital data, such as text/image/audio/video, some encryption standards have been developed. Among them, DES [53], RSA [54], AES [55] and IDEA [56] etc. are elaborately designed and widely adopted.

2.3.1 Multimedia Encryption

Multimedia encryption [16, 17, 18] converts the media into unintelligible ciphers and thus protects the confidentiality of media as well as the information contained inside. The word 'Multimedia' collectively refers to image/video in this thesis.

There are two levels of security for multimedia encryption:

- *Low-level security encryption:* The encrypted multimedia data has degraded visual quality compared to that of the original one, but the content of the image is still visible and understandable to the viewers.
- *High-level security encryption:* The content is completely scrambled and the multimedia data looks like random noise. In this case, the multimedia data is not understandable to the viewers at all.

By carefully designing the encryption technology, it is possible to provide advanced functionalities. For example by a low-level security encryption approach, a CAS can be efficiently designed. Conditional access amounts to providing different portions of a multimedia content under different policies; a thumbnail or a low-resolution version of the content can be made available for free, whereas the user may have to pay in order to see the high quality content.

If the multimedia data is considered just as a data bit-stream, there is no fundamental difference between multimedia encryption and other types of data encryption. Generally these kinds of encryption approaches target high-level security. We may simply input the multimedia data bit-stream into the standard encryption system. Secure video-conferencing in the area of defense is the best suited application for such high-level security encryption approaches.

For multimedia encryption, the following properties listed below are al-

ways desired:

- The encryption/decryption algorithm has to be very fast in order to meet the performance requirements of real-time applications.
- The encryption algorithms should be robust against the general multimedia processing procedures.
- The encryption/decryption procedure should not degrade the quality of the original media.

Considering the typical size of a multimedia data compared to that of a text message, it is important to meet the speed requirements for real-time multimedia processing/transmission applications. Some of the encryption techniques proposed recently include Fourier-based methods [57], SCAN-based methods [58, 59], chaos based methods [60] and quadtree-based methods [61].

Due to the variety of constraints mentioned above (such as near-real-time speed, etc.), communication security for streaming multimedia is harder to accomplish. To meet the above constraints for encrypted multimedia communication, it involves careful analysis to determine and identify the optimal encryption method. Current research is focused on modifying and optimizing the existing cryptosystems for real-time multimedia applications. It is also oriented towards exploiting the format-specific properties of many standard multimedia formats in order to achieve the desired speed and enable real-time streaming. This is referred to as selective encryption and is described next.

2.3.2 Selective Encryption

Selective encryption is a technique to save computational complexity or enable new system functionality by only encrypting a portion of a bit-stream while achieving adequate security. Although suggested in a number of specific cases, selective encryption could be much more widely used in consumer electronic applications ranging from mobile multimedia terminals through digital cameras were it subjected to a more thorough security analysis. We target Selective encryption for two types of applications;

- To design a conditional access based system for digital image.
- To achieve almost high-level encryption security for image/video for possible applications in the field of defense like secure video-conferencing.

The Moving Pictures Experts Group (MPEG) has produced a number of standards related to multimedia representation, compression, and processing [62]. In particular, the MPEG-1 and MPEG-2 video standards are widely used for compression of video (often in entertainment and information applications). Spanos and Maples [63] were the first proponents of a selective encryption style algorithm; they applied selective encryption to MPEG I-frames. But, since I-frames are non-predicted, they require a large number of bits per frames as compared to P and B-frames. So, this approach means that typically more than half of the bit-stream needs to be encrypted. Agi and Gong [64] criticized the Spanos and Maples approach upon observing a decoder operating on the selectively encrypted material and recommended encrypting I-blocks (non-predicted blocks) in P and B-frames in addition to I-frames. Alattar and Al-Regib came to a similar conclusion and recommendation in [65]. Kunlemann and Rienema [66] suggested for the encryption of high order DCT coefficients, while Shi and Bhargava [67] and Shin et al. [68] evaluate encrypting only the sign bits of the DCT coefficients. Griwodz et al. [69] took the approach of random selective corruption to address a caching

application. They found that corrupting 1% or less of the stream was sufficient to render the content sufficiently unsatisfactory for video-on-demand. It is worth noting the marked difference between this conclusion and earlier conclusions that encrypting substantially all I-frames and I-blocks are necessary for security. Obviously the definition of how much damage needs to be done to avoid the unauthorized users reproduction is critical to conclusions on whether adequate security has been provided.

Cheng and Li [70] apply selective encryption to quad-tree and wavelet based image compression algorithms. Pommer and Uhl [71] also use wavelet based compression in a selective encryption scheme. Roche et al. [72], on the other hand, use fractal image compression as the basis for their algorithm but propose that a reduced quality but not entirely useless image will be available (for inspection and to prompt interest).

It is clear that several researchers have seen the potential for the selective encryption idea in specific consumer electronic applications and have developed proposals for its application. We propose a new CAS based model for image on demand by using a novel selective encryption approach in chapter 5. It has been widely established that if selective encryption approach is used, then one has to compromise with the security and the encrypted results are perceptual to get the feel of the original data (although may not be commercially usable). In chapter 6 we re-analyze this fact and develop a system which generates completely obscure results by using selective encryption approach.

In the next chapter we analyze some of the existing reversible steganography techniques generally used for covert communication. We also propose an improved scheme for the same with higher embedding capacity with relatively less degradation of the cover image.

Chapter 3

Reversible Data Hiding on Gray Level Images

The art of secretly hiding and communicating information has gained immense importance in the last two decades due to the advances in generation, storage, and communication technology of digital content. Watermarking is one of the promising solutions for tamper detection and protection of digital content. However, watermarking can cause damage to the sensitive information present in the cover work. Therefore, at the receiving end, the exact recovery of cover work may not be possible. Additionally, there exist certain applications that may not tolerate even small distortions in cover work prior to the downstream processing. In such applications, reversible data hiding instead of conventional watermarking is employed. Reversible data hiding of digital content allows full extraction of the watermark along with the complete restoration of the cover work. For the last few years, reversible data hiding techniques are gaining popularity because of its increasing applications in some important and sensitive areas, i.e., military communication, healthcare, and law-enforcement.

In this chapter we present an improved lossless data hiding scheme for digital images using integer wavelet transform and threshold embedding technique. This is basically our first motivation related to covert communication aspect as discussed in chapter 1. Data are embedded into the least two significant bit-planes of high frequency CDF (2,2) integer wavelet coefficients whose magnitudes are smaller than a certain predefined threshold. Histogram modification is applied as a preprocessing to prevent overflow/underflow. Experimental results show that this scheme outperforms the prior techniques in terms of a higher payload and better image quality.

3.1 Introduction

Data hiding is an important method for embedding secret data in a meaningful cover medium (such as an image or a video stream) to generate a stego-medium with a small distortion. One of the major requirements of data hiding is that the hidden data must be imperceptible [73]. In order to satisfy the imperceptibility requirement, the quality of stego-image must be improved. In practice, when a sender delivers a stego-image to a receiver, an illegal observer may not perceive the distortion in the transmission and so believes that it is only a common image.

Reversible data hiding can provide the extracted data as well as recover the original image at the receiver end without any loss. This property makes it very useful in the areas where image quality is strictly required though the images need the embedded data (watermark) to protect their authenticity/integrity or for some special purposes. The potential applications for this technique are cover authentication or content integrity verification, covert communication, and image/video coding (e.g., [74]).

Many existing data hiding algorithms are reversible or lossless (e.g., [48,

75, 51]). Typical embedding strategies include lossless compression in [48], difference expansion in [51], and histogram modification in [75]. Most of DE-based reversible data hiding algorithms (e.g.: [76, 77, 73, 78, 51]) prefer choosing small pixel pair differences for embedding. For example,Tian et al. [51] first selected the high-frequency coefficients of integer Haar wavelet transform (i.e., image pixel-pair differences) with small magnitude for DE expansion embedding. Alattar et al. [76] extended [51]'s pixel-pair difference expansion method using difference expansion of vectors.Kamstra et al. [77] improved [51] and selected embeddable differences using a sorting list based on the characteristics of the low-pass image. Small differences tend to occur at the beginning of the sorting list. In addition to the methods developed in integer Haar wavelet transform domain, some researchers also proposed DE expansion methods in other domains. For example, to better use the correlation information of neighboring pixels, [73] used image prediction rather than integer Haar wavelet transform. They still gave priority to small predicted pixel errors for DE expansion embedding. Thodi et al. further proposed a histogram-based selection scheme for choosing small differences in [78]. The reason of giving priority to small differences for DE expansion embedding is to acquire a high PSNR value of the embedded image. In the aforementioned algorithms, PSNR is used as a metric to evaluate visual quality of watermarked images.

Xuan et al. in [79] losslessly compresses one or more than one middle bit-planes to save space for data embedding. The bookkeeping data are also embedded as overhead. Later he applied threshold embedding technique to embed data in high frequency IWT coefficients in [80]. Lin et al. [81] presented a high-performance reversible data hiding technique based on the block difference histogram of a host image. A delicate lossless data hiding algorithm was proposed by [82]. Zeng et al. [83] used adjacent pixel difference and multi-layer embedding techniques on a scan path to obtain a reversible

watermarking technique. Coefficient-bias algorithm is utilized in [84, 85] to propose the technique of combinational reversible watermarking in both spatial and frequency domains.

The main contributions of this chapter is in enhancement of the data hiding capacity by introducing a new histogram shifting equation and an embedding mechanism. This modification can greatly improve the embedding capacity with graceful degradation of image quality. In addition we have the advantage of selecting a smaller difference coefficient as a threshold value to attain a particular payload requirement.

The rest of this chapter is organized as follows. Basic theory involved is explained in section 3.2. Section 3.3 describes our reversible data hiding algorithm in detail. Section 3.4 gives the experimental results of our algorithm. In Section 3.5, we draw the conclusion.

3.2 Theoretical Framework

The overall scheme is lossless so we use the CDF (2,2) integer wavelet transform. It is also adopted by JPEG2000 to obtain the wavelet coefficients for lossless image compression. As per the human visual system, human eye is not sensitive to distortions occurring in the high frequency subbands. So we embed data into HL, LH and HH subbands.

Because of the shifting of histograms of high-frequency integer wavelet subbands, it is quite possible that after inverse integer wavelet transform the pixel gray scale value may exceed the upper bound of 255 for an 8-bit image leading to overflow and/or may reduce to value less than the lower bound of 0 for an 8-bit image leading to the problem of underflow which ultimately violates the losslessness requirement. In order to overcome overflow and/or underflow, the histogram modification technique is applied to narrow

down the histogram from both sides. The bookkeeping information will be embedded into the cover media together with the information data.

In the aforementioned algorithms, PSNR is used as a metric to evaluate visual quality of watermarked images. PSNR $Q(I^P, I)$ of any image I^P with respect to another image I is calculated by

$$Q(I^P, I) = 10 \cdot \log_{10} \frac{MAX_I^2}{MSE} \tag{3.1}$$

where MAX_I represents the maximum possible pixel value of the image. When the pixels are represented using 8 bits per pixel, this is 255. The MSE of any image I^P with respect to another image I is calculated by (5.1).

$$MSE = \frac{1}{NM} \sum_{u=1}^{N} \sum_{v=1}^{M} [I^P(u,v) - I(u,v)]^2 \tag{3.2}$$

However, the PSNR value is essentially the measurement of statistical errors of a modified image rather than a metric for visual perception of the human eye. On the other hand, small differences usually correspond to flat image regions. So alteration to those differences would lead to less artifacts to which the human eye is very sensitive.

3.3 Proposed Algorithm

This section gives the details of our algorithm. We first discuss the embedding and extraction formulas, and then, show how to overcome the problem of overflow/underflow problem.

The absolute value of the high frequency coefficient x is compared with T. If $|x| < T$, the coefficient value is quadrupled and the last two LSBs are

replaced with the data to be hidden. The resultant coefficient is denoted by x'. If $x \geq T$, then $3T$ will be added to the coefficient, and if $x \leq -T$, the coefficient will be subtracted by $3(T-1)$, and no bit is embedded into this coefficient. These rules are summarized in Equation (3.3).

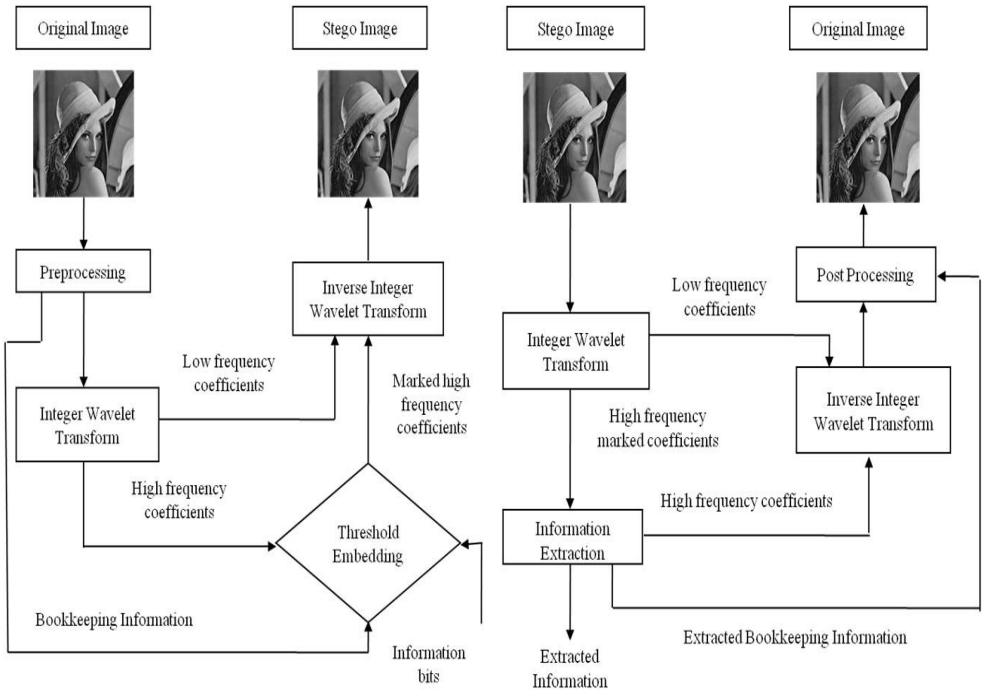
$$x' = \begin{cases} 4x + b & \text{if } |x| < T \\ x + 3T & \text{if } x \geq T \\ x - 3(T-1) & \text{if } x \leq -T \end{cases} \tag{3.3}$$

In the data extraction stage, IWT is applied to the marked image to obtain the marked IWT coefficients. For a coefficient, if it is less than 4T and larger than (-4T+3), the last two LSBs of this coefficient are the bits embedded into this coefficient. Otherwise, we proceed to the next coefficient since the current coefficient has no hidden bit in it. In addition to the data extraction, the original cover image should also be possible to be recovered. We can perfectly recover each high frequency coefficient and thus original value can also be recovered by applying Equation (3.4).

$$x = \begin{cases} \lfloor \frac{x'}{4} \rfloor & \text{if } 4T > x' > -4T + 3 \\ x' - 3T & \text{if } x' \geq 4T \\ x' + 3(T-1) & \text{if } x' \leq -4T + 3 \end{cases} \tag{3.4}$$

where $\lfloor y \rfloor$ takes the largest integer value that is smaller than y. The proposed lossless data hiding scheme embeds data into the first level high frequency subbands of images, namely, HL1, LH1 and HH1. Preprocessing is performed prior to data embedding to ensure no overflow/underflow will take place. The bookkeeping data of histogram modification (preprocessing) and the payload

are to be embedded into the high frequency IWT coefficients. The stego-image carrying hidden data will be obtained after inverse integer wavelet transform. Figure 3.1a and 3.1b show the flowchart of the proposed threshold embedding data hiding and data extraction.



(a) Embedding Scheme (b) Extraction Scheme

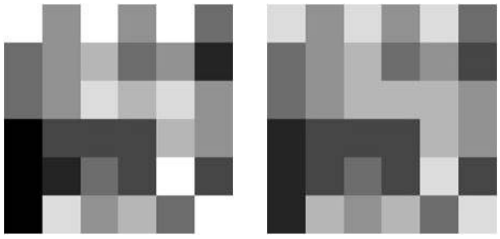
Figure 3.1: Flowchart of the proposed scheme: Embedding and Extraction

In order to illustrate the histogram narrow down process, we use the following simplified example, where the size of an original image is 6x6 with 8 grayscales (6x6x3) as shown in Figure 3.2.

Grayscale Value	0	1	2	3	4	5	6	7
Pixel no. before mod.	3	2	5	6	8	4	3	5
Pixel no. after mod.	0	3	7	6	8	7	5	0

Table 3.1: Histogram Data Before and After Modification

Bookkeeping information: For image of size $6 \times 6 \times 3$, the histogram is



(a)

(b)

7	4	7	4	7	3
3	4	5	3	4	1
3	4	6	5	6	4
0	2	2	2	5	4
0	1	3	2	7	2
0	6	4	5	3	7

(c)

6	4	6	4	6	3
3	4	5	3	4	2
3	4	5	5	5	4
1	2	2	2	5	4
1	2	3	2	6	2
1	5	4	5	3	6

(d)

Figure 3.2: Example of preprocessing: Sequence of display: Original Image; After preprocessing; Gray levels of original image: Gray levels of modified image

narrowed down 1 gray scale for both sides. $G = 2$, $\frac{G}{2} = 1$. The total bits length is 38 bits. S = the total book-keeping bit length 38 bits (00100110) + compressed number of gray scale 2 (010) + the first histogram from left hand side grayscale "1"(001) + record length 7(0111) + scan sequence (0111011) + the first histogram from right hand side grayscale "6"(110) + record length 7(0111) + scan sequence (1010101)

S = [001000110 010 001 0111 0111011 110 0111 1010101]

This is just for illustrative purpose only although it seems that the book-keeping information overhead is quite large but is not the case when gray level images of 256×256 and 256 gray level or more is taken as a cover image. The advantage is that a proper syntax has been defined for the formation of bookkeeping information.

The left hand side record bits with its left neighbor grayscale (0111011) in bookkeeping information shows that both first and fifth "2" by scanning ($< x = 2, y = 6 >, < x = 5, y = 2 >$) in Figure 3.2d are "1" in Figure 3.2c originally. Similarly 1010101 in the right hand side record bits in bookkeeping information show that the second, fourth and sixth "5" by scanning in Figure 3.2d is "6" in Figure 3.2c originally. Though this example is simple, the histogram modification algorithm illustrated here can be applied to image

of large size efficiently in terms of less computation and smaller amount of bookkeeping data.

From Figure 3.2 and Table 3.1, we can see that the range of the modified histogram now is from $1-6$ instead of $0-7$, i.e., no pixel assumes gray scales 0 and 7. After modification, grayscale 1 is merged into gray scale 2. Grayscale 0 becomes grayscale 1. In the same way, grayscale 6 is merged into grayscale 5. Grayscale 7 becomes grayscale 6. Histogram before and after modification is shown in Table 3.1 and bookkeeping information is also shown subsequently.

3.4 Experimental Results

We tested our algorithm on different types of images. Some experimental results are given in Figure 3.3 and Table 3.2. Figure 3.4 presents the graphical variation between the payload and the corresponding PSNR of the stego/embedded image with respect to the original image for few standard gray level images.

Images	Payload (bpp)	PSNR (dB)
Lena	1.45	30.56
House	1.50	35.59
Peppers	1.41	30.20
Jetplane	1.42	31.03

Table 3.2: Payload vs. PSNR for various images

According to Table 3.3 it is very clear that our algorithm has higher embedding capacity around a specific PSNR value with respect to previous existing schemes. Our algorithm satisfies the specific payload requirement with a smaller threshold value in comparison to Xuan et al's in [80] i.e. the data embedded is denser in the low magnitude difference coefficients. This

modification if wisely used with a genuine selection of threshold value can yield better results in terms of payload with relatively less proportionate degradation in PSNR.

(a) Original Image (b) 0.45; 1; 43.66 (c) 0.9; 2; 39.3 (d) 1.4; 8; 32.12

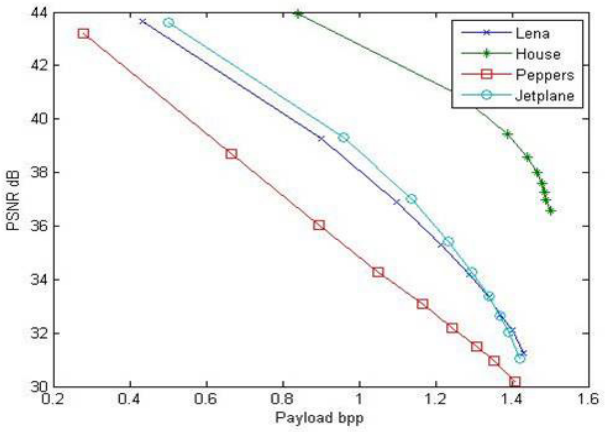
(e) Original Image (f) 0.5; 1; 43.6 (g) 0.82; 2; 39.3 (h) 1.4; 8; 32

(i) Original Image (j) 0.28; 1; 43.2 (k) 0.7; 2; 38.7 (l) 1.35; 8; 31

Figure 3.3: Experimental results: Sequence of display: Original Image; Embedded Image with following parameters (payload (bpp); Threshold (T); PSNR (dB))

Table 3.4 shows the relative percentage as well as payload size of overhead bits embedded as bookkeeping information with respect to the total payload size on various images. We can conclude that the overhead constitutes a very less portion of the total payload which is generally less than 1

Very high payload requirement could also be achieved by increasing the



(a) Embedding Scheme

Figure 3.4: Experimental Results

value of threshold. The advantage of the proposed scheme is that it requires less computation and time for high embedding scenarios since the embedding is done in single step only instead of multiple steps in the previous schemes.

Methods	Images		
	Lena	Peppers	Jetplane
Lin et al.'s [81]	231,971/30.2	268,042/30.2	289,877/30.1
Hsiao et al.'s [82]	303,700/30.0	303,736/30.0	286,488/ 30.0
Zeng et al.'s [83]	282,147/30.1	317,194/29.6	338,492/30.0
Yang et al.'s [84]	314,573/30.0	317,194/29.6	311,404/ 30.7
Yang et al.'s [85]	362,840/30.0	333,622/29.6	300,608/30.7
Proposed method	**379,461/30.6**	**369,317/30.2**	**372,513/31.0**

Table 3.3: Payload size (in no. of bits) and PSNR (in dB) comparison between the proposed payload size and PSNR (around 30 dB)

To attain a specific payload, our proposed algorithm requires smaller value of threshold. This results into less perceptual distortion in the embedded image by visual aspects of human eye as is shown through the help of results.

Images	No. of overhead bits	% relative to total bits embedded
Lena	214	0.09
House	2102	0.63
Peppers	8492	4.86
Jetplane	220	0.09

Table 3.4: Overhead information in terms of size and percentage relative to total bits embedded

3.5 Conclusion

In this chapter, we have discussed a new algorithm for reversible data hiding. Unlike the previous schemes which aim at embedding single bit per difference coefficient, we embed two bits per coefficient. Under the same threshold value our algorithm yields better payload or embedding capacity with less or equal distortion. The overall process is performed in single step with less computational complexity. Steganography schemes are generally weak enough to attack once the adversary suspects the existence of covert communication. To resist attack even after detection, one may embed the secret data in encrypted form so that adversary doesn't get hold of the actual secret message even after breaking the scheme. In the next chapter we will analyze the robustness of the existing digital watermarking technique (which is basically our second aspect of study) to ensure whether it can survive against forgery or can solve the issue of copyright protection.

Chapter 4

Cryptanalysis of Robust Digital Watermarking Technique

Most of the existing digital watermarking schemes use complicated signal processing technique to gain user confidence and most of them are also robust to benchmark attacks. However, there is a need to analyze each of the popular schemes individually and to check whether customized attacks can be mounted to highlight the weaknesses of the individual scheme itself.

In this chapter, we show that a generic watermark removal attack on a correlation-based watermarking scheme can be extended in general to a forgery attack on the same. In certain cases, even if there exists a weak watermark removal strategy, it may be extended to a strong forgery attack. We prove our case by implementing our strategy against MDEW [1] which is considered to be one of the robust correlation-based watermarking schemes in the DCT domain.

4.1 Introduction

Digital Watermarking is a method to insert secret user-specific information in a digital object (e.g., image, video, audio, etc.) that may later be used to ensure authenticity of the content. In case of image watermarking schemes, the basic philosophy is to produce marked copies $\tilde{I}^{(1)}, \tilde{I}^{(2)}, \ldots, \tilde{I}^{(n)}$ of an original image I, to be sold to authentic buyers $B_1, B_2, \ldots, B_n$, respectively. There are many standard image processing benchmarks to study whether an image watermarking scheme is robust or not [11] and most of the proposed schemes pass those benchmarks. However, from the point of view of cryptology, the scenario is considerably different, as the standard benchmarks mostly work on general image processing ideas, and are not customized to attack a specific watermarking scheme.

One of the applications of digital watermarking is to produce multiple marked copies $\tilde{I}^{(1)}, \tilde{I}^{(2)}, \ldots, \tilde{I}^{(n)}$ of an original image I, to be sold to authentic buyers $B_1, B_2, \ldots, B_n$, respectively. The i-th authentic buyer B_i, turned an attacker, has either of the two basic motives – removal of watermark from his marked image $\tilde{I}^{(i)}$, or producing a forged watermarked image $\tilde{I}^{(i,\#)}$ from his copy $\tilde{I}^{(i)}$, such that the forgery cannot be traced back to B_i.

In case of a correlation-based watermarking scheme, the marked copies are created from the original image I as follows. For each authentic buyer B_i, where $i = 1, 2, \ldots, n$, the owner of the image I first fixes a buyer-specific fingerprint $s^{(i)}$. Using the watermarking algorithm W, the i-th buyer-specific fingerprint $s^{(i)}$ is inserted within the original image I to produce the watermarked copy $\tilde{I}^{(i)} \leftarrow W(I, s^{(i)})$, specifically to be sold to the i-th buyer B_i. For each buyer B_i, fingerprint $s^{(i)}$, and hence the marked copy $\tilde{I}^{(i)}$, is unique.

From the point of view of cryptanalysis, it is assumed that the watermarking algorithm W is public and only the watermark information or the fingerprint $s^{(i)}$ is secret. It is also assumed that an attacker possesses one or

more watermarked copy of the original image I. This may be possible if an authentic buyer turns out to be a potential attacker, or if a group of authentic buyers collude to produce pirated copies of the image. The correlation-based watermarking techniques are known to be vulnerable to collusion attack [6]. This strategy, however, requires $O(\sqrt{\frac{n}{\ln n}})$ number of watermarked copies of the original image, where n is the effective length of the document. Naturally, if n is large, then the required number of copies is also large, and this many copies may not be available to the attacker. Thus it is more practical to consider attacks based on a single watermarked copy.

The general objective of a single-copy attack against the correlation-based schemes is either of the following.

- *Watermark Removal:* Given a single watermarked image $\tilde{I}^{(i)}$, remove the watermark information $s^{(i)}$ from the copy, and retrieve the original image I.
- *Watermark Forgery:* Given a single watermarked image $\tilde{I}^{(i)}$, produce a forged watermarked image $\tilde{I}^{(i,\#)}$ such that the forgery cannot be traced back to its origin, $\tilde{I}^{(i)}$.

The attacker, assumed to be B_i in our case, has complete information about the watermarking algorithm W, and his/her own watermarked copy $\tilde{I}^{(i)}$. However, B_i does not possess any information about the secret fingerprint $s^{(i)}$, or any other secret buyer-specific bits used in the process of watermarking. Of course, B_i does not possess the original image I either, or otherwise the attacks would be trivial.

Motivation: For correlation-based watermarking schemes, some *single-copy attacks* are already studied in the literature [12, 1, 13]. Especially, in [12], the authors have proposed a single-copy forgery attack on correlation-based watermarking schemes. They had illustrated the effectiveness of their strategy by attacking the Cox-Kilian-Leighton-Shamoon (CKLS) algorithm, and

later extended the same idea in [1] to cryptanalyse the optimal Differential Energy Watermarking (DEW) scheme, proposed in [86]. However, the attack model proposed in [12, 1] is not completely general, as it does not work against the watermarking scheme they have themselves proposed in [1] – the MDEW watermarking algorithm. In fact, the authors of [1] have presented the MDEW scheme as a conscious design to avoid this kind of attacks. It remains an open question whether there exists a general strategy to cryptanalyze correlation-based watermarking schemes, and mount single-copy forgery attacks on them. We tackle this question in our current work.

Contribution: In this chapter, we propose a strategy that converts a single-copy watermark removal attack on any correlation-based scheme to a single-copy forgery attack on the same. In particular, we show that if a correlation-based watermarking scheme, like MDEW [1], has the chance of even a very weak single-copy watermark removal attack, the same strategy may be extended to obtain a strong single-copy forgery attack.

We choose MDEW as our target as it has a conscious design principle that tries to avoid straight-forward but customized single-copy forgery attacks, as claimed in [1] by the designers of MDEW. However, the conscious design of MDEW [1] scheme, towards having better security, is shown to be vulnerable against our general watermark removal-to-forgery attack.

Organization of the Chapter: In Section 4.2, we present our idea for extending a watermark removal strategy to forgery against a specific example – MDEW watermarking scheme, as proposed in [1]. In Section 4.3, we present detailed experimental results, and extend our strategy to propose similar attack against correlation-based watermarking schemes in general. Finally, Section 4.4 concludes the chapter.

4.2 Forgery against MDEW watermarking scheme

MDEW [1] works alike most of the correlation-based watermarking schemes, as in [87, 86]. Let the original image be I, and the owner wants to sell authentic copies of I to buyers $B_1, B_2, \ldots$. Then, the embedding and extraction of the watermark is performed by the owner as follows.

4.2.1 Watermark Embedding and Extraction in MDEW

Let the size of the original image I be $N \times N$. First the owner applies 8×8 block-wise DCT on I to get the DCT-transformed image I_d. Then, the owner performs a random grouping on the 8×8 DCT blocks of I_d, considering it as a two-dimensional array. One may perform this random grouping using a random permutation P on the blocks of I_d. An example of the random grouping, as a result of applying the random permutation P on I_d, is illustrated in Figure 4.1 over a matrix of size 8×8. The groups, each consisting of n blocks, are termed as 'lc-regions', and in Figure 4.1, we have four $n = 16$ size lc-regions marked with different colors.

0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

(a) DCT Image

0*	1$	2$	3*	4*	5$	6*	7$
8*	9$	10*	11$	12*	13*	14$	15$
16$	17*	18$	19*	20$	21*	22$	23*
24$	25$	26*	27*	28$	29$	30*	31*
32*	33$	34$	35*	36$	37*	38$	39*
40*	41$	42*	43*	44$	45*	46$	47$
48$	49*	50$	51*	52*	53$	54$	55*
56$	57*	58$	59*	60$	61*	62$	63*

(b) Permuted DCT Image

Figure 4.1: DCT images where numerals represent blocks of 8×8.

Every lc-region is again subdivided into two lc-subregions A and B, as illustrated in Figure 4.1 by the symbols $*$ and \$ respectively, and the energies E_A and E_B of the lc-subregions are calculated. The expressions for the energies are given by

$$E_A(q,n) = \sum_{b=0}^{\frac{n}{2}-1} \sum_{j=1}^{q} |\theta_{j,b}|, \quad E_B(q,n) = \sum_{b=\frac{n}{2}}^{n-1} \sum_{j=1}^{q} |\theta_{j,b}| \tag{4.1}$$

where $|\theta_{j,b}|$ is the absolute value of DCT coefficient of the 8×8 DCT block b in that lc-subregion (A or B), corresponding to frequency j, where $j = 0$ means the DC coefficient of the block that is not considered in the sum. Note that we write $E_A(q,n), E_B(q,n)$ as E_A, E_B, where the values of n, q are implicitly understood for a specific image I.

The condition in MDEW is that the initial random grouping P and the subdivision into lc-subregions A and B for the DCT image I_d has to be performed in such a fashion that

$$|E_A - E_B| \leq \Delta, \tag{4.2}$$

where Δ is a predetermined small threshold. In fact, all that we require is a margin with which the condition $E_A \approx E_B$ is satisfied after grouping. This may not be true for all random permutations, and hence P is chosen over a few iterations such that this condition is satisfied. The information regarding this lc-region and lc-subregion distribution can be stored in a matrix, π, say. This information, π, is determined by the owner for every image I, and is kept secret during the whole process. In fact, π is the same for all the buyers of image I, and serves as the primary key for the MDEW scheme.

For each legitimate buyer B_i, the watermark signal or fingerprint is generated as a pseudo-random bit string $s^{(i)}$ of length l, where $l = G/n$ denotes

the number of lc-regions in the DCT image I_d, which has a total G number of 8×8 DCT blocks and each lc-region is of size n. Now, the goal of watermark embedding is to insert each bit of $s^{(i)}$ into one lc-region of I_d. This modified DCT image, $\tilde{I}_d^{(i)}$, may then be subjected to inverse DCT transform to obtain the watermarked image $\tilde{I}^{(i)}$, to be sold to buyer B_i.

Note that we have $E_A \approx E_B$ for each lc-region of I_d, after grouping according to π. To embed a bit of $s^{(i)}$ in an lc-region, the owner introduces the following modifications in the energies of the individual blocks:

$$\begin{aligned} \text{Embed 0:} \qquad E'_A(q,n) &= \sum_{b=0}^{\frac{n}{2}-1} \sum_{j=1}^{q} (1+\alpha_1)|\theta_{j,b}|, \text{ and} \\ E'_B(q,n) &= \sum_{b=\frac{n}{2}}^{n-1} \sum_{j=1}^{q} (1-\alpha_2)|\theta_{j,b}|; \end{aligned} \tag{4.3}$$

$$\begin{aligned} \text{Embed 1:} \qquad E'_A(q,n) &= \sum_{b=0}^{\frac{n}{2}-1} \sum_{j=1}^{q} (1-\alpha_2)|\theta_{j,b}|, \text{ and} \\ E'_B(q,n) &= \sum_{b=\frac{n}{2}}^{n-1} \sum_{j=1}^{q} (1+\alpha_1)|\theta_{j,b}|, \end{aligned} \tag{4.4}$$

where $\alpha_1, \alpha_2 > 0$ are chosen such that $E'_A - E'_B > \Delta'$ if bit 0 is embedded, and $E'_B - E'_A > \Delta'$ if bit 1 is embedded, where Δ' is once again a predetermined threshold. The parameters α_1, α_2 should be small so that after the modification of the DCT values, the image quality is not degraded.

During watermark extraction for the i-th buyer, note that the owner does not specifically require the original image I. All he/she requires is the grouping information (or the secret key) π, the predetermined threshold Δ', and the watermarked image $\tilde{I}^{(i)}$ corresponding to the i-the buyer B_i. To extract the fingerprint $s^{(i)}$, the owner first takes the DCT-transform of $\tilde{I}^{(i)}$ to obtain $\tilde{I}_d^{(i)}$, say. Then the owner may apply the grouping π on $\tilde{I}_d^{(i)}$, and examine the polarity of $E'_A - E'_B$ with respect to Δ' in each lc-region. This will reveal

the exact bitstream $s^{(i)}$ embedded in the image, and the owner may now verify the identity of the buyer by searching for this $s^{(i)}$ in the database of legitimate buyers. If $s^{(i)}$ does not match with any fingerprint produced by the owner, then it may be concluded that the specific watermarked copy $\tilde{I}^{(i)}$ is not created by the owner and that $\tilde{I}^{(i)}$ may be a forged copy.

4.2.2 Formal model of forgery attack on MDEW

Based on the discussion so far, we may frame the model of forgery attack on MDEW scheme as follows. The watermark embedding algorithm is denoted as W, and the watermark extraction algorithm is denoted by W^{-1}, to imply the inverse of the embedding process. Let F denote the algorithm for forgery, as used by an attacker, and T be the algorithm that the owner uses to trace the attacker in case a forgery has been made. If there are N_B legitimate buyers in total, including the attacker, then the advantage of the owner in tracing the attacker from a forged copy of the image $F(\tilde{I}^{(i)})$ may be defined as

$$\mathrm{Adv}(\tilde{I}^{(i,\#)}) := \left| \Pr\left(T\left(W^{-1}(F(\tilde{I}^{(i)}))\right) = B_i\right) - \frac{1}{N_B} \right|.$$

In general terms, the above expression denotes the probability with which the owner can trace back the attacker, above the probability of a random guess, $\frac{1}{N_B}$. The goal of a forger is to lower the value of owner's advantage, $\mathrm{Adv}(\tilde{I}^{(i,\#)})$, and the attack is completely successful if $\mathrm{Adv}(\tilde{I}^{(i,\#)}) = 0$.

In general, the algorithm T that the owner uses to trace the attacker in such case of forgery is as follows:

1. Step I: Extract the watermark fingerprint from the forged image $\tilde{I}^{(i,\#)} = F(\tilde{I}^{(i)})$ to get $s^{(i,\#)} \leftarrow W^{-1}(\tilde{I}^{(i,\#)})$.

2. Step II: Find the correlations between $s^{(i,\#)}$ and all valid owner-generated $s^{(i)}$ in the buyer database.

3. Step III: Identify B_j as the attacker if $s^{(i,\#)}$ has significantly high (far from 0) correlation with $s^{(j)}$.

Under this consideration, we may simplify the attack model to say that the attacker will be successful in forgery if the correlation between $s^{(i,\#)}$ and $s^{(i)}$ is considerably low, that is, numerically close enough to 0, and the advantage of the owner may be expressed as:

$$\mathrm{Adv}(\tilde{I}^{(i,\#)}) := \left|\mathrm{Cor}\left(s^{(i)}, W^{-1}(F(\tilde{I}^{(i)}))\right)\right|. \tag{4.5}$$

The attacker, B_i in this case, will be successful in untraceable forgery if there exists a j for which

$$\left|\mathrm{Cor}\left(s^{(j)}, W^{-1}(F(\tilde{I}^{(i)}))\right)\right| > \mathrm{Adv}(\tilde{I}^{(i,\#)}).$$

However, we impose a stricter condition than what is required, and call a forgery F successful only if $\mathrm{Adv}(\tilde{I}^{(i,\#)}) \approx 0$.

4.2.3 General Forgery Attack on MDEW

The performance of MDEW scheme is quite robust against the standard signal processing attacks, as experimented in [1]. Certain statistical analysis had also been made in [1] to explain the security parameters. We further perform some analysis on MDEW to set the base for a general forgery attack. For a simplified analysis, we assume $\alpha_1 = \alpha_2 = \alpha$.

Note that the DCT values of neighboring blocks in an image may be correlated, but after the random distribution π is made, the values in the DCT blocks, whether or not neighboring, can always be assumed to be independent. We assume that the energies of the 8×8 DCT blocks of I_d are *i.i.d.*

random variables X_b, for $0 \leq b \leq G-1$, satisfying

$$X_b \sim N\left(\mu = \frac{1}{G}\sum_{b=0}^{G-1} X_b, \sigma^2 = \frac{1}{G-1}\sum_{b=0}^{G-1}(X_b - \mu)^2\right).$$

The energy difference D between the two lc-subregions A and B within a specific lc-region is given by

$$D = \sum_{k=1}^{n/2} X_{A_k} - \sum_{k=1}^{n/2} X_{B_k}, \tag{4.6}$$

where X_{A_k} is the energy of the k-th block of the subregion A and X_{B_k} is the energy of the k-th block of subregion B. D is a linear combination of $i.i.d.$ random variables, and thus itself a random variable satisfying $D \sim N(0, n\sigma^2)$ (see [1] for details). After inserting watermark bits, the energy difference in the lc-region will change to

$$D' = \sum_{k=1}^{n/2} X_{A_k}(1+\alpha) - \sum_{k=1}^{n/2} X_{B_k}(1-\alpha), \tag{4.7}$$

where the value of α could be positive or negative depending on whether 0 or 1 is inserted in the corresponding region. The expectation of D', the modified energy difference, will be

$$E(D') = E\left(\sum_{k=1}^{n/2} X_{A_k}(1+\alpha) - \sum_{k=1}^{n/2} X_{B_k}(1-\alpha)\right) = n\alpha\mu, \tag{4.8}$$

and the variance of D' will be

$$V(D') \;=\; V\left(\sum_{k=1}^{n/2} X_{A_k}(1+\alpha) - \sum_{k=1}^{n/2} X_{B_k}(1-\alpha)\right)$$

$$\begin{aligned} &= \sum_{k=1}^{n/2} \left((1+\alpha)^2 V(X_{A_k}) + (1-\alpha)^2 V(X_{B_k})\right) \\ &= n(1+\alpha^2)\sigma^2. \end{aligned} \tag{4.9}$$

Now that we have all statistical properties of the important parameters, we may device and analyze a naive forgery attack on the MDEW scheme.

First note that the distribution of lc-regions/subregions is coded in a permutation π, unknown to the attacker. After taking the DCT transform of watermarked image $\tilde{I}^{(i)}$, suppose that the attacker finds $G = 2^\omega$ many 8×8 DCT blocks in $\tilde{I}_d^{(i)}$, and let each lc-region consists of $n = 2^{\frac{\omega}{2}}$ such blocks. In this case, the number of all possible groupings comes to

$$\binom{G}{n} \cdot \binom{G-n}{n} \cdot \binom{G-2n}{n} \cdots \binom{n}{n} = \frac{(2^\omega)!}{((2^{\frac{\omega}{2}})!)^{2^{\frac{\omega}{2}}}}.$$

For large values of ω (≥ 4), we have $\frac{(2^\omega)!}{((2^{\frac{\omega}{2}})!)^{2^{\frac{\omega}{2}}}} > 2^{2^\omega}$. One should further consider the possibilities of creating two subregions inside each lc-region. Naturally, this makes a naive guessing of π impossible in all respects, and we may safely assume that π remains an unknown random permutation of the DCT blocks from the point of view of the attacker.

Once the distribution π is unknown, the attacker has only one choice left – that is to look into each of the blocks and try to modify the energies. The idea for forgery is as follows.

General Forgery Attack on MDEW
Input – Authentic watermarked image $\tilde{I}^{(i)}$
Output – Forged watermarked image $\tilde{I}^{(i,\#)}$
Preprocessing – Take DCT transform of $\tilde{I}^{(i)}$ to get $\tilde{I}_d^{(i)}$
Algorithm – For each block of $\tilde{I}_d^{(i)}$, do the following

- Guess whether the energy of the block had been increased or decreased

during watermark embedding.

- Depending on the guess, modify the DCT values to reverse the effects of watermark embedding. That is, if the energy of the block was increased (respectively decreased), then decrease (respectively increase) the energy.

The effectiveness of this forgery will directly depend on the correctness of the initial guess for each block. If the attacker knew π, each of these guesses would be correct, and the attacker could completely reverse the effect of watermarking. However, with π an unknown random permutation, the guessing strategy is of prime importance.

4.2.4 Forgery on MDEW using Random Guess

An adversary can obviously try a naive approach of random guessing. In random guessing the probability of every correct guess is $\frac{1}{2}$. In this strategy, we randomly decide, with equal probability, whether to increase or decrease the DCT values of each 8×8 DCT block in $\tilde{I}_d^{(i)}$, and construct the forged image $\tilde{I}^{(i,\#)}$, as illustrated in Algorithm 1. We model the random guess

Algorithm 1 Forgery on MDEW using Random Guess

1: Apply 8×8 DCT on $\tilde{I}^{(i)}$ to obtain $\tilde{I}_d^{(i)}$.
2: **for** $y = 1$ to G **do**
3: Generate a random bit d by tossing an unbiased coin.
4: **if** $d = 1$ **then**
5: Decrease DCT values $\theta_{j,y} \leftarrow \theta_{j,y} \cdot (1 - \alpha_1')$ for the known subset of coefficients $j = 1, 2, \ldots, q$.
6: **else**
7: Increase DCT values $\theta_{j,y} \leftarrow \theta_{j,y} \cdot (1 + \alpha_2')$ for the known subset of coefficients $j = 1, 2, \ldots, q$.
8: **end if**
9: **end for**
10: Apply inverse 8×8 DCT to construct forged image $\tilde{I}^{(i,\#)}$.

strategy by a binomial random variable Z, where $Z = 1$ if the guess is correct and $Z = -1$ if the guess is incorrect. Thus the distribution of Z is as follows:

$$Z = \begin{cases} 1\ ; & \text{prob.} = 1/2 \qquad E(Z) = 0 \\ -1\ ; & \text{prob.} = 1/2 \qquad V(Z) = 1 \end{cases}$$

If after forgery, the energy difference between the lc-subregions A and B is denoted by D'', then Eqn. (4.10) represents the effect of Z on D'', where we assume $\alpha'_1 = \alpha'_2 = \alpha'$.

$$\begin{aligned} D'' = & \sum_{k=1}^{n/2} X_{A_k}(1+\alpha)(1-\text{sgn}(\alpha)\alpha' Z_k) \\ & - \sum_{k=1}^{n/2} X_{B_k}(1-\alpha)(1+\text{sgn}(\alpha)\alpha' Z'_k). \end{aligned} \tag{4.10}$$

Here $0 < \alpha' < 1$, and sgn(.) is the signum function, i.e., $\text{sgn}(\alpha) = 1$ if $\alpha > 0$ and $\text{sgn}(\alpha) = -1$ if $\alpha < 0$. Furthermore, Z_k, Z'_k (where $1 \leq k \leq \frac{n}{2}$) are *i.i.d.* random variables with the same distribution as Z, i.e., $E(Z_k) = E(Z'_k) = 0$, $V(Z_k) = V(Z'_k) = 1$. Then,

$$\begin{aligned} E(D'') &= E\left(\sum_{k=1}^{n/2} X_{A_k}(1+\alpha)(1-\text{sgn}(\alpha)\alpha' Z_k) \right. \\ &\qquad \left. - \sum_{k=1}^{n/2} X_{B_k}(1-\alpha)(1+\text{sgn}(\alpha)\alpha' Z'_k) \right) \\ &= n\mu\left(\alpha - \text{sgn}(\alpha)\alpha' E(Z_k)\right) = n\alpha\mu = E(D'), \end{aligned} \tag{4.11}$$

and the variance of D'' is

$$\begin{aligned} V(D'') &= V\left(\sum_{k=1}^{n/2} X_{A_k}(1+\alpha)(1-\mathrm{sgn}(\alpha)\alpha' Z_k) \right. \\ &\qquad \left. -\sum_{k=1}^{n/2} X_{B_k}(1-\alpha)(1+\mathrm{sgn}(\alpha)\alpha' Z'_k)\right) \\ &= \sum_{k=1}^{n/2} \big((1+\alpha)^2 V(X_{A_k}(1-\mathrm{sgn}(\alpha)\alpha' Z_k)) \\ &\qquad +(1-\alpha)^2 V(X_{B_k}(1+\mathrm{sgn}(\alpha)\alpha' Z'_k)\big). \end{aligned} \tag{4.12}$$

Now, we may compute the variance $V(X_{A_k}(1-\mathrm{sgn}(\alpha)\alpha' Z_k))$ rigorously as $E(X_{A_k}^2)E((1-\mathrm{sgn}(\alpha)\alpha' Z_k)^2) - (E(X_{A_k})E(1-\mathrm{sgn}(\alpha)\alpha' Z'_k))^2 = \sigma^2\alpha'^2 + \mu^2\alpha'^2+\sigma^2$, and similarly obtain $V(X_{A_k}(1+\mathrm{sgn}(\alpha)\alpha' Z_k)) = \sigma^2\alpha'^2+\mu^2\alpha'^2+\sigma^2$. From Eqn. (4.12), we get

$$\begin{aligned} V(D'') &= \frac{n}{2}\left((1+\alpha)^2+(1-\alpha)^2\right)(\sigma^2\alpha'^2+\mu^2\alpha'^2+\sigma^2) \\ &= n(1+\alpha^2)(\sigma^2\alpha'^2+\mu^2\alpha'^2+\sigma^2). \end{aligned} \tag{4.13}$$

In the above analysis, we have considered a random region [SR(A), SR(B)] and analyzed the effect of forgery based on random guess. Since the expectation of the energy difference D'' in case of the forged image $\tilde{I}^{(i,\#)}$ is the same as that in case of the authentic copy $\tilde{I}^{(i)}$, the reversal of energy polarity $(E'_A - E'_B)$ in the lc-region considered above will be insignificant. Thus, the correlation between $s^{(i)} \leftarrow W^{-1}(\tilde{I}^{(i)})$ and $s^{(i,\#)} \leftarrow W^{-1}(\tilde{I}^{(i,\#)})$ will be considerably high, and hence we prove that the random guess strategy is not useful for mounting a forgery attack on MDEW.

The variance of D'' changes from that of D', and the change is proportional to the square of the parameter α' which is used to reverse the effect of α.

The change in variance only signifies the increased dispersion of energies in the forged image.

4.2.5 Forgery on MDEW using Informed Guess

Suppose that there is some information available to the attacker that helps him/her to guess the increase/decrease in energy per block with probability slightly higher than that in case of random guess. In particular, the attacker can guess correctly, whether the DCT values in a block has been increased or decreased, with probability $\frac{1}{2}+\epsilon$, for some non-negligible $\epsilon > 0$. That is, the distribution of the random variable Z, in this strategy, is:

$$Z = \begin{cases} 1\ ; \quad \text{prob.} = \frac{1}{2}+\epsilon & E(Z) = 2\epsilon \\ -1\ ; \quad \text{prob.} = \frac{1}{2}-\epsilon & V(Z) = 1-4\epsilon^2 \end{cases}$$

In this case of an informed guess, the expectation of D'' is

$$\begin{aligned} E(D'') &= E\left(\sum_{k=1}^{n/2} X_{A_k}(1+\alpha)(1-\text{sgn}(\alpha)\alpha' Z_k) \right. \\ &\qquad \left. -\sum_{k=1}^{n/2} X_{B_k}(1-\alpha)(1+\text{sgn}(\alpha)\alpha' Z'_k)\right) \\ &= \sum_{k=1}^{n/2} ((1+\alpha)E(X_{A_k})(1-\text{sgn}(\alpha)\alpha' E(Z_k)) \\ &\qquad -(1-\alpha)E(X_{B_k})(1+\text{sgn}(\alpha)\alpha' E(Z'_k))) \\ &= \frac{n\mu}{2}((1+\alpha)(1-2\text{sgn}(\alpha)\alpha'\epsilon) \\ &\qquad -(1-\alpha)(1+2\text{sgn}(\alpha)\alpha'\epsilon)) \end{aligned}$$

$$
\begin{aligned}
&= n\mu(\alpha - 2\text{sgn}(\alpha)\alpha'\epsilon) \\
&= E(D') - 2\text{sgn}(\alpha)n\mu\epsilon\alpha', \qquad (4.14)
\end{aligned}
$$

and the variance of D'' is given by

$$
\begin{aligned}
V(D'') = V \Bigg(& \sum_{k=1}^{n/2} X_{A_k}(1+\alpha)(1-\text{sgn}(\alpha)\alpha' Z_k) \\
& - \sum_{k=1}^{n/2} X_{B_k}(1-\alpha)(1+\text{sgn}(\alpha)\alpha' Z'_k) \Bigg) \\
= & \sum_{k=1}^{n/2} \big((1+\alpha)^2 V(X_{A_k}(1-\text{sgn}(\alpha)\alpha' Z_k)) \\
& + (1-\alpha)^2 V(X_{B_k}(1+\text{sgn}(\alpha)\alpha' Z'_k)) \big) . \qquad (4.15)
\end{aligned}
$$

After simplifying the above expression, we get $V(D'')$ as $n(\mu^2\alpha'^2(1+\alpha^2)(1-4\epsilon^2) + \sigma^2((1+\alpha^2)(1+\alpha'^2)$ - $8\text{sgn}(\alpha)\alpha\alpha'\epsilon))$.

From Eqn. (4.14), it is obvious that expectation of D'' differs from that of D', and the difference depends on ϵ, α, μ and α'. Among these parameters, the attacker has control only over α', the amount of increase/decrease in the DCT values while forging the image. The other parameters α, μ and ϵ are fixed, either by the owner of the image, or by the information the attacker has got to base his/her guesses on.

If the attacker can obtain any significant information that makes $\epsilon > 0$, he/she may tune the parameter α' to create a large enough difference between D' and D'', possibly to the extent that the energy difference polarity is reversed. This helps the attacker to mount a successful forgery attack on the MDEW scheme, and constitutes the main theme of our work.

4.2.6 Watermark Removal Attack extended to Forgery on MDEW

So far we have seen that if the attacker gets a good guessing probability for each block of the DCT domain image $\tilde{I}_d^{(i)}$, by some strategy, then the probability of success for the forgery increases. Suppose that there exists a weak watermark removal attack against MDEW that produces a not-so-good approximation of the original image I from $\tilde{I}^{(i)}$. Let us denote the estimate of I as I^C. If the attacker possesses both $\tilde{I}^{(i)}$ and the approximate original image I^C, then he/she may transform both to the DCT domain, compare $\tilde{I}_d^{(i)}$ with I_d^C block by block, and take a good guess as to whether the DCT values for each block were increased or decreased during watermark embedding. The closer the approximate image I^C is to I, the better will be the guess probability, i.e., ϵ, for the attacker. We know from the previous subsection that even if the watermark removal attack is weak, that is, even if it provides only a very small ϵ, the attacker may still magnify its effects in the final forgery attack, by tuning other parameters.

This provides a general platform to extend any watermark removal attack on MDEW to a forgery attack on the same scheme. In fact, even a very weak and practically unusable watermark removal technique for MDEW can be exploited against the scheme, quite effectively, in such a forgery attack. We substantiate our claim through the following example.

4.2.7 Median Filter based Forgery on MDEW

Watermark embedding on any image I is generally considered as adding noise in the image where the watermark fingerprint is treated as noise. Thus, any suitable noise removal filter may work as a naive watermark removal strategy that approximates I from a marked copy $\tilde{I}^{(i)}$. Median filter is one of the

simplest examples that could be applied on the noisy image $\tilde{I}^{(i)}$ to get back I^C, a very crude approximation of I.

The attacker may now exploit the knowledge of $\tilde{I}^{(i)}$ and I^C together to form his/her guesses. The attacker takes both the images $\tilde{I}^{(i)}$ and I^C to the transformed domain by applying 8×8 DCT. In the DCT domain, he/she compares the energy X of the corresponding blocks in both the images and tries to guess whether the energy of that specific block has been increased or decreased during watermark embedding process. After the guess is finalized, the attacker may try to reverse the embedding effect by modifying the DCT values towards the opposite polarity with respect to the embedding process, so that a forged copy $\tilde{I}^{(i,\#)}$ is created.

Let $|\theta_j^w|$ and $|\theta_j^m|$ represent the absolute values of the DCT coefficients corresponding to frequency j in a specific block of $\tilde{I}^{(i)}$ and I^C, respectively. Similarly, let X_Φ and X_Ψ represent the energy corresponding to a specific block of $\tilde{I}^{(i)}$ and I^C, respectively. Then the median filter based forgery may be summarized as in Algorithm 2.

In case of median filtering, we notice that the extra margin in the probability of guessing, ϵ, is not just a constant, but it depends directly on the energy of a block, that is X. In fact, ϵ behaves proportional to the value of X, and gives a better guessing probability for the high energy blocks. From our experiments, we have found that the relation between ϵ and X can be modeled as $\epsilon = \frac{X}{2M}$, where $M = \max\{X\}$. Thus, the bias in the guessing probability can be modeled as

$$Z = \begin{cases} 1\ ; & \text{prob.} = \frac{1}{2} + \frac{X}{2M} \\ -1\ ; & \text{prob.} = \frac{1}{2} - \frac{X}{2M}, \end{cases}$$

and the expectation and variance of Z can be computed as

$$E(Z) = E(E(Z|X)) = E(X)/M = \mu/M, \quad \text{and}$$

$$V(Z) = E(Z^2) - (E(Z))^2 = E(E(Z^2|X)) - (E(E(Z|X))^2$$

$$= V(X)/M^2 = \sigma^2/M^2.$$

Algorithm 2 Median Filter based Forgery on MDEW

1: Apply median filter with dimensions $r \times s$ on $\tilde{I}^{(i)}$ and store the resultant image as I^C, an approximation to I.
2: Apply 8×8 DCT on both $\tilde{I}^{(i)}, I^C$ to obtain $\tilde{I}_d^{(i)}$ and I_d^C.
3: **for** $y = 1$ to G **do**
4: Calculate $X_{\Phi,y} = \sum_{j=1}^{q} |\theta_{j,y}^{(i)}|$, $X_{\Psi,y} = \sum_{j=1}^{q} |\theta_{j,y}^{C}|$.
5: **if** $X_{\Phi,y} > X_{\Psi,y}$ **then**
6: Decrease DCT values $\theta_{j,y}^{w} \leftarrow \theta_{j,y}^{w} \cdot (1 - \alpha_1')$ for the known subset of coefficients $j = 1, 2, \ldots, q$.
7: **else**
8: Increase DCT values $\theta_{j,y}^{w} \leftarrow \theta_{j,y}^{w} \cdot (1 + \alpha_2')$ for the known subset of coefficients $j = 1, 2, \ldots, q$.
9: **end if**
10: **end for**
11: Apply inverse 8×8 DCT to construct forged image $\tilde{I}^{(i,\#)}$.

Now we may calculate the expected value of D'' as follows:

$$E(D'') = E\left(\sum_{k=0}^{n/2} X_{A_k}(1+\alpha)(1-\text{sgn}(\alpha)\alpha' Z_k) - \sum_{k=0}^{n/2} X_{B_k}(1-\alpha)(1+\text{sgn}(\alpha)\alpha' Z_k')\right)$$

$$= \sum_{k=0}^{n/2} \left((1+\alpha)E(X_{A_k}(1-\text{sgn}(\alpha)\alpha' Z_k)) - (1-\alpha)E(X_{B_k}(1+\text{sgn}(\alpha)\alpha' Z_k'))\right).$$

We have the distribution of Z_i and Z_i' identical to Z, and hence dependent on X. Thus, we may compute $E(D'')$ as

$$\begin{aligned} E(D'') &= \sum_{k=0}^{n/2} ((1+\alpha)E(E(X_{A_k}(1-\text{sgn}(\alpha)\alpha' Z_k)|X_{A_k})) \\ &\qquad -(1-\alpha)E(E(X_{B_k}(1+\text{sgn}(\alpha)\alpha' Z_k')|X_{B_k}))) \\ &= \sum_{k=0}^{n/2} ((1+\alpha)E(X_{A_k})(1-\text{sgn}(\alpha)\alpha' E(X_{A_k}/M)) \\ &\qquad -(1-\alpha)E(X_{B_k})(1+\text{sgn}(\alpha)\alpha' E(X_{B_k}/M))), \end{aligned}$$

which, in turn, provides

$$\begin{aligned} E(D'') &= \frac{n\mu}{2}((1+\alpha)(1-\text{sgn}(\alpha)\alpha'\mu/M)) \\ &\qquad -(1-\alpha)(1+\text{sgn}(\alpha)\beta\mu/M)))) \\ &= n\mu(\alpha - \text{sgn}(\alpha)\alpha'\mu/M) \\ &= E(D') - \text{sgn}(\alpha)n\alpha'\mu^2/M. \end{aligned} \tag{4.16}$$

Since the mean value of $E(D'')$ is changed from $E(D')$ by the factor proportional to $\alpha'\mu/M$. So if the attacker chooses the parameter $\alpha' > |\frac{\alpha M}{\mu}|$, the polarity of the energy difference in the specific lc-region will get reversed.

Note that we want the probability of polarity reversal in the lc-regions to be close to $\frac{1}{2}$, as in that case, the two watermark fingerprints $s^{(i)} \leftarrow W^{-1}(\tilde{I}^{(i)})$ and $s^{(i,\#)} \leftarrow W^{-1}(\tilde{I}^{(i,\#)})$ will have about half of the bits matching. This condition makes the correlation between $s^{(i)}$ and $s^{(i,\#)}$ close to zero, or negligible, as desired in a forgery attack.

In the next section, we present the experimental results of our forgery at-

tacks on MDEW, in both cases – random guess and median filter based guess – to illustrate the power of extending a weak watermark removal technique to a strong forgery attack on correlation-based watermarking schemes.

Table 4.1: Results of Forgery Attack on MDEW based on Random Guess

Image	Forgery values		Quality factors (dB)		$\mathrm{Cor}(s^{(i)}, s^{(i,\#)})$		Guess probability $(1/2+\epsilon)$	
	α_1'	α_2'	$Q^{(\#)}$	$Q^{(i,\#)}$	(mean)	(SD)	(mean)	(high energy blocks)
Watermark embedding parameters: $\alpha_1 = 0.1$ and $\alpha_2 = 0.1$.								
Lena	0.200	0.200	37.800	38.760	0.980	0.010	0.501	0.500
Lena	0.270	0.270	35.620	36.180	0.970	0.020	0.500	0.500
Cameraman	0.270	0.270	34.400	34.800	0.870	0.040	0.500	0.500
Lake	0.270	0.270	33.000	33.440	0.970	0.020	0.500	0.500
Peppers	0.270	0.270	35.300	35.800	0.920	0.030	0.500	0.500
Jetplane	0.270	0.270	34.100	34.660	0.940	0.030	0.500	0.500
Lena	0.300	0.300	34.820	35.280	0.960	0.020	0.500	0.500
Cameraman	0.300	0.300	33.550	34.000	0.790	0.050	0.500	0.500
Lake	0.300	0.300	32.100	32.540	0.930	0.040	0.500	0.500
Peppers	0.300	0.300	34.500	34.930	0.910	0.040	0.499	0.499
Jetplane	0.300	0.300	33.300	33.800	0.870	0.040	0.500	0.500

Table 4.2: Results of Forgery Attacks on MDEW based on Median Filter Guess

Image	Forgery values		Quality factors (dB)		$\mathrm{Cor}(s^{(i)}, s^{(i,\#)})$		Guess probability $(1/2+\epsilon)$	
	α_1'	α_2'	$Q^{(\#)}$	$Q^{(i,\#)}$	(mean)	(SD)	(mean)	(high energy blocks)
Watermark embedding parameters: $\alpha_1 = 0.1$ and $\alpha_2 = 0.1$.								
Lena	0.200	0.200	39.660	38.740	0.660	0.080	0.590	0.659
Lena	0.270	0.270	37.100	36.150	-0.050	0.100	0.590	0.660
Cameraman	0.270	0.270	35.120	34.500	0.300	0.090	0.540	0.610
Lake	0.270	0.270	34.050	33.390	0.340	0.100	0.575	0.637
Peppers	0.270	0.270	37.000	35.670	-0.300	0.090	0.600	0.696
Jetplane	0.270	0.270	35.400	34.600	0.140	0.100	0.560	0.642
Lena	0.300	0.300	36.130	35.240	-0.240	0.120	0.590	0.651
Cameraman	0.300	0.300	34.190	33.600	0.200	0.100	0.540	0.609
Lake	0.300	0.300	33.120	32.500	0.200	0.110	0.570	0.639
Peppers	0.300	0.300	36.000	34.770	-0.450	0.090	0.600	0.700
Jetplane	0.300	0.300	34.500	33.690	-0.010	0.100	0.560	0.635

4.3 Experimental results and generalized model

Table 4.1 and Table 4.2 enlist our experimental observations. We have used some benchmark gray level test images of size 512×512 available in uncompressed TIFF at [88]. We choose the watermark embedding parameters $\alpha_1 = \alpha_2 = 0.1$, and various values for the forgery parameters α_1' and α_2' such that the image quality remains acceptable. The quality of the forged image $\tilde{I}^{(i,\#)}$ is tested against the original image I and the watermarked copy $\tilde{I}^{(i)}$, using the perceptual quality parameters $Q^{(\#)}$ and $Q^{(i,\#)}$ respectively, represented in terms of PSNR in dB (see [9], p.112). $\mathrm{Cor}(s^{(i)}, s^{(i,\#)})$ is calculated as $\frac{\beta-\delta}{l}$ where β and δ represent the number of matches and mismatches between the corresponding bits of $s^{(i,\#)}$ and $s^{(i)}$ respectively, and l represents the total bit-length of the fingerprints. The last two columns illustrate the experimental values of ϵ, the bias in correct guess, on an average, as well as for the high energy blocks, which have more effect on the polarity reversal process of the energy difference.

Each row in Table 4.1 and Table 4.2 represents the mean and SD of the data for over 100 iterations of the forgery algorithms, with different random watermark fingerprint $s^{(i)}$ in each case. The image key π is calculated uniquely for each image, and then maintained over all the iterations with that image. The values $l = 64$, $\Delta = 100$, and $q = 5$ are kept fixed for all cases. In all experiments listed in Table 4.2, the additional parameters $r = 3$, $s = 3$ are chosen to perform the median filtering.

Discussion on Table 4.1: One may note that the guessing probability in each case is approximately 0.5, including that for the higher energy blocks. This implies that $\epsilon \approx 0$, which is in line with the relation derived in Eqn. (4.11). $\mathrm{Cor}(s^{(i)}, s^{(i,\#)})$ is quite significant in each case, and hence, the forgery can

easily be traced back to the attacker. This proves the robustness of MDEW against naive forgery attack based on random guess.

Discussion on Table 4.2: One may note that the probability of correct guess, $(1/2+\epsilon)$, is significantly greater than 0.5 in all the cases and the mean value of ϵ is approximately 0.07. It is high enough to assist the attacker in guessing whether the significant DCT coefficients of a block have been increased or decreased. The value of ϵ is even greater for the high energy blocks. High energy blocks contribute more significantly to create energy differences D' with a particular polarity. So if the attacker can guess those blocks correctly and apply forgery on the same, then the chances of reversing the polarity of D'' with respect to D' increases significantly. This, in turn, leads to significant decrease in the value of $\mathrm{Cor}(s^{(i)}, s^{(i,\#)})$, as evident from the data. The value of $\mathrm{Cor}(s^{(i)}, s^{(i,\#)})$ ranges close to 0 in most of the cases, thus making attacker-tracing very hard. Values of $Q^{(\#)}$ and $Q^{(i,\#)}$ are significantly greater than 30 dB in all cases, keeping the image quality satisfactory even after the forgery attack.

Generalized model: Consider the space of all possible watermark fingerprints $s^{(i)}$ to be S. The origin in space S may be defined as $s^{(0)} \equiv \overline{0}$, the zero vector, which represents the original image I. Suppose that there exists a definition of distance $d()$ between two fingerprints $s^{(i)}$ and $s^{(j)}$ in S, which, in case of MDEW, is the regular Hamming distance between vectors. Then, our generalized forgery model proposes that

> *If there exists a single-copy watermark removal method that reduces the distance $d(s^{(0)}, s^{(i)})$ from the knowledge of only the watermarked image $\tilde{I}^{(i)} \leftarrow W(I, s^{(i)})$, then the same technique can be amplified to mount a single-copy forgery attack that reduces the distance $d(s^{(j)}, s^{(i)})$, for any arbitrary j, using only the knowledge of $\tilde{I}^{(i)}$.*

This may be exploited against any correlation-based scheme, similar to the attack that we have proposed for MDEW. Only the details of forgery implementation have to be customized for each scheme, and every other principle of this attack will remain the same as our general approach. To the best of our knowledge, such a general scheme for extending a single-copy watermark removal method to a single-copy forgery attack on correlation-based watermarking schemes has not been proposed in the literature. It will be interesting to observe the ramifications of this attack on the new dirty-paper-based watermarking schemes [89, 90, 91, 92], if any at all.

4.4 Conclusion

In this chapter, we have described a general strategy that converts a single-copy watermark removal attack on any correlation-based scheme to a single-copy forgery attack on the same. We have taken the example of MDEW [1], one of the strongest correlation-based schemes, to mount our attack, and prove its effectiveness. The beauty of our attack model is that even a very weak single-copy watermark removal attack may be extended to obtain a strong single-copy forgery attack on correlation-based watermarking schemes. We have substantiated our model through attacks on MDEW, and complete theoretical analysis and experimental verification of the same. In the future, a similar strategy may possibly be exploited against other genres of watermarking schemes as well. In the next chapter we perform analysis of current state of CAS for IOD. We also propose an efficient IOD system by using another major technology as discussed in the first chapter i.e Selective Encryption.

Chapter 5

Efficient Image on Demand System

Digital Rights Management is a rapidly growing area of research that provides solutions towards several aspects of secure data communication [93, 94, 95, 96]. It includes system-level key exchange protocols, signal processing and encryption algorithms that make contents unusable for unauthorized parties. Some major applications designed with the help of DRM techniques are copyright protection, authentication and CAS.

In CAS, multimedia content can be shared following certain policies; a thumbnail or a low-resolution version of the content can be made available for free and the user has to pay in order to see the high quality content. One major CAS based system is Image On Demand, where a user browses a database of multimedia files in order to retrieve the content of interest. In a typical IOD scenario, a low-resolution image can be quickly downloaded from image databases in order to select the desired content, which can be purchased in a higher resolution version later. Figure 5.1 is a block dia-

gram representation of the general methodology adopted for any IOD based systems.

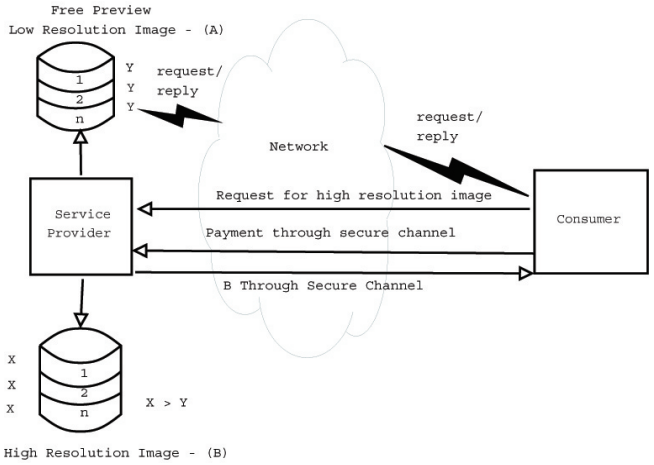


Figure 5.1: An outline of a typical IOD System

In this chapter, we present a novel scheme that can efficiently be adapted in such a scenario.

5.1 Introduction

Most of the existing conditional access based systems follow a standard methodology. The service provider shares two copies for a single information (specifically image for this work). One copy is a low-resolution version which is shared in the public domain for preview purpose. The other one is a high-resolution version to be provided to the customers through a secure channel on demand (after payment). We analyze the images in the DCT domain and note that polynomials of suitable degree, representing the sorted DCT coefficients together with original index locations, can uniquely represent an image. The DCT coefficients are sorted by its magnitude, which results into two set of data: (a) Sorted DCT coefficients and (b) An array which contains their original index locations. We show that the distribution of values (DCT

Index locations) in the generated array is significantly different for various images, and we exploit this to design an efficient CAS based scheme. The amount of private data, which a service provider needs to transmit through a secure channel to the customers on demand, is reduced significantly by our technique. This reduction in transmitted data makes the system apt for real-time secure applications.

Many websites with huge image databases are available today [97, 98, 99]. Most of these existing websites target a specific segment of customers who require very high-resolution images. They usually share a visible watermarked image of low quality for the purpose of preview and send the high-resolution version through a secure channel when paid for the same. The preview versions are generally freely downloadable and are acceptable for the purpose of recognizing the content.

One major technique being used to realize CAS based systems is selective encryption. Suitable portion and size of the actual data (image in this case) is scrambled in the process of selective encryption. It is performed in such a way that the image rendered from the rest of the 'in-the-clear portion' (i.e., the segment of the data that is not scrambled) is imperceptible to a significant fraction of the consumers [14]. In CAS like systems, one does not need to obscure the data completely to support rights management but make it such that the rendered data is indiscernible.

The majority of existing encryption standards such as DES and AES have been developed for independent and identically distributed $i.i.d$ data sources. However, multimedia data are typically non $i.i.d$, so applying encryption on the pixel domain is not at all feasible due to computational complexity, and its in-suitability for the real-time applications. But, transform domain is preffered [100, 101, 102] for applying selective encryption approach since we can exploit the fact that the data are represented as a sequence of approximately $i.i.d$ samples. This samples contribute unequally to the quality of

the reconstructed signal. So it is sufficient to target only a specific portion of the coefficients as well as provide advanced functionalities for conditional access [103, 104].

Motivation: Existing IOD schemes keeps at least tow copies of a particular image: one for preview purpose and the other is the high-resolution version which is sent separately through secure channel when customer pays for the same. This is one of the major drawback , since to follow this protocol, the amount of storage required is quite high. Another drawback is that, the huge amount of data in the form of high-resolution image needs to be sent through the secure channel. This increases the computational and communication overhead at real-time. In this chapter, we resolve the drawbacks mentioned above.

Real-time data transmission and computations should be minimized to the best possible extent to make the above mentioned system simple and efficient. At the same time, quality and security aspects should also be ascertained. Security aspects include data integrity, authentication etc. [105, 53, 106, 107]. Efficient and secure key management protocols are also necessary to exchange keys between service providers and users. Some of the risk aspects related to piracy are explained and solutions have been proposed through a two-period model in [94]. A novel privacy preserving content distribution mechanism for digital rights management without relying on the trusted third party assumption has been proposed in [96]. Authors have used some simple primitives such as blind decryption and one way hash chain to avoid the assumption of trusted third party. Delgado et al.in [93] proposes a modular architecture which provides digital rights and privacy policies management features. It can be integrated by invoking some web service calls, depending on which services are needed. Several similar protocols and scheme exist, such as those described in [95, 108, 109].

Result: In this chapter we propose a scheme for image on demand in which

we store only single copy of the data to represent an image in the database. It leads to significant reduction in the storage requirement. Figure 5.2 gives a broad overview of the proposed IOD based system. An image is transformed

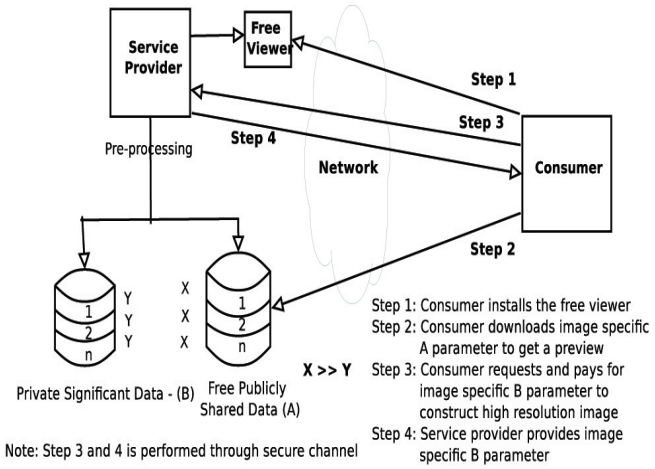


Figure 5.2: Proposed IOD system

into the DCT domain. After a certain preprocessing methodology (explained in Section 5.3) we divide the transformed data of each image into two subsets namely private significant data and free publicly shared data. We construct a low quality version from one subset (free publicly shared data subset) and keep the other subset (private significant data subset) private. The low quality version is sufficient to preview but is not usable in any sense to any group of customers. We provide the private significant data subset to construct a high-resolution version only when the customer demands and pays for the same. The private significant data subset of an image which is kept secret, constitutes of an optimal fraction of the total data required to represent a single image and the remaining data related to the image is publicly downloadable for preview purpose. In general the size of private significant data subset is significantly less than the free publicly shared data subset for any specific image (explained in Section 5.5.1). So the amount of data required to be sent through the secure channel in real-time is significantly less than most of the existing schemes. One time installation of free image viewer

application is required at the customer end which is inline with the already existing similar kind of service providers. We focus here on gray level images while the scheme can be generalized for colour images and video streams.

An image I, in the DCT domain can be efficiently represented by a set of polynomials of suitable degree together with the corresponding index location matrix Π_{I_d} [12, 13]. In this work we show that Π_{I_d} is the most significant attribute and can be used as a unique descriptor for any image while on the other hand the polynomials that approximate the actual DCT coefficients, as such have less significance. We utilize Π_{I_d} to develop a new IOD system. We would also like to claim that to the best of our knowledge that there is no existing work which utilizes Π_{I_d} for designing any application.

Organization of the chapter: A brief survey of existing selective encryption techniques which could possibly be used for various commercial applications is given in Section 5.2. We present the methodology in Section 5.3. Detailed description of the proposed IOD scheme is given in Section 5.4. Experimental results, interpretations, analysis of efficiency and robustness of our scheme are given in Section 5.5 followed by conclusion in Section 5.7.

5.2 Existing Selective Encryption Schemes

Selective encryption is a technique to save computational complexity or enable interesting new system functionality by only encrypting a portion of a compressed bitstream while still achieving adequate security. Although suggested in a number of specific cases, selective encryption could be much more widely used in consumer electronic applications ranging from mobile multimedia terminals through digital cameras. Some of the schemes based on the concept are presented next.

Two efficient approaches to conceal Regions Of Interest (ROIs) based

on transform-domain or code-stream-domain scrambling have been proposed in [110]. In the first technique, the sign of selected transform coefficients is pseudo-randomly flipped during encoding. In the second method, some bits of the code-stream are pseudo-randomly inverted. An index-based selective audio encryption scheme for Wireless Multimedia Sensor Networks (WMSNs) is presented in [111]. It protects data transmissions by incorporating both resource allocation and selective encryption based on Modified DCT (MDCT). In this proposed scheme, the audio data importance is leveraged using the MDCT audio index, and wireless audio data transmission proceeds with energy efficient selective encryption.

A partial encryption scheme in wavelet domain based on secure encryption principles with respect to the existing attacks (cryptographic attack, replacement attack and statistical model based attack) is proposed in [112]. Schemes have been proposed in [113] to optimize the energy, distortion, and encryption performance of video streaming in WSNs. Two significant contributions have been claimed. First, a channel-aware selective encryption approach is proposed to minimize the extra encryption dependency overhead at the application layer. Second, an Unequal Error Protection (UEP)-based network resource allocation scheme is proposed to improve the communication efficiency at the lower layers. An integrated approach of fingerprinting and encryption is proposed in [114] where keys of different receivers helps in the fingerprinting aspects. A joint encryption and compression framework based on selective bit scrambling, block shuffling and block rotation of the transform coefficients and motion vectors of video is proposed in [102].

A fine-grained access control mechanism based on selective encryption is proposed in [115]. Using this approach, the owner of a file specifies access control policies over various byte ranges in the file. The separate byte ranges are then encrypted and signed with different keys. Users of the file only receive the encryption keys for the ranges they are authorized to read and signing

keys for the ranges they are authorized to write. An approach to reduce the computational cost of multimedia encryption while also preserving the properties of compressed video is presented in [116]. A hardware-amenable design of the proposed algorithms makes them suitable for real-time embedded multimedia systems. This approach alleviates the need for additional hardware for encryption in resource-constrained scenarios and can be otherwise used to augment existing encryption methods used for content delivery on the internet or in other applications.

A novel method allowing the protection of the newly emerging video codec HEVC (High Efficiency Video Coding) is presented in [117]. Visual protection is achieved through the selective encryption of HEVC-CABAC binstrings in a format compliant manner. To protect the privacy in the CCTV video, an encryption scheme for region of interest of H.264 video based on flexible macroblock ordering and chaos is proposed in [118]. The proposed scheme can effectively protect the private information of H.264 video and, therefore, can strike a good balance among the security, encryption efficiency, and coding performance.

Cryptanalysis of various discrete orthogonal transforms have been carried out in [100]. They have also proposed a DCT-based scheme which significantly improves the security of the scrambler. A design which selectively encrypts the fixed-length codewords of MPEG-video bit streams is proposed in [119]. Strict size-preservation, on-the-fly encryption and multiple perceptibility are the features supported in this design.

Before proceeding further, let us now describe our methodology in detail.

5.3 Our Methodology

5.3.1 Polynomial representation of an image

Any digital image I can be uniquely represented by a set of polynomial equations P_i's and the corresponding permutation of actual index locations Π_{I_d} of the DCT transformed image I_d. Details of the representation scheme are given next.

Step 1: Image Representation

- A given digital image I can be interpreted as a 2-dimensional matrix in spatial domain.
- Let N and M be the width and height of I.
- We perform $N \times M$ DCT transform on I to form I_d also of size $N \times M$. This is given as

$$I_d(k_1, k_2) = \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} x_{n,m} \cos\left[\frac{\pi}{M}(m + \frac{1}{2})k_2\right] \cdot \cos\left[\frac{\pi}{N}(n + \frac{1}{2})k_1\right]$$

$$I_d \;:=\; DCT_{N\times M}[I]$$

- Scan I_d in zig-zag manner (similar to the one used in baseline JPEG compression technique [7]) and store the resultant array as Z_{I_d} also of length $N \times M$.

$$Z_{I_d} \;:=\; SCAN_{zig-zag}[I_d]$$

- Now sort the DCT coefficients of Z_{I_d} in descending order and store in an array A_{I_d}.
- Simultaneously store the initial index locations corresponding to each DCT coefficient of A_{I_d} in an array Π_{I_d}.

$$\begin{aligned} A_{I_d} &:= SORT_{(Desc.)}[Z_{I_d}[i]; 1 \leq i \leq N \times M] \\ \Pi_{I_d} &:= [\Pi_{I_d}(i) : A_{I_d}[\Pi_{I_d}(i)] = Z_{I_d}[i]] \end{aligned}$$

Π_{I_d} will be required during recovery of the image.

Step 2: Polynomial Approximation

- Now, partition the values of A_{I_d} contiguously in q different parts$A_{I_{d_1}}$, $A_{I_{d_2}}, \ldots, A_{I_{d_q}}$ leaving aside the DC value. Note that each of $A_{I_{d_1}}$, $A_{I_{d_2}}, \ldots, A_{I_{d_q}}$ is also a sorted array.

$$A_{I_{d_1}} = [A_{I_d}[j] : 2 \leq j \leq \frac{NM}{q}]$$

  j starts from 2 for $A_{I_{d_1}}$ since DC value i.e. $A_{I_d}[1]$ is not included for polynomial approximation process.

- For $2 \leq i \leq q$:

$$A_{I_{d_i}} = [A_{I_d}[j] : (i-1)\frac{NM}{q} + 1 \leq j \leq i\ \frac{NM}{q}]$$

  $A_{I_{d_1}}, A_{I_{d_2}}, \ldots, A_{I_{d_q}}$ are also sorted arrays.

- Now corresponding to each $A_{I_{d_i}}$, we fit a polynomial of degree θ_i, such that the Mean Square Error (MSE) is minimized. It is clear that as we increase the degree θ_i of the polynomial, the mean square error is less. However, since the data in $A_{I_{d_i}}$'s are monotonically decreasing,

very good approximation can be obtained by using polynomials with moderate degrees. Thus, we get a series of polynomials $P_1, P_2, \ldots, P_q$ approximating the DCT coefficient matrix I_d. Apart from the polynomials, we also have the DC value $\eta = I_d[1,1]$ which is kept intact.

$$P_i \;=\; Poly_{\theta_i}(A_{I_{d_i}}) \;,\; \forall\; 1 \leq i \leq q;\; deg(P_i) = \theta_i$$

$Poly_{\theta_i}$ is used to denote approximation by a polynomial of degree θ_i. We keep the values of θ_i's constant for all i and call it θ. The MSE $\phi(I^P, I)$ of any image I^P (approximation of I in this case) with respect to another image I is calculated by (5.1).

$$\phi(I^P, I) = \frac{1}{NM} \sum_{u=1}^{N} \sum_{v=1}^{M} [I^P(u,v) - I(u,v)]^2 \tag{5.1}$$

Step 3: Image Reconstruction through Polynomials

- To reconstruct an approximated image I' of size $N \times M$, we first extract data from the corresponding P_i's (DCT polynomials).

$$\begin{aligned} A'_{I_{d_1}} &= [P_1(k); \quad 1 \leq k \leq \frac{NM}{q} - 1], \\ A'_{I_{d_i}} &= [P_i(k); \quad 1 \leq k \leq \frac{NM}{q}], \text{ for } 2 \leq i \leq q. \end{aligned}$$

  The size of first segment is $\frac{NM}{q} - 1$ instead of $\frac{NM}{q}$ since DC coefficient is not included.

- Then we place them back into their proper locations in the DCT matrix

using the index matrix $\Pi_{I_d}[i]$ to get $Z'_{I_d}[i]$.

$$\begin{aligned} A'_{I_d} &= \{\eta\} \bigcup_{i=1}^{q} A'_{I_{d_i}} \\ Z'_{I_d} &:= [A'_{I_d}[\Pi_{I_d}(k)] : 1 \leq k \leq NM] \end{aligned}$$

Above step actually places the DCT coefficient back to their original locations where it was present before sorting.

- Now we perform inverse zig-zag scan on Z'_{I_d} to get I'_d.

$$I'_d := SCAN_{inv-zig-zag}[Z'_{I_d}]$$

- Finally $N \times M$ Inverse DCT (IDCT) is applied to get an image I' of size $N \times M$.

$$I' := IDCT(I'_d)$$

For example, if we take $q = 16$ for a 256×256 gray level image of Lena and approximate each $A_{I_{d_i}}$ by a polynomial P_i of degree $\theta = 15$ then Figure 5.3(b) is the resultant image of Lena which is visually indistinguishable and has PSNR value as high as 55 dB w.r.t. the original Lena image.

5.3.2 Significance of Π_{I_d}

A_{I_d} follows a generic pattern and may be considered almost similar for most images. Even if A_{I_d} is completely known then also it is computationally infeasible to recover the corresponding I' without the knowledge of Π_{I_d}.

The above statement is justified by certain experimental analysis whose

details are given below.

- Let $I,\ J$ be two distinct images. Let A'_{I_d} be the set of DCT coefficients of I which have been approximated by polynomials of suitable degree. We know that along with A'_{I_d}, we require the set of DCT index locations Π_{I_d} to reconstruct the image I' which is visually close to I. Suppose we attempt to perform the reconstruction using A'_{I_d} and the DCT index locations of the other image J i.e. Π_{J_d}, and obtain the reconstructed image I''. Then it has been observed that I'' is visually almost same as J instead of I.
- Figure 5.3(a) shows the curve corresponding to A_{I_d} of Lena (DC value has been discarded for better visual). Figure 5.3(c) is the resultant I'' by using the A_{I_d} of Lena (I) and Π_{J_d} of Peppers (J).
- Similarly Figure 5.3(d) and Figure 5.3(e) are recovered by using A_{I_d} of Lena and Π_{J_d} of mandrill and jetplane image respectively.

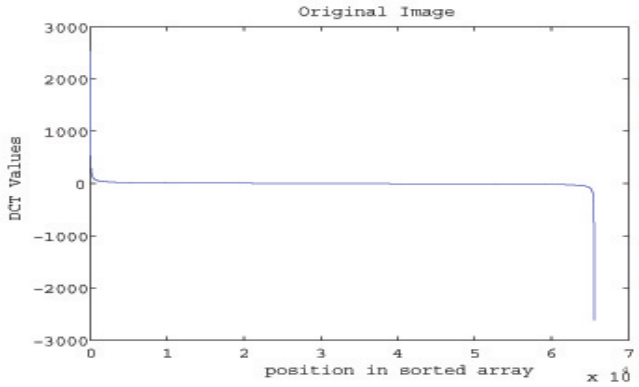
The above analysis proves that Π_{I_d} is the most important information required for proper recovery of I'.

On the basis of the methodology described above we utilize the uniqueness property of Π_{I_d} and propose a new IOD scheme described in detail in the next section.

5.4 Proposed Scheme

The methodology developed in Section 5.3 can be suitably adapted for any CAS based application, but we will explain the overall scheme in context of a new IOD system. In the proposed IOD system given an image I,

- A specific subset of Π_{I_d} known as $\Pi^{\$}_{I_d}$ is kept secret by the service



(a) A_{I_d} dataset

(b) Recovered Image

(c) Image 1

(d) Image 2

(e) Image 3

Figure 5.3: Sorted DCT coefficient (A_{I_d}) dataset of Lena (q number of partitions of A_{I_d}); Recovered image I'' using A_{I_d} corresponding to Lena and DCT index location dataset (Π_{I_d}) of Lena; Π_{J_d} of Peppers image as J; Π_{J_d} of Mandrill image as J; Π_{J_d} of Jetplane image as J respectively.

provider.

- The service provider constructs a low quality image $I^{\$}$ by using $\Pi_{I_d} \backslash \Pi^{\$}_{I_d}$ and set of coefficients $A'_{I_{d_1}}, A'_{I_{d_2}}, \ldots, A'_{I_{d_q}}$.
- $I^{\$}$ is shared in the public domain to lure customers. The finer details $\Pi^{\$}_{I_d}$ needed to construct the corresponding high quality image I^* is sent only when the customer demands and pays for it.

A general overview of the scheme is shown in Figure 5.4. Major steps involved

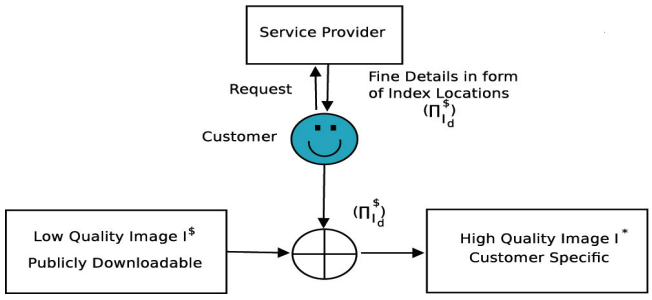


Figure 5.4: Overview of proposed Image on Demand System

in the design of the proposed IOD system is described next.

5.4.1 Major steps in design of proposed IOD system

1. Calculate a set of minimum K number of segments S_i from Π_{I_d} and accumulate and store it in an array $\Pi^*_{I_d}$, which makes $\Pi^*_{I_d}$ a subset of Π_{I_d}. S_i is defined as an array which consists of $\frac{B}{2}$ number of contiguous index locations picked from the beginning and $\frac{B}{2}$ number of contiguous index locations picked from the end side of Π_{I_d} and stored from the beginning towards end in sequential manner as shown in Figure 5.5 (details given in Algorithm 3). K and B are numerical values related to actual experiments. We call this process as **Calculation of** $\Pi^*_{I_d}$.

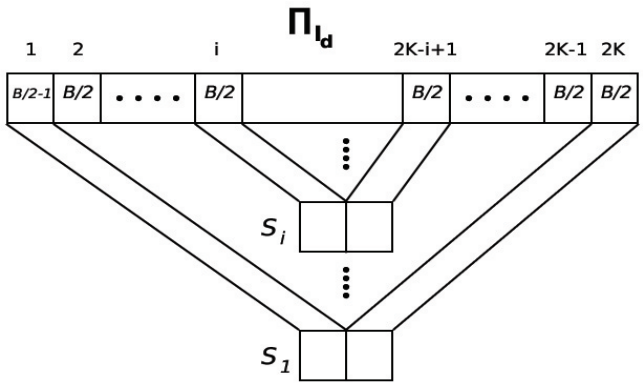


Figure 5.5: Construction of Segment S_i

2. From the K number of segments already defined in $\Pi^*_{I_d}$ we identify a specific segment S_i and store it in an array $\Pi^{\#}_{I_d}$. We call this process as a **Broad Search** operation.

3. Again find a minimum possible subset of index locations from $\Pi^{\#}_{I_d}$ and store it in an array $\Pi^{\$}_{I_d}$. We call this process as a **Narrow Search** operation.

4. The DC value η and $A_{I_{d_1}}, A_{I_{d_2}}, \ldots, A_{I_{d_q}}$ information of I in the form of $P_1, P_2, \ldots, P_q$ polynomials of degree θ and $\Pi^*_{I_d} \setminus \Pi^{\$}_{I_d}$ set of index locations are declared in public so that $I^{\$}$ could be constructed for preview purpose.

5. $\Pi^{\$}_{I_d}$ constitutes the secret data which is supplied to the customer on demand to construct the corresponding high quality image I^*.

PSNR $Q(I^P, I)$ of any image I^P with respect to another image I is calculated by

$$Q(I^P, I) = 10 \cdot \log_{10} \frac{MAX_I^2}{MSE} \tag{5.2}$$

where MAX_I represents the maximum possible pixel value of the image. When the pixels are represented using 8 bits per pixel, this is 255.

Let us assume that I to be an $i.i.d$ information source which generates a random sequence of symbols from a finite set of possible gray level values $g_1, \ldots, g_n$ and n represents the span of gray level [120]. For example, in case of a 8-bit gray level image $n = 256$ and $g_i = 0, 1, \ldots, 255$. The probability of the event that the source will produce symbol g_i is $p_I(g_i)$. $p_I(g_i)$ is calculated as

$$p_I(g_i) = \frac{\#\ of\ pixels\ having\ value\ g_i\ in\ I}{N \times M}$$

and $\sum_{i=0}^{255} p_I(g_i) = 1$ then the entropy of an image I tells the amount of information contained in that and is given by

$$H(I) = -\sum_{i=0}^{n} p_I(g_i) \log_2 p_I(g_i) \tag{5.3}$$

Details of Step 1, 2 and 3 are given next.

Step 1: Calculation of $\Pi^*_{I_d}$ Let us first calculate and identify $\Pi^*_{I_d}$ required for constructing a high quality image I^* (for example, PSNR around 40 dB with respect to I).

To calculate $\Pi^*_{I_d}$ we chose a threshold Q_T for $Q(I^*, I)$, where $Q(I^*, I)$ is the PSNR of I^* w.r.t. I. Then we find out the minimum K number of S_i's from Π_{I_d} which are required to construct I^* such that $Q(I^*, I) \geq Q_T$. Accumulate and store $S_1, S_2, \ldots, S_K$ in $\Pi^*_{I_d}$. The detailed algorithm to calculate $\Pi^*_{I_d}$ is described in Algorithm 3.

Details of the notations and abbreviations used in the subsequent algorithms.

Algorithm 3 Calculation of $\Pi^*_{I_d}$

1: Perform step 1, 2 and first operation of step 3.
2: Choose a sufficient size B of a specific S_i of $\Pi_{I_d} : (N \times M) \mod B = 0$. $\#(B\text{-sized } S_i) = \frac{NM}{B}$.
3: D = 0.
4: **while** $Q(I^*, I) < Q_T$ **do**
5: $D = D + 1$.
6: $\Pi^*_{I_d} \leftarrow Zeros(BD, 1)$
7: **for** $i = 1$ to $\frac{BD}{2}$ **do**
8: $\Pi^*_{I_d}[i] = \Pi_{I_d}[i]$.
9: **end for**
10: $k = \frac{BD}{2}$.
11: $r = (NM) - k$.
12: **for** $i = 1$ to $\frac{BD}{2}$ **do**
13: $\Pi^*_{I_d}[k + i] = \Pi_{I_d}[r + i]$.
14: **end for**
15: $V \leftarrow Zeros(NM, 1)$
16: **for** $j = 1$ to $\frac{BD}{2}$ **do**
17: $V[\Pi^*_{I_d}[j]] = A'_{I_d}[j]$
18: **end for**
19: $p = 1$.
20: **for** $j = \frac{BD}{2} + 1$ to BD **do**
21: $V[\Pi^*_{I_d}[j]] = A'_{I_d}[r + p]$
22: $p = p + 1$.
23: **end for**
24: $I^* := IDCT_{N\times M}\ (SCAN_{inv-zig-zag}(V))$
25: Calculate PSNR $Q(I^*, I)$ of I^* w.r.t I.
26: **end while**
27: $\Pi^*_{I_d}$ is the set of required minimum number of index locations corresponding to I^*. D is the required K.

- $Zeros(x, y)$: Initialization of an array of size $x \times y$ with all zero values.
- $SCAN_{inv-zig-zag}()$: Scan the array in inverse zig-zag manner.
- $SORT_{(Asc.)}()$: Sort the array in ascending order.
- $SORT_{(Desc.)}()$: Sort the array in descending order.
- $CORR(X, Y)$: Correlation between random variables X and Y.
- $mean()$: Average or mean of the input array.

$\Pi^*_{I_d}$ is the subset of minimum size identified from Π_{I_d} i.e. required to construct a high quality image I^* whose PSNR $Q(I^*, I)$ is greater than a particular threshold value Q_T. The reason behind taking half of the coefficients from beginning and half from the end is that A'_{I_d} contains the high magnitude coefficients but with negative sign towards the end of the array.

Step 2: Broad Search In this we identify a specific segment S_i and store it in an array $\Pi^\#_{I_d}$. This $\Pi^\#_{I_d}$ should be such that if the image $I^\#$ constructed from $\Pi^*_{I_d} \setminus \Pi^\#_{I_d}$ number of index locations should have the lowest entropy $H(I^\#)$ using (5.3) and maximum MSE $\phi(I^\#, I)$. $I^\#$ is constructed from $\Pi^*_{I_d} \setminus \Pi^\#_{I_d}$ number of index locations assuming that V is available, where V is the specific subset of A'_{I_d} corresponding to $\Pi^*_{I_d}$ index locations. Detailed description of broad search is given in Algorithm 4.

Figures 5.6a and 5.6b shows the variation of $H(I^\#)$ and $\phi(I^\#, I)$ of $I^\#$ with respect to different index location segments of size B (except for the first segment where size is $B - 1$). Mostly the images are of low frequency nature and since the DCT coefficients are sorted in descending order, so the resultant curves will be of similar pattern for most of the images. It has also been verified through experiments. Curves shown in Figures 5.6a and 5.6b correspond specifically for Lena image. First segment will always be the best choice for $\Pi^\#_{I_d}$ since A'_{I_d} is in sorted form. In almost all of the cases, the segment corresponding to first entry of sorted E and F will be same. If not

same then first segment of E will be selected for $\Pi^{\#}_{I_d}$. E and F contains the $H(I^{\#})$ and $\phi(I^{\#}, I)$ of the $I^{\#}$ constructed from step 11 of Algorithm 4 in ascending and descending order respectively.

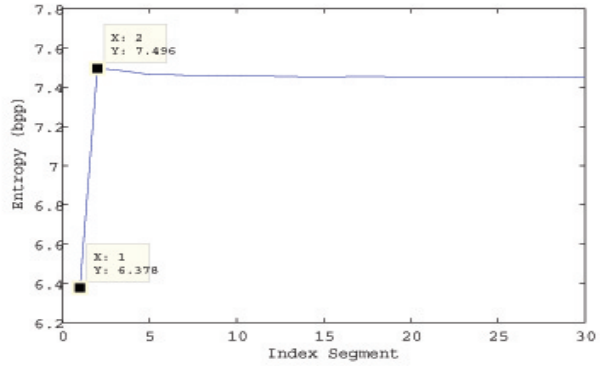
Algorithm 4 Broad Search

1: **for** $j = 0$ to $K - 1$ **do**
2: **for** $r = 1$ to $\frac{B}{2}$ **do**
3: **if not** ($j = 0$ **and** $r = 1$) **then**
4: $V[\Pi_{I_d}[j\frac{B}{2} + r]] = 0$.
5: **end if**
6: **end for**
7: $p = (KB) - \frac{B(j+1)}{2}$.
8: **for** $r = 1$ to $\frac{B}{2}$ **do**
9: $V[\Pi_{I_d}[p + r]] = 0$
10: **end for**
11: $I^{\#} := IDCT_{(N\times M)}(SCAN_{inv-zig-zag}(V))$
12: Calculate entropy $H(I^{\#})$ using (5.3) and store it in an array E.
13: Calculate $\phi(I^{\#}, I)$ using (5.1) and store it in an array F
14: **end for**
15: $E \leftarrow SORT_{(Asc.)}(E)$. $F \leftarrow SORT_{(Desc.)}(F)$
16: Select the segment of Π_{I_d} corresponding to the first entry of the sorted E and F as $\Pi^{\#}_{I_d}$ if the corresponding segment is same. Else pick the one with the first entry of E.

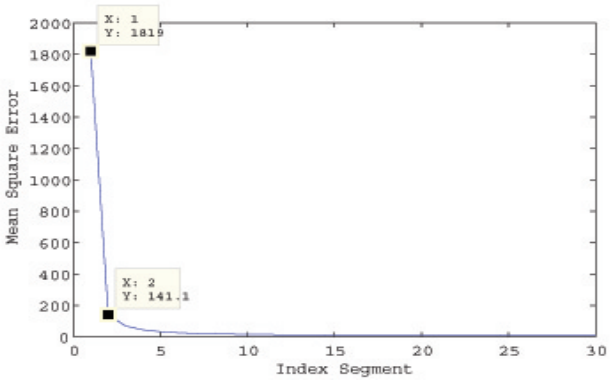
Step 3: Narrow Search Once $\Pi^{\#}_{I_d}$ is identified for an I, we go one more step further to find and narrow it down to an optimal subset of index locations $\Pi^{\$}_{I_d}$ such that the following conditions could be satisfied.

- Correlation ν between $\Pi^{\$}_{I_d}$'s of the various test images should be significantly low. ν between any two dataset $\Pi^{\$}_{I^1_d}$ and $\Pi^{\$}_{I^2_d}$ is calculated as

$$\nu = \frac{\sum_{i=1}^{\tau}(\Pi^{\$}_{I^1_d}(i) - \overline{\Pi^{\$}_{I^1_d}})(\Pi^{\$}_{I^2_d}(i) - \overline{\Pi^{\$}_{I^2_d}})}{\sqrt{\sum_{i=1}^{\tau}(\Pi^{\$}_{I^1_d}(i) - \overline{\Pi^{\$}_{I^1_d}})^2 \sum_{i=1}^{\tau}(\Pi^{\$}_{I^2_d}(i) - \overline{\Pi^{\$}_{I^2_d}})^2}} \tag{5.4}$$



(a) Entropy Variation



(b) Mean Square Error Variation

Figure 5.6: Graphs: Variation of $H(I^{\#})$) and $\phi(I^{\#}, I)$ with respect to different index location segments of size B

Here τ represents the size of $\Pi^{\$}_{I_d}$. $\overline{\Pi^{\$}_{I_d^1}}$, $\overline{\Pi^{\$}_{I_d^2}}$ are the means of $\Pi^{\$}_{I_d^1}$ and $\Pi^{\$}_{I_d^2}$ respectively.

- Corresponding PSNR $Q(I^{\$}, I)$ of $I^{\$}$ w.r.t. I suffices for preview purpose, where $I^{\$}$ is constructed from $\Pi^{*}_{I_d} \setminus \Pi^{\$}_{I_d}$ number of index locations.
- The size τ of $\Pi^{\$}_{I_d}$ is sufficient enough to resist cryptanalytic attacks by exhaustive search.
- $H(I^{\$})$ is sufficiently low.

Algorithm 5 describes the pseudo-code to find out a set of mean correlation data $\Omega(y)$. $\Omega(y)$ represents the mean of ν's being calculated over all possible combination of test images for a specific data size corresponding to the value of y, where $1 \leq y \leq 128$. Size of the resultant $\Pi^{\$}_{I_d}$ is given by $\tau = 2y - 1$.

Figure 5.7a shows the variation of Ω with respect to y by performing Algorithm 5 on various test images. Similarly Figure 5.7b and Figure 5.7c show the variation of $H(I^{\$})$ and $Q(I^{\$}, I)$ respectively.

On the basis of Figures 5.7a, 5.7b, 5.7c and considering the conditions to be satisfied by $\Pi^{\$}_{I_d}$ the minimum possible value of τ and corresponding $\Pi^{\$}_{I_d}$ is finalized.

Now if a customer is interested in the high quality version of $I^{\$}$ and pays for the same then the service provider may provide $\Pi^{\$}_{I_d}$ to the customer so that I^* which is a high quality version of $I^{\$}$ can be constructed at the customer end.

Next we describe the various results which have been achieved through the experiments performed and give the analysis of the efficiency and robustness of the system against possible attack scenario.

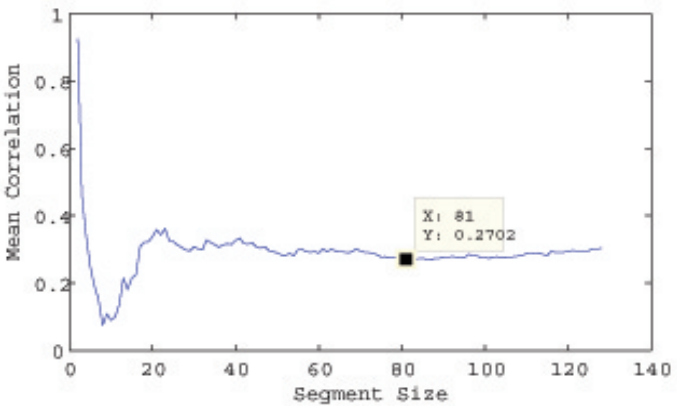
Algorithm 5 Calculation of $\Omega(y)$

Let T number of test images be used.
$y = 1$.
for $j = 2 : 2 : B$ **do**
  for $p = 1$ to T **do**
    if $j \neq 2$ **then**
      for $i = 1$ to $\frac{j}{2} - 1$ **do**
        $\Pi^{\$}_{I_{d_p}}[i] = \Pi^{\#}_{I_{d_p}}[i]$.
      end for
    end if
    $temp = \frac{j}{2} - 1$
    $h = 1$.
    for $i = \frac{j}{2} : -1 : 1$ **do**
      $\Pi^{\$}_{I_{d_p}}[temp + h] = \Pi^{\#}_{I_{d_p}}[B - i]$.
      $h = h + 1$.
    end for
  end for
  for $s = 1$ to $\binom{T}{2}$ **do**
    Calculate $\nu[s] = \text{CORR}(\Pi^{\$}_{I_{d_e}}, \Pi^{\$}_{I_{d_f}})$: $1 \leq e \neq f \leq T$.
  end for
  Calculate $\Omega(y) = \text{mean}(\nu)$.
  $y = y + 1$.
end for

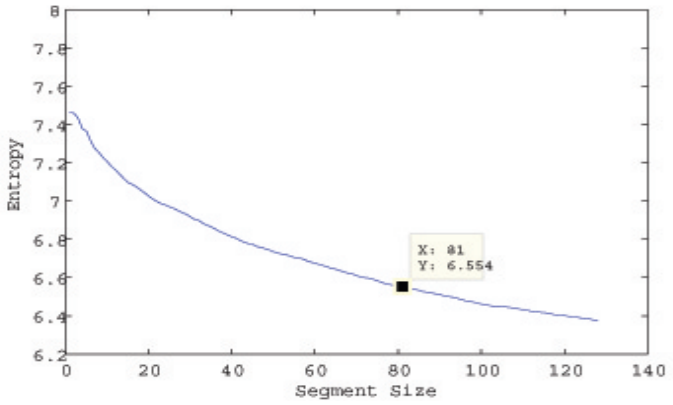
5.5 Experimental Results, System's Efficiency and Robustness Analysis

We conducted experiments on a number of standard gray level test images of size 256×256 available in uncompressed TIFF at [88] to prove the suitability of proposed scheme for IOD system on the basis of the methodology developed. **Experimental Results and Observations:** As stated earlier,

the low frequency images in general depict similar pattern of curves as shown in Figure 5.6a and 5.6b. Figures also show that if the segment indexed 1 is removed from A_{I_d} then the corresponding entropy $H(I^{\#})$ of $I^{\#}$ is the lowest as well as the corresponding MSE $\phi(I^{\#}, I)$ will be maximum. Therefore this segment is chosen during **Broad Search** for removal. Size of $\Pi^{\#}_{I_d}$ will be 255 since we don't consider DC whose location will always be $\Pi_{I_d}[1]$.

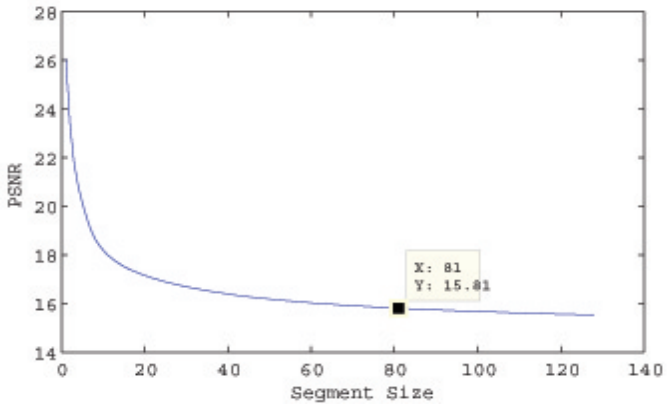


(a) Ω Variation



(b) Entropy Variation

Figure 5.7



(c) PSNR $Q(I^{\$}, I)$ Variation

Figure 5.6: Graphs: Variation of ν, $H(I^{\$})$ and $Q(I^{\$}, I)$ of $I^{\$}$ w.r.t τ

By analyzing Figures 5.7a, 5.7b, 5.7c and considering the conditions to be satisfied by $\Pi^{\$}_{I_d}$ as previously mentioned in **Step 3: Narrow Search** in Section 5.4, the optimal value of τ comes out to be 161 (this corresponds to $y = 81$). For $y = 81$ the value of Ω is 0.27 which is significantly low. Size of $\Pi^{\$}_{I_d}$ i.e. τ should also be not low enough which could be approximated by an adversary. So with respect to this condition also $y = 81$ is an apt value since trying out 161! number of trials is significantly complex enough from an adversary's point of view. Table 5.1 shows the correlation between $\Pi^{\$}_{I_d}$ segment of various test images for $y = 81$.

	Lena	Jetplane	Mandrill	Peppers	House	Tree	Elaine	Clock
Lena	1	0.29	0.18	0.16	0.15	0.24	0.30	0.28
Jetplane	0.29	1	0.26	0.40	0.29	0.31	0.30	0.36
Mandrill	0.18	0.26	1	0.31	0.13	0.31	0.17	0.24
Peppers	0.16	0.40	0.31	1	0.28	0.22	0.31	0.25
House	0.15	0.29	0.13	0.28	1	0.23	0.34	0.16
Tree	0.24	0.31	0.31	0.22	0.23	1	0.31	0.21
Elaine	0.30	0.30	0.17	0.31	0.34	0.31	1	0.40
Clock	0.28	0.36	0.24	0.25	0.16	0.21	0.40	1

Table 5.1: Correlation between $\Pi^{\$}_{I_d}$ segment of various test images for $y = 81$

Figure 5.7(b) is the preview version of I with PSNR value of around 15

dB with respect to I. Figure 5.7(c) is the resultant attacked image $\tilde{I}$ when an adversary tries to recover I^* by adding $\Pi^{\$}_{J_d}$ of another image J. In this case I corresponds to lena and J corresponds to peppers image.

(a) Desired image

(b) Shared image

(c) Attacked image

Figure 5.7: Images:Desired image (I^*); Shared image ($I^{\$}$); Attacked image $\tilde{I}$

Interpretation:

- $\Pi^{\$}_{I_d}$ represents the optimal segment of index locations which has very low ν with respect to the same attribute of another images.
- So I can not be approximated even by $\Pi^{\$}_{J_d}$ of any J or by any random $\Pi^{\$}_{I_d}$.
- It also signifies that $A_{I_d}[\Pi^{\$}_{I_d}]$ represents the minimal segment of coefficients which if kept hidden leads to a maximum degradation in visual quality of $I^{\$}$.
- $\Pi^{\$}_{I_d}$ also represents the minimal segment of index locations which if received by a customer in image on demand system will lead to a construction of high quality image similar to I^*.

- A_{I_d} corresponding to any image has negligible significance.
- Figure 5.7(c) resembles more closely to J instead of I with fair enough perception of I as well. So we can conclude that an adversary can not recover a good I^* corresponding to I by adding the $\Pi^{\$}_{J_d}$ of any J on the publicly available $I^{\$}$.

5.5.1 System's efficiency

The scheme proposed manages that the amount of data to be transmitted through secure channel is kept as low as possible. Exact details of the amount of data which is publicly available in the form of image database and the amount of data which is kept secret by considering a 256×256 gray level images is shown below.

1. Since each coefficient of the polynomials P_i have been represented by using 16 bytes, the size of Polynomial Representation Set (ρ) shared in public domain (OFF-LINE) is calculated as $\rho = q \times (\theta_i + 1) \times 16 + 2$ bytes, where the 2 extra bytes is for the DC value.
2. The size of Initial index locations (χ) also shared in public domain (OFF-LINE) is calculated as $\chi = B \times K \times 2 - \tau \times 2$ bytes.
3. The size of on demand data (ψ) which is transmitted only when demanded (REAL-TIME) consists of the finer details in the form of $\Pi^{\$}_{I_d}$ and is given by $\psi = \tau \times 2$ bytes. This is the data that is communicated through a secure channel on demand.

For example, Figure 5.7(a) represents I^* where $Q_T = 40$ dB, $q = 16$, $\theta = 15$, $B = 256$ and the corresponding value of K from Algorithm 3 is 121. So the overall data transmission required is given by

- ρ (Constant for same set of q and θ) is 4098 bytes.

- χ is 61630 bytes.
- ψ is 322 bytes.
- Total transmission (η), where $\eta = \rho + \chi + \psi$ comes out to be 66050 bytes.

From the above analysis we may conclude the following.

1. Publicly available data comprises of $\rho + \chi$ which in the given case comes out to be 65728 bytes and the secret data ψ merely consists of 322 bytes. So real-time transmission of secret data through secure channel hardly consists of 0.0048 (less than 0.5 %) of η. This feature makes the proposed system efficient in real-time.
2. Since ψ is negligible, the amount of secure communication is very low, which is advantageous due to less computational and communication overheads.
3. Only $\frac{66050-65536}{65536} = 0.78\%$ of the actual image size (for the given case image size is of 65536 bytes) is the only extra data required for storing the complete data for a single image. This is significantly much less when compared to the existing schemes where one preview copy and one actual high-resolution copy of the image is simultaneously stored in the image database.

5.5.2 Robustness Analysis

For an adversary the main challenge to attack the proposed scheme are:

1. To find out the exact reverse permutation of $\Pi^{\$}_{I_d}$ whose size is τ in a possible space of $Z = N \times M - \frac{\chi}{2} - 1$.
2. To find out the sign's of the DCT coefficients for the corresponding

reverse permutation.

With respect to the given values an adversary needs to try at-least $\binom{Z}{\tau} \times \tau! \times 2^{\tau}$ number of trials to get one instance of $\tilde{I}$ equivalent to I^*. So if all other values remains same then $Z = 34720$ and $\tau = 161$. Accordingly the number of trials comes out to be $\frac{34720!}{34559!} \times 2^{161}$, which is a huge number and will require a very strong computational resource for the same.

5.6 Possible application in Image/Video Encryption

Another very useful and efficient application that can be designed by the similar approach as discussed in this chapter could be to apply it for image/video encryption. More specifically for JPEG/MPEG standards since they work on the DCT domain. But as of now in the standard encoder structure of JPEG/MPEG, they compulsorily work on 8×8 DCT blocks. Applying the similar kind of scheme in 8×8 DCT block is although feasible, but it will result into a complex system with lot of computations as well as there will be significant increase in the storage requirement as well. If the DCT based image/video standard could be defined for a global DCT block size as being adopted in the proposed scheme for IOD or if the compulsion of using 8×8 DCT block size may be removed from the existing JPEG/MPEG standard, then there is a very good possibility to design an efficient image/video encryption in general or specifically for JPEG/MPEG.

5.7 Conclusion

In this chapter we have proposed a scheme for CAS. The actual DCT index locations are the most important attributes of any image in the DCT domain. Thus, it can be utilized to uniquely represent an image and for designing simple and efficient system for CAS based applications like image on demand. We use this attribute of the DCT indices, in which the real-time transmission of the secure and significant data is negligible. Our strategy suffices as the good quality image can never be discovered without this data and thus it helps in achieving the cryptanalytic security. In the proposed scheme, the real-time transmission of most significant and secret data is only around 0.5% of the total data required to represent an image. This leads to significant reduction in the overhead of secure communication. Further, data storage requirement is also less when compared to the existing schemes as we do not need to maintain two separate copies (one low quality and another high quality). All these salient features make the proposed scheme highly suitable for designing an efficient and simple real-time IOD application with less communication in the secure channel and less requirement of power, which is a significant advantage in wireless applications.

In the next chapter we present an efficient encryption scheme for JPEG/MPEG which results into complete obscure results by using a selective encryption approach in the DCT domain.

Chapter 6

Format Preserving JPEG/MPEG encryption

There may be many instances when there may be a need to perform secure video-conferencing in the military organizations through a public channel with limited bandwidth capacity. The communication should almost satisfy the high-level security constraints that is strictly met through a secure dedicated channel by adopting standard data encryption algorithms.

In this chapter, we develop a new format preserving selective encryption scheme for JPEG/MPEG which is compression friendly as well as highly secure. We choose quantized DCT coefficients of the I-frame for encryption. The resultant image/video is completely obscure and is suitable mainly for high end security applications. We use RC4 encryption in an intelligent manner such that zeros remain zeros even after encryption. Because of this there is no reduction in the performance of compression algorithms applied later in the standard JPEG/MPEG pipeline. So it may possibly be feasible to conduct a secure video communication within the bandwidth constraints

of already existing public channels. Experiments show that the encrypted image/video file is almost of the same size as that of un-encrypted version.

6.1 Introduction

Multimedia encryption [16, 17, 18] converts the media into unintelligible data-stream and thus protects the confidentiality of media as well as the information which is contained inside. Image/video encryption [19] converts the image/video in such a manner that it can not be understood. In many cases, when the multimedia is textual or static data, and not a real-time streaming media, we can treat it as an ordinary binary data and use the conventional encryption techniques. Encrypting the entire multimedia stream using standard encryption methods is often referred to as the "naive approach". Generally for military and law enforcement applications require full encryption and they are being sent over a fast dedicated channel. Secure Real-time Transport Protocol [121], or shortly SRTP, is an application of the naive approach. The naive approach enables the same level of security as that of the utilized conventional cryptosystem. Unfortunately, encrypting the entire bit stream is typically not possible for higher bit rate multimedia, especially when the transmission is done over a non-dedicated channel.

Current research is focused towards exploiting the format specific properties of many standard multimedia formats in order to achieve the desired performance. This is referred to as the selective encryption [110, 112, 14, 111, 14, 113]. Selective encryption consists of encrypting only a relatively small portion of the multimedia data. Selective encryption just prevents abuse of the data. In the context of video, it refers to destroying the commercial value of video to a degree which prevents a pleasant viewing experience. A common approach in selective encryption is to integrate compression with encryption.

Transformed domain is the best choice [101], where data are represented as a sequence of approximately independent and identically distributed ($i.i.d.$) samples that unequally contribute to the quality of reconstructed signal. So it is sufficient to target only a specific portion of the coefficients for encryption. Multimedia compression and encryption are usually very incompatible. Encrypting the multimedia content before compression removes a lot of redundancy and this results in a very poor compression ratio. On the other hand, encrypting the data after compression destroys the codec format, which causes decoders to crash.

Note that encryption and compression have mutually contradictory objectives. Encryption is generally an entropy increasing process. It generally works by introducing redundancy into the unencrypted data [122]. Therefore, large bandwidth or storage space is required by the encrypted data. However, to perform transmission and storage efficiently, data compression is necessary which is generally an entropy reducing transformation, i.e., it works by removing redundancy from any data-block. This is one of the key contradictory requirements for any system which provides simultaneous encryption and compression of data.

Generally for military applications we require that the encrypted image/video should be completely obscure. To achieve this, the existing schemes use naive encryption approach and a dedicated channel is required for secure transmission. While if we use selective encryption method for the same then the resultant data is still viewable although unpleasant. There may be many scenarios where without compromising much on security constraints (similar to naive approach) we may have to transmit image/video through an open public network. An efficient selective encryption scheme which can completely obscure the image/video without degrading the performance of the compression block present in the general multimedia pipeline is required. This will allow the data to be transmitted successfully within the available

channel capacity of the public network which is the basic requirement for such scenario.

In this chapter we present a selective encryption scheme applied on the non-zero DCT coefficients of the macroblocks belonging to I-frame of the JPEG/MPEG family such that the resultant image/video is completely obscure. We also take care that the performance of the compression blocks present next in the pipeline does not get affected by selective encryption process. We focus on achieving content confidentiality during real-time multimedia distribution, archiving, and other delegate processing without inducing any reduction in the performance of the compression blocks used in the next stages of the JPEG/MPEG pipeline. To achieve this goal, we have chosen the quantized non-zero DCT coefficients and applied RC4 encryption, which is one of the popular stream cipher on the same. Any other stream cipher may also be used instead of RC4 with different preprocessing. Standard quantization process has been suitably adapted so that the DCT coefficients become suitable for application of RC4 on it. Special care has been taken so that encryption process does not modify the zero coefficients. Hence performance of compression blocks placed next to this does not get hampered. The resulting system takes into consideration the structure and syntax of multimedia sources and protects the content confidentiality during delegate processing.

We have also included a Knuth shuffling block just after the encryption stage in the whole image/frame, before applying image/frame reconstruction related processes. This block provides additional security against the prediction attack performed by an adversary. Especially in the cases where scene contains lots of smooth regions or in case of black and white image/video; an adversary can easily succeed in prediction attack by placing a random DC value for each 8×8 DCT block. Application of Knuth shuffling (or any other good random shuffle) can avoid this kind of attack to a significant level.

Organization of the Chapter: The possible domains of encryption and reviews of the prior works are introduced in Section 6.2. Brief concepts of RC4, Knuth shuffling and Format Preserving Encryption are given in Section 6.3, 6.4 and 6.5 respectively. We then propose a new JPEG/MPEG encryption scheme in Section 6.6. Section 6.7 presents experimental results. In Section 6.8, we discuss the security evaluation, performance analysis and possible applications for the proposed scheme. Conclusions are drawn in Section 6.9.

6.2 Relevant Theory and Related Work

We illustrate the possible domains in which encryption can be applied to multimedia in this section, along with a review of prior work. Figure 6.1 shows the candidate domains for applying encryption to multimedia in the widely adopted multimedia coding framework.

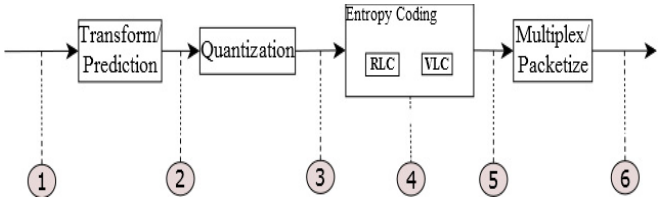


Figure 6.1: General video pipeline and possible domains to apply encryption to multimedia

6.2.1 Encryption before and after coding

According to Figure 6.1, there are 6 possible straightforward places to apply generic encryption to multimedia. The first possibility is to encrypt multimedia samples before any compression (i.e., Stage 1 in Figure 6.1). This results

into significant reduction in the compression factor because of the change in the statistical characteristics of the original multimedia source. However [123] has proposed a novel approach based on distributed source coding theory assuming an ideal Gaussian source to efficiently compress encrypted data. But for general source the compression gain, however, would be reduced, and it cannot easily support many other forms of delegate processing.

Generic encryption could be applied to the encoded bitstream after compression (i.e., Stages 5 and 6 in Figure 6.1) [124]. Bit overhead is little but applying encryption at this stage may destroy the structures and syntax of the unencrypted bitstream. Special header/marker patterns which are the part of structures enables many kinds of processing in delegate service providers and intermediate network links, such as bandwidth adaptation, unequal error protection, and random access [125], [126], [127]. Syntax-aware encryption is required to provide the above listed functionalities. One can only encrypt the content-carrying fields of the compressed multimedia bitstream, such as the fields of motion vectors and the DCT coefficients in MPEG video, and keep the structure and headers/markers of the bitstream unchanged [128], [129] to realize syntax-aware encryption with limited functionality.

6.2.2 Encryption at intermediate stages of coding

In last few years there have been thrust in the research activities to design systems which can encrypt multimedia data in such a way that the encrypted data can still be represented in a meaningful, standard-compliant format [130]. Certain multimedia coding standards, such as JPEG or MPEG-1/2/4 standard can provide secure delegate services and multimedia communications on the basis of this technique [126], [104]. For example in [126], the motion vectors in video are encrypted by applying DES to their codeword

indices at Stage 2. DC and selected AC coefficients in each block of a JPEG image or an MPEG video frame can be shuffled within the block [131], or across blocks but within the same frequency band [132] at Stage 3. At Stage 4, the entropy codeword can be spatially shuffled within the compressed bitstream [104]. There are some selective encryption schemes [124, 104, 133, 18, 134] which encrypt only portions of multimedia data stream that carry rich content. This solves the problem of high computational complexity and the potential bitrate overhead. Generally most of the existing works try to solve any particular set of problems only. For example if selective encryption is used than the encrypted data is still perceptual and if the target is to make the media completely obscure than computational complexity is high and is not suitable for real-time processing. Another important issue is of bitrate overhead. There hardly exists any scheme which simultaneously solves all of the above issues.

In the next section, as an effort to resolve most of the above listed issues through a single scheme we propose a JPEG/MPEG encryption scheme applying RC4 encryption on non-zero quantized DCT coefficients of I-frame only. The proposed scheme is general and can be easily extended to encrypt I-macroblocks of all frames as well as motion vector data also for better security. Since we don't modify the zeros of the DCT blocks, so the performance of the compression blocks used in the next stages are not affected. The resultant encrypted image/frame is completely obscure. It is Stage 3 encryption as well as structure and syntax compliant, because of which all advanced functionalities can be provided without any complications. The main motive of our design is the security and speed so that it can be used for real-time applications like secure video-conferencing. Analysis of the achieved security and the performance is given in Section 6.8.

6.3 RC4 stream cipher algorithm

Basically, there exist two types of encryption algorithms: block cipher algorithms and stream cipher algorithms. Block cipher algorithms, like the AES and the DES, operate on large blocks of plaintext, whereas stream cipher algorithms, like the RC4 or the SEAL6 [135], manipulate stream of bits/bytes of plaintext.

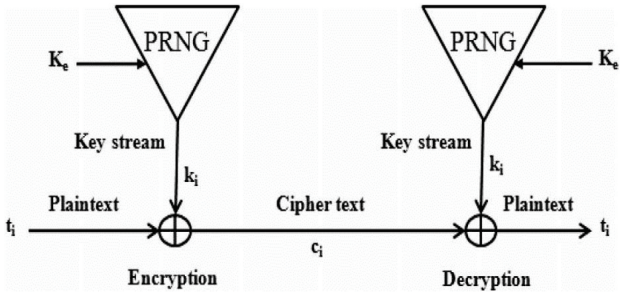


Figure 6.2: General stream cipher structure: Encryption/decryption processes of a stream cipher algorithm in which secret key is K_e. t_i, c_i, and k_i correspond to the plain text bits/bytes, the cipher text bits/bytes, and the secret keystream bits/bytes, respectively. k_i is issued by a PRNG.

As described in Figure 6.2, stream cipher algorithms combine the bits/bytes of plaintext $T = [t_1, ...t_i, ..., t_n]$ with a secret keystream of bits/bytes $K = [k_1, ...k_i, ..., k_n]$ issued from a pseudorandom number generator (PRNG), through a XOR operation typically. The keystream generation depends on one secret key K_e, making stream cipher algorithms as part of symmetric encryption techniques. Thus, bits/bytes of cipher text $C = [c_1, ...c_i, ..., c_n]$ are usually defined as

$$c_i = t_i \oplus k_i \tag{6.1}$$

Some of the main advantages of this type of algorithms are that they are simple and operate at a higher speed than block cipher algorithms [136].

The specificity of such stream cipher algorithm resides in how the bit/byte keystream is generated by the PRNG. The RC4 PRNG is based on two steps.

1. Initialization, where a table of 256 bytes is filled by repeating the encryption key as often as necessary until to fill this table.

2. Byte keystream generation, where the elements of the table are combined by applying permutations and additions to generate the keystream. More details about stream cipher algorithms can be found in [135].

6.4 Knuth Shuffling

A simple algorithm to generate a permutation of n items uniformly at random without retries, known as the Knuth shuffle, is to start with any permutation (for example, the identity permutation), and then go through the positions 1 through n - 1, and for each position k swap the element currently there with a randomly chosen element from positions k through n, inclusive. It can be verified that any permutation of n elements will be produced by this algorithm with probability exactly $\frac{1}{n!}$, thus yielding a uniform distribution over all such permutations. More details about Knuth Shuffling can be found in [137]. Knuth Shuffling can be implemented to shuffle any array of length n given a sequence of n pseudorandom entries in $[0, n-1]$. We present an algorithm to shuffle the contents of any n-element array A by using the sequence of pseudorandom entries in the array R.

Algorithm 6 Knuth Shuffle(A, R)

1: Let A be the unshuffled array of n elements.
2: $k = 0$.
3: **while** $k < n$ **do**
4: $\quad temp = A[k]$.
5: $\quad A[k] = A[R[k]]$.
6: $\quad A[R[k]] = temp$.
7: **end while**

The entries in the array R may be generated by any pseudorandom gen-

erator like RC4. The Key required to generate the array R using RC4 may be the same one used for encryption, or a different Key may be used.

6.5 Format Preserving Encryption

Format-preserving encryption (FPE) is the name given to the encryption paradigm in which output (the ciphertext) is in the same format as the input (the plaintext). The meaning of the word "format" varies. Typically it means that the plaintext and the ciphertext are from the same finite set. Typical applications that require FPE are credit card numbers. Typically 16 digits long, some systems require that these numbers must be encrypted in such a way that ciphertext is also a 16 digit number. Other uses of FPE may occur in image encryption where the image headers after encryption must be of the format prescribed by the compression protocol etc.

The seminal work in this area was written by Black and Rogaway [138], in 2002. For encrypting 16 digits the domain becomes the integer ring $Z_{10^{16}}$. Since $10^{16} < 2^{54}$, one of the techniques they propose is a 54 bit block cipher based on Feistel networks. The credit card number is converted into a 54 bit binary string and encrypted using this cipher. There is a high chance that the ciphertext will be an integer less than 10^{16} (prob = $10^{16}/2^{54} = 0.55$). If however the ciphertext is not less than 10^{16}, we carry out successive encryptions till it becomes less than 10^{16}. Using standard randomness assumptions one requires less than 2 encryptions on an average to get the required format. Black and Rogaway, proved that this technique is as secure as the block cipher that is used to construct it.

Bellare, Ristenpart, Rogaway and Stegers wrote a paper on Format Preserving Encryption [139]. This paper formally defines FPE and security goals for it. This paper also adds the concept of a tweakable block cipher to the

FPE construction to significantly enhance security and resist dictionary attacks when encrypting small domains.

6.5.1 FPE on Image/Video

In [140] two atomic encryption operations have been proposed that can preserve standard compliance and are friendly to delegate processing. But in this scheme compressibility has been compromised on an average between 3% to 7%. Extra processing to prepare a look up table (LUT) has been adopted as well as there is significant change in the entropy of the source. A transparent scrambling algorithm resulting in arbitrarily degraded view of the decoded picture is proposed in [141]. Shuffling of huffman code words is proposed in [103]. New methods of performing selective encryption and spatial/frequency shuffling of compressed digital content that maintain syntax compliance after securing the content has been introduced in [104]. The encrypted content bitstream works with many existing random access, network bandwidth adaptation, and error control techniques that have been developed for standard-compliant compressed video, thus making it especially suitable for wireless multimedia applications. Standard compliance also allows subsequent signal processing techniques to be applied to the encrypted bit-stream. But because of the restriction of a valid codeword generation as a ciphertext the process gets slow as well as security is also compromised. Since it is a selective encryption technique so the encrypted video is also perceptual.

In [142], another selective encryption for JPEG image is presented, based on the encryption of DCT coefficients. In this method, the JPEG Huffman encoder terminates runs of zeros with special symbols in order to increase the source entropy. Extra bits are added to these symbols to fully specify the magnitudes and signs of non-zero coefficients which are then encrypted using DES or IDEA.

The authors of [61] propose wavelet packet based compression scheme in which the header of a wavelet packet image coding scheme that is based on either a uniform scalar quantizer or zero-trees is protected by using AES to encrypt only the subband decomposition structure.

In [143], the authors employ a hyper-chaotic discrete nonlinear dynamic system to shuffle the plain image, and then they apply Chinese remainder theorem (well known in number theory) to diffuse and compress the shuffled image, simultaneously. In a similar work presented in [144], image scrambling encryption algorithm was proposed based on a chaotic map. The algorithm applies a transform based on the chaotic map to the pixel values as well as the positions to achieve a high degree of scrambling. This algorithm, was however completely cryptanalyzed in [145], proving that permutation based scrambling alone does not guarantee security.

A joint scrambling and compression framework [132] in which digital video data are efficiently scrambled in the frequency domain without affecting the compression efficiency significantly has been proposed in [102]. Attack on scrambling techniques has been claimed in [100, 146]. Only DC values are scrambled within a slice which makes it vulnerable since DC values of most of the blocks are almost of same value. The encrypted results are perceptual for most of the techniques proposed.

In this chapter we propose a JPEG/MPEG selective encryption technique which is format compliant as well as the encrypted result is completely obscure.

6.6 JPEG/MPEG Encryption

JPEG is the basic building block which has been extended to design general MPEG structure. Figure 6.3 shows the standard encoder structure of MPEG

video. Generally when we encrypt the media data before the coding and

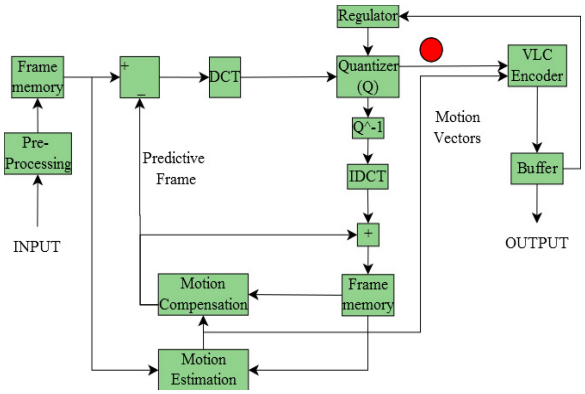


Figure 6.3: Standard MPEG Encoder Structure

compression block then the compression ratio achieved is significantly less in comparison to the un-encrypted pipeline, while after coding and compression results into destruction of syntax. Encryption process introduces delay, so we need to minimize the delay as best as possible so that it can be efficiently used for real-time streaming of video data. To achieve this, the general technique used is selective encryption. But selective encryption results in perceptual encrypted video i.e. the video content can be perceived even after encryption. Our proposed scheme successfully solves all of the above issues. It is a selective encryption scheme with significantly less computation (resulting in less delay) as well as completely obscure encryption which is achieved generally by naive approach. The details of the proposed scheme is described below as three major steps.

- Calculate minimum possible value of scale factor α used during quantization process (as in the standard JPEG/MPEG compression) of the DCT coefficients $\theta_j(i)$. It is performed so that the resultant $\theta_{j_q}(i)$ becomes compatible for applying RC4 encryption on the same, where i is the index location resulted after the zig-zag scanning of the DCT coefficients of macroblock j of an I-frame of uncompressed video V of width N and height M.

- Second step is to apply encryption on non-zero quantized DCT coefficients $\theta_{j_q}(i)$ of each macroblock of I-frame.
- Third and last step is to apply corresponding decryption process.

Step one: Calculation of Scale Factor: We have used RC4 encryption which is the most prevalently used stream cipher in use today. All standard and already verified virtues and security features of RC4 as a stream cipher are the direct advantages which we can achieve by using it in the proposed system. But as we know that general RC4 works on the data set of 0-255 so we need to convert $\theta_j(i)$ into $\theta_{j_q}(i)$ in such a manner that the difference $\delta_j = \beta_j - \gamma_j$ should be less than or equal to 255, where β_j is the maximum value of $\theta_{j_q}(i)$ and γ_j is the corresponding minimum value. We decide on a particular pattern of encoded video V' which consists only of I and P frames with an interval of λ between two I-frames. We have not considered B frames as of now. We pick the macroblocks of the DCT coefficient of I-frames only for encryption which is shown as dotted red in the Figure 6.3. The pseudo-code for calculation of α is given in Algorithm 7.

Details of the notations and abbreviations used in the subsequent algorithms.

- $QUANT(\theta_j(i), \alpha)$: Standard quantization applied on $\theta_j(i)$ using α parameter as quality factor similar to JPEG/MPEG encoder.
- $RC4ENC(\theta'_{j_q})$: RC4 encryption on θ'_{j_q}.
- $RC4DEC(\phi''_{j_q})$: RC4 decryption on ϕ''_{j_q}.

Although it is calculated for a single DCT maroblock, but a slightly increased value of α will mostly satisfy the required criterion for all DCT macroblocks of all I-frame of V.

Step two: Encryption: Now we will apply RC4 encryption on $\theta_{j_q}(i)$. Let the number of DCT macroblocks be given by τ. Algorithm 8 describes the

Algorithm 7 Calculation of α

1: $\alpha = 0$.
2: **while** $\delta > 255$ **do**
3: $\alpha = \alpha + 1$.
4: $\theta_{j_q}(i) = QUANT(\theta_j(i), \alpha)$.
5: Calculate $\delta = \beta - \gamma$.
6: **end while**
7: α is the minimum possible value of scale to be used during quantization.

exact details of encryption process.

Algorithm 8 RC4 Encryption on macroblocks of I-frame

1: **for** $j = 1$ to τ **do**
2: **for** $i = 1$ to 64 **do**
3: $\theta'_{j_q}(i) = \theta_{j_q}(i) + (-1 * \gamma(j))$.
4: **if** $\theta'_{j_q}(i) \neq (-1 * \gamma(j))$ **then**
5: $\phi_j(i) = RC4ENC(\theta'_{j_q}(i))$
6: **end if**
7: $\phi'_j(i) = \phi_j(i) + \gamma(j)$
8: **end for**
9: **end for**

Step three: Shuffling: Apply Knuth shuffling on $\phi'_j(i)$ to get $\phi''_j(i)$ and then construct back encrypted video V''.

Step four: Inverse Shuffling: Apply Inverse Knuth shuffling on $\phi''_j(i)$ to get $\phi'_j(i)$.

Step five: Decryption: Algorithm 9 presents the corresponding RC4 decryption on ϕ'_j.

6.6.1 Possible cases of conflicts and their remedies

There are two cases of conflict which may lead to an error during decryption process. They are.

Algorithm 9 RC4 Decryption on macroblocks of encrypted I-frame

1: **for** $j = 1$ to τ **do**
2: $\omega_j(k) = Zeros(k) \forall 1 \leq k \leq 64$.
3: **for** $i = 1$ to 64 **do**
4: $\phi''_{j_q}(i) = \phi'_j(i) + (-1 * \gamma(j))$.
5: $\omega_j(i) = RC4DEC(\phi''_{j_q}(i))$
6: **end for**
7: **end for**
8: Perform reverse process to construct back encrypted video V''.

1. When $\phi'_j(i) = (-1 * \gamma_j(i))$, such that the corresponding $\theta'_{j_q}(i) \neq (-1 * \gamma_j(i))$.
2. When $\phi'_j(i) = (-1 * \gamma_j(i))$, such that the corresponding $\theta'_{j_q}(i) = 0$. This case arises due to the solution provided for the first and is explained in detail below.

6.6.2 Solution for both cases

1. If first case occurs, then we replace $\phi'_j(i) \leftarrow B_j(i)$ during the $RC4ENC$ process at step 5 of Algorithm 8, where $B_j(i)$ is the state generated by the standard RC4 encryption algorithm for the corresponding $\theta'_{j_q}(i)$.
2. During decryption at step 5 of Algorithm 9, if $\phi''_j(i) = B'_j(i)$ where $B'_j(i)$ is the state generated during RC4 decryption process then two possible case arises. They are: 1) A possible solution to solve first case of conflict. 2) $\phi''_j(i) = B'_j(i)$ for a particular $\theta'_{j_q}(i)$, which is possible only when $\theta'_{j_q}(i) = 0$.
3. So we need to store an array F whose length will be equal to the number of possible error cases. In this we will store a binary flag bit which will be '1' in second case and '0' for the first case.

Now here along with the encrypted and encoded MPEG file we need to send a keyfile G which consists of RC4 encryption key π,initial seed value of Knuth Shuffle ρ, dataset $\gamma(j)$ and the flag array F to the genuine receiver to decrypt and decode the video perfectly.

6.7 Experimental Results

Figure 6.4 shows the snapshot of the original I-frame and its corresponding encrypted frame of various videos of qcif size (176×144).

Discussion on encryption results: In Figure 6.4a, 6.4b and 6.4c, the left half shows the snapshot of the original I-frame and the right side snapshot shows the corresponding encrypted version of the I-frame. One may note that the encrypted version is completely obscure and any information regarding the perception of the particular video can not be guessed. With significantly less number of computations, complete obscurity has been achieved by selectively encrypting only non-zero DCT coefficients of each macroblock of I-frame.

6.8 Security and Performance Analysis

In this section we analyze the security properties as well as the performance for the corresponding security level been achieved. For simplicity in understanding, we will present analysis for single I-frame only with sampling format of 4:2:0 [147]. Suppose the frame dimension of color video V is $N \times M$. So the number of macroblocks τ will be given by $\tau = \frac{N \times M}{16 \times 16}$. Further each macroblock is a collection of four 8×8 DCT blocks corresponding to luma component and 1 each for two chroma components. So for an adversary there

(a) Foreman

(b) Hall monitor

(c) Bus

Figure 6.4: Snapshots: Original and Encrypted frame

are various aspects of challenges.

1. To completely recover the keyfile G.
2. Try to predict the DCT coefficients of each 8×8 block and reconstruct an I-frame, provided adversary has been able to compute the correct ρ data.

First case includes the computation of ρ, π as well as $\gamma(j)$ and F. The best possible cryptanalytic result towards state recovery of RC4 requires around 2^{241} computations [148], so it is almost impossible to recover π by the generally available computational resources. Assuming that the shuffling operation permutes the DCT coefficient array using a uniformly random permutation the computational complexity required to invert it is not better than a brute force attack: which requires either guessing the permutation from the space of $N^2!$ permutations or guessing the Secret Key of the pseudo-random generator used to implement it.

In the second case even provided that adversary has somehow computed or acquired the knowledge of ρ; even than he has the only option to follow hit and trial approach. At this stage also we have two stages of security involved.

1. To guess the non-zero coefficients of all 8×8 DCT blocks independently.
2. An adversary needs to guess atleast a certain minimum number of consecutive macroblocks, in order to get slight perception of I-frame. And to completely recover the I-frame adversary needs to guess all 8×8 DCT blocks simultaneously.

An adversary can easily get the knowledge of quantity and location of zeros in a particular DCT block. Suppose on an average if Y number of locations have non-zero values then an adversary needs to compute the magnitude of Y coefficients as well as sign of $Y - 1$ coefficients (the DC coefficient is always

positive). Let's assume that $\frac{\tau}{3}$ number of macroblocks, if guessed correctly, then an adversary may be able to perceive the encrypted video. In that case, $\frac{\tau}{3} \cdot 4 \cdot Y$ (since there are $4Y$ DCT coefficients in the luminance blocks of each macroblock) number of computations are required. Only a single I-frame could be recovered by the above number of computations. Fresh π can be sent after transmitting a certain number of I-frames for better security.

6.8.1 Performance Analysis

As per the proposed encryption algorithm the number of basic operations performed during actual encryption are following:

1. To check whether quantized DCT coefficient θ_{j_q} is non-zero or not.
2. If Step 1 is true then performing XOR operation between plaintext (i.e processed DCT coefficient θ') and pseudo random sequence (i.e K) generated by the RC4 algorithm to create ciphertext (i.e. ϕ).
3. Perform Knuth shuffling on the resultant ciphertext.

Flowchart shown in Figure 6.5 explains the steps followed.

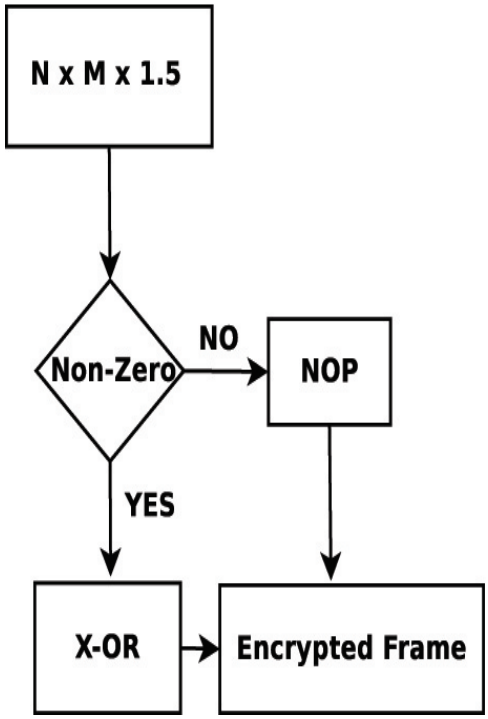


Figure 6.5: Flowchart of overall encryption process

Step 1 will require one operation each for the complete data i.e. $N \times M \times 1.5$. While Step 2 in worst case will also require $N \times M \times 1.5$ number of operations. So in total $N \times M \times 3$ number of operations need to be performed in worst case. If we consider a square frame for instance then broadly the worst case computational complexity will be $O(N^2)$. The shuffling operation takes time proportional to the size of the coefficient array, and so the number of steps taken here is $O(N^2)$.

Effect on Compression Performance: In general, the inclusion of encryption in the multimedia pipeline has an adverse effect on the compression performance. This is because any encryption technique would normally map the components of the signal to random values which increases the signal entropy resulting in degradation in compression performance. However, the proposed scheme does not modify the value as well as location of the zeros.

So the performance of compression blocks involved in the pipeline doesn't get hampered. Through experiments it has also been verified that the file size of the original and the encrypted version after applying compression scheme on the corresponding data remains same. Table 6.1 shows the file sizes of a few compressed original and encrypted videos from our database. As can be seen, the sizes of the compressed encrypted videos are almost equal to the sizes of the original compressed unencrypted videos.

6.9 Conclusion

A new format preserving selective encryption scheme for JPEG/MPEG has been developed in this chapter which is both compression friendly as well as highly secure. Quantized DCT coefficients of the I-frame have been chosen for encryption. The RC4 stream cipher has been used to provide encryption in a manner such that zeros remain unaltered after encryption. Due to this there is negligible impact on the performance of compression algorithms applied later in the standard JPEG/MPEG pipeline. It has been experimentally proven that the encrypted image/video file after compression is almost of the same size as the un-encrypted version. Whereas in this work we choose to encrypt the DCT coefficients of the I-Frame only, such an approach may also be extended to motion vectors and I-macroblocks of other frames.

			Compressed Video Sizes	
Name	Frame Size	# Frames	Original	Encrypted
Foreman	176×144	20	159 KB	159 KB
Bus	176×144	20	165 KB	165 KB
Hall monitor	176×144	20	164 KB	149 KB
Husky	176×144	20	166 KB	156 KB
Carphone	176×144	20	150 KB	162 KB
Foreman	352×288	20	595 KB	614 KB
Bus	352×288	20	619 KB	620 KB
Hall monitor	352×288	20	617 KB	587 KB
Husky	352×288	20	622 KB	617 KB
Mobile	352×288	20	600 KB	617 KB

Table 6.1: Sizes of Compressed versions of Original and Encrypted video files

Chapter 7

Conclusions and Future Directions

7.1 Summary of Studies

In this thesis we have studied the underlying technologies (for eg. Digital Watermarking, Steganography and Encryption) which are deployed to design various SDMCS based applications. We investigate the extent to which the proposed technology has been successful in providing a fool-proof solution for the relevant SDMCS. We also propose better/improved systems and scheme as a solution to those identified problems.

The SDMCS based systems which have been analyzed, improved or new models have been developed for them are as follows.

- Covert Communication system using reversible data hiding techniques.
- Robustness analysis against the possible attacks of forgery or watermark removal by cryptanalysing the existing robust correlation-based

digital watermarking scheme.

- CAS for IOD using selective encryption technique.
- Secure multimedia communication through selective encryption of the multimedia signals.

7.2 Contribution of the Thesis

The contribution of the thesis towards improvement of existing SDMCS and new system designs are as follows.

In Chapter 3 we analyze the problem and propose a reversible data hiding scheme for digital images using integer wavelet transform and threshold embedding technique. Data are embedded into the least two significant bitplane (LSB) of high frequency CDF (2,2) integer wavelet coefficients whose magnitudes are smaller than a certain predefined threshold. Histogram modification is applied as a preprocessing step to prevent overflow/underflow. Experimental results show that this scheme performs better than prior techniques in terms of a higher payload and better image quality.

In Chapter 4 we show that a generic watermark removal attack on a correlation-based watermarking scheme can be extended in general to a forgery attack on the same. In certain cases, even if there exists a weak watermark removal strategy, it may be extended to a strong forgery attack. We prove our case by implementing our strategy against MDEW [1] which is considered to be one of the robust correlation-based watermarking schemes in the DCT domain.

Chapter 5 presents a novel CAS for 'image on demand' commercial applications, using index locations of the DCT coefficients. Here we point out the significance of using the index locations of the DCT coefficients as a unique

descriptor of any image and propose a novel scheme that can be efficiently adapted for any CAS. In the proposed scheme, we share a low quality version of an image with the customers in the form of polynomials that approximate the sorted DCT coefficients and major fraction of index locations. We keep secret an optimal number of index locations which are the most significant. These are shared to the customers only on demand, to construct the corresponding high quality image.

Finally in Chapter 6 we present a novel research work around JPEG and MPEG encryption. Through this research we have proposed a new format preserving selective encryption scheme for JPEG/MPEG which is compression friendly as well as highly secure. We choose quantized DCT coefficients of the I-frame for encryption. The resultant image/video is completely obscure and is suitable mainly for high end security applications. We use RC4 encryption in an intelligent manner such that zeros remain zeros even after encryption. Because of this there is negligible impact on the performance of compression algorithms applied later in the standard JPEG/MPEG pipeline. Shuffling has also been applied to avoid prediction based attacks possible in smooth image/videos.

7.3 Summary of Possible Directions

The investigation carried out in the present work leaves enough scope for extension and application of the concepts presented in this thesis in the field of secure digital multimedia communication.

In Chapter 3, we have proposed a reversible data hiding scheme using integer wavelet transform using an arbitrary threshold value selection. Arbitrary selection of threshold may not yield the best payload capacity for different images. So if threshold may be calculated on the basis of image attributes

then it is fairly possible to achieve the maximum data hiding capacity of a particular image with minimum possible degradation of the image.

In Chapter 4, we have described a general strategy that converts a single-copy watermark removal attack on any correlation-based scheme to a single-copy forgery attack on the same. We have taken the example of MDEW [1], one of the strongest correlation-based schemes, to mount our attack, and prove its effectiveness. The beauty of our attack model is that even a very weak single-copy watermark removal attack may be extended to obtain a strong single-copy forgery attack on correlation-based watermarking schemes. We have substantiated our model through attacks on MDEW, and complete theoretical analysis and experimental verification of the same. In the future, a similar strategy may possibly be exploited against other categories of watermarking schemes as well.

We have proposed a scheme for CAS using the DCT indices in Chapter 5, in which the real-time transmission of the secure and significant data is negligible. However, it suffices as the good quality image can never be discovered without this data and thus it helps in achieving the cryptanalytic security. Few other CAS based systems can also be explored and the suitability of the proposed strategy in those systems can be investigated.

A new format preserving selective encryption scheme for JPEG/MPEG has been developed in Chapter 6, which is both compression friendly as well as highly secure. Quantized DCT coefficients of the I-frame have been chosen for encryption. The RC4 stream cipher has been used for encryption. The scheme can further be enhanced by encrypting the I-macro blocks of other frames as well. Motion vectors may also be encrypted. Suitability of some other stream cipher which may reduce the number of computations must be investigated in future.

Bibliography

[1] T.K. Das, S. Maitra, and J. Mitra. Cryptanalysis of optimal differential energy watermarking (dew) and a modified robust scheme. *Signal Processing, IEEE Transactions on*, 53(2):768–775, Feb 2005.

[2] Wenjun Zeng, Heather Yu, and Ching-Yung Lin. *Multimedia Security Technologies for Digital Rights Management.* Academic Press, Inc., Orlando, FL, USA, 2006.

[3] T. Meenpal and A.K. Bhattacharjee. High capacity reversible data hiding using iwt. In *Electronic System Design (ISED), 2011 International Symposium on*, pages 352–357, Dec 2011.

[4] Chun-Shien Lu. *Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property.* IGI Global, Hershey, PA, USA, 2004.

[5] Gerrit C. Langelaar, Reginald L. Lagendijk, and Jan Biemond. Real-time labeling of mpeg-2 compressed video. *Journal of Visual Communication and Image Representation*, 9(4):256 – 270, 1998.

[6] Funda Ergun, Joe Kilian, and Ravi Kumar. A note on the limits of collusion-resistant watermarks. In Jacques Stern, editor, *Advances in Cryptology EUROCRYPT 99*, volume 1592 of *Lecture Notes in Computer Science*, pages 140–149. Springer Berlin Heidelberg, 1999.

[7] Gregory K. Wallace. The jpeg still picture compression standard. *Commun. ACM*, 34(4):30–44, April 1991.

[8] S.G. Mallat. A theory for multiresolution signal decomposition: the wavelet representation. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 11(7):674–693, Jul 1989.

[9] Stefan Katzenbeisser and Fabien A. Petitcolas, editors. *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House, Inc., Norwood, MA, USA, 1st edition, 2000.

[10] FabienA.P. Petitcolas, RossJ. Anderson, and MarkusG. Kuhn. Attacks on copyright marking systems. In *Information Hiding*, volume 1525 of *Lecture Notes in Computer Science*, pages 218–238. Springer Berlin Heidelberg, 1998.

[11] Fabien A.P. Petitcolas and R.J. Anderson. Evaluation of copyright marking systems. In *Multimedia Computing and Systems, 1999. IEEE International Conference on*, volume 1, pages 574–579 vol.1, Jul 1999.

[12] T.K. Das and S. Maitra. Cryptanalysis of correlation-based watermarking schemes using single watermarked copy. *Signal Processing Letters, IEEE*, 11(4):446–449, April 2004.

[13] T.K. Das, S. Maitra, and Jianying Zhou. Cryptanalysis of chu's dct based watermarking scheme. *Multimedia, IEEE Transactions on*, 8(3):629–632, June 2006.

[14] T. Lookabaugh and D.C. Sicker. Selective encryption for consumer applications. *Communications Magazine, IEEE*, 42(5):124–129, May 2004.

[15] Toshanlal Meenpal, Subhadeep Banik, and Subhamoy Maitra. A scheme for conditional access-based systems using index locations of

dct coefficients. *Journal of Real-Time Image Processing*, pages 1–11, 2014.

[16] E.T. Lin, A.M. Eskicioglu, R.L. Lagendijk, and E.J. Delp. Advances in digital video content protection. *Proceedings of the IEEE*, 93(1):171–183, Jan 2005.

[17] S.S. Maniccam and N.G. Bourbakis. Image and video encryption using {SCAN} patterns. *Pattern Recognition*, 37(4):725 – 737, 2004. Agent Based Computer Vision.

[18] Chung ping Wu and C.-C. Jay Kuo. Efficient multimedia encryption via entropy codec design. In *IS&T/SPIE 13th Annual Symposium on Electronic Imaging, Proceedings of SPIE*, pages 128–138, 2001.

[19] Lintian Qiao and Klara Nahrstedt. A new algorithm for mpeg video encryption. In *In Proceedings of The First International Conference on Imaging Science, Systems, and Technology (CISST97*, pages 21–29, 1997.

[20] Gregory Kipper. *Investigator's Guide to Steganography*. CRC Press, Inc., Boca Raton, FL, USA, 2003.

[21] Andreas Westfeld and Andreas Pfitzmann. Attacks on steganographic systems - breaking the steganographic utilities ezstego. In *Jsteg, Steganos, and S-Tools - and Some Lessons Learned, Lecture Notes in Computer Science*, pages 61–75. Springer-Verlag, 2000.

[22] Jessica J. Fridrich, David Soukal, and Miroslav Goljan. Maximum likelihood estimation of length of secret message embedded using k steganography in spatial domain. In *Security, Steganography, and Watermarking of Multimedia Contents*, volume 5681, pages 595–606, 2005.

[23] Xiaolong Li, Bin Yang, Daofang Cheng, and Tieyong Zeng. A generalization of lsb matching. *Signal Processing Letters, IEEE*, 16(2):69–72,

Feb 2009.

[24] J. Mielikainen. Lsb matching revisited. *Signal Processing Letters, IEEE*, 13(5):285–287, May 2006.

[25] S. Dumitrescu, Xiaolin Wu, and N. Memon. On steganalysis of random lsb embedding in continuous-tone images. In *Image Processing. 2002. Proceedings. 2002 International Conference on*, volume 3, pages 641–644 vol.3, June 2002.

[26] R. Crandall. Some notes on steganography, 1998.

[27] Eiji Kawaguchi and Richard O. Eason. Principle and applications of bpcs-steganography, 1998.

[28] IngemarJ. Cox, Joe Kilian, Tom Leighton, and Talal Shamoon. A secure, robust watermark for multimedia. In Ross Anderson, editor, *Information Hiding*, volume 1174 of *Lecture Notes in Computer Science*, pages 185–206. Springer Berlin Heidelberg, 1996.

[29] E. Koch and J. Zhao. Towards robust and hidden image copyright labeling. pages 452–455, 1995.

[30] Xiang-Gen Xia, C.G. Boncelet, and G.R. Arce. A multiresolution watermark for digital images. In *Image Processing, 1997. Proceedings., International Conference on*, volume 1, pages 548–551 vol.1, Oct 1997.

[31] G.B. Rhoads. Method and apparatus responsive to a code signal conveyed through a graphic image, January 20 1998. US Patent 5,710,834.

[32] M.D. Swanson, Bin Zhu, and A.H. Tewfik. Transparent robust image watermarking. In *Image Processing, 1996. Proceedings., International Conference on*, volume 3, pages 211–214 vol.3, Sep 1996.

[33] N.F. Johnson and S. Jajodia. Exploring steganography: Seeing the unseen. *Computer*, 31(2):26–34, Feb 1998.

[34] Gerhard C. Langelaar, Jan C. A. van der Lubbe, and Reginald L. Lagendijk. Robust labeling methods for copy protection of images, 1997.

[35] N. Provos and P. Honeyman. Hide and seek: an introduction to steganography. *Security Privacy, IEEE*, 1(3):32–44, May 2003.

[36] Peter Wayner. *Disappearing Cryptography (Third Edition)*. Morgan Kaufmann, 2009.

[37] C. Manikopoulos, Yun-Qing Shi, Sui Song, Zheng Zhang, Zhicheng Ni, and D. Zou. Detection of block dct-based steganography in gray-scale images. In *Multimedia Signal Processing, 2002 IEEE Workshop on*, pages 355–358, Dec 2002.

[38] Wen-Yuan Chen. Color image steganography scheme using set partitioning in hierarchical trees coding, digital fourier transform and adaptive phase modulation. *Applied Mathematics and Computation*, 185(1):432 – 448, 2007.

[39] V.M. Potdar, Song Han, and E. Chang. A survey of digital image watermarking techniques. In *Industrial Informatics, 2005. INDIN '05. 2005 3rd IEEE International Conference on*, pages 709–716, Aug 2005.

[40] B. Verma, S. Jain, and D. P. Agarwal. Watermarking image databases: a review. In *Proceedings of the International Conference on Cognition and Recognition, Mandya, Karnataka, India,*, pages 171–179, December 2005.

[41] N.K. Abdulaziz and K.K. Pang. Robust data hiding for images. In *Communication Technology Proceedings, 2000. WCC - ICCT 2000. International Conference on*, volume 1, pages 380–383 vol.1, 2000.

[42] L.D. Paulson. News briefs. *Computer*, 39(12):23–25, Dec 2006.

[43] J.M. Barton. Method and apparatus for embedding authentication information within digital data, July 8 1997. US Patent 5,646,997.

[44] C.W. Honsinger, P.W. Jones, M. Rabbani, and J.C. Stoffel. Lossless recovery of an original image containing embedded data, August 21 2001. US Patent 6,278,791.

[45] C. De Vleeschouwer, J.F. Delaigle, and B. Macq. Circular interpretation of histogram for reversible watermarking. In *Multimedia Signal Processing, 2001 IEEE Fourth Workshop on*, pages 345–350, 2001.

[46] C. De Vleeschouwer, J.-F. Delaigle, and B. Macq. Circular interpretation of bijective transformations in lossless watermarking for media asset management. *Multimedia, IEEE Transactions on*, 5(1):97–105, March 2003.

[47] J. Fridrich, M. Goljan, and Rui Du. Invertible authentication watermark for jpeg images. In *Information Technology: Coding and Computing, 2001. Proceedings. International Conference on*, pages 223–227, Apr 2001.

[48] Jessica Fridrich, Miroslav Goljan, and Rui Du. Lossless data embedding–new paradigm in digital watermarking. *EURASIP J. Appl. Signal Process.*, 2002(2):185–196, February 2002.

[49] M.U. Celik, G. Sharma, A.M. Tekalp, and E. Saber. Lossless generalized-lsb data embedding. *Image Processing, IEEE Transactions on*, 14(2):253–266, Feb 2005.

[50] The Duc Kieu and Chin-Chen Chang. A high stego-image quality steganographic scheme with reversibility and high payload using multiple embedding strategy. *Journal of Systems and Software*, 82(10):1743 – 1752, 2009. SI: {YAU}.

[51] Jun Tian. Reversible data embedding using a difference expansion. *Circuits and Systems for Video Technology, IEEE Transactions on*, 13(8):890–896, Aug 2003.

[52] A. J. A. J.Menezes, P. C. Van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[53] *FIPS PUBS 46-2: Data Encryption Standard*. 1993.

[54] R.L. Rivest, A. Shamir, and L.M. Adleman. Cryptographic communications system and method, September 20 1983. US Patent 4,405,829.

[55] *FIPS PUB 197: Advanced Encryption Standard (AES)*. 2001.

[56] J.L. Massey and X. Lai. Device for the conversion of a digital block and use of same, May 25 1993. US Patent 5,214,703.

[57] S. Sridharan, E. Dawson, and B. Goldburg. Fast fourier transform based speech encryption system. *Communications, Speech and Vision, IEE Proceedings I*, 138(3):215–223, June 1991.

[58] N. Bourbakis and A. Dollas. Scan-based compression-encryption-hiding for video on demand. *MultiMedia, IEEE*, 10(3):79–87, July 2003.

[59] S.S. Maniccam and N.G. Bourbakis. Lossless image compression and encryption using {SCAN}. *Pattern Recognition*, 34(6):1229 – 1245, 2001.

[60] Josef Scharinger. Fast encryption of image data using chaotic kolmogorov flows. *J. Electronic Imaging*, 7(2):318–325, 1998.

[61] Andreas Pommer and Andreas Uhl. Selective encryption of wavelet-packet encoded image data: efficiency and security. *Multimedia Systems*, 9(3):279–287, 2003.

[62] *ISO-IEC 13818-2: Information technology 'generic coding of moving pictures and associated audio information: video*. December 15 2000.

[63] G.A. Spanos and T.B. Maples. Performance study of a selective encryption scheme for the security of networked, real-time video. In *Computer Communications and Networks, 1995. Proceedings., Fourth International Conference on*, pages 2–10, Sept 1995.

[64] I. Agi and Li Gong. An empirical study of secure mpeg video transmissions. In *Network and Distributed System Security, 1996., Proceedings of the Symposium on*, pages 137–144, Feb 1996.

[65] A.M. Alattar and G.I. Al-Regib. Evaluation of selective encryption techniques for secure transmission of mpeg-compressed bit-streams. In *Circuits and Systems, 1999. ISCAS '99. Proceedings of the 1999 IEEE International Symposium on*, volume 4, pages 340–343 vol.4, Jul 1999.

[66] T. Kunkelmann and R. Reinema. A scalable security architecture for multimedia communication standards. In *Multimedia Computing and Systems '97. Proceedings., IEEE International Conference on*, pages 660–661, Jun 1997.

[67] Changgui Shi and Bharat Bhargava. A fast mpeg video encryption algorithm. In *Proceedings of the Sixth ACM International Conference on Multimedia*, MULTIMEDIA '98, pages 81–88, New York, NY, USA, 1998. ACM.

[68] SangUk Shin, KyeongSeop Sim, and KyungHyune Rhee. A secrecy scheme for mpeg video data using the joint of compression and encryption. In *Information Security*, volume 1729 of *Lecture Notes in Computer Science*, pages 191–201. Springer Berlin Heidelberg, 1999.

[69] Carsten Griwodz, Oliver Merkel, Jana Dittmann, and Ralf Steinmetz. Protecting vod the easier way. In *Proceedings of the Sixth ACM International Conference on Multimedia*, MULTIMEDIA '98, pages 21–28, New York, NY, USA, 1998. ACM.

[70] H. Cheng and Xiaobo Li. Partial encryption of compressed images and videos. *Signal Processing, IEEE Transactions on*, 48(8):2439–2451, Aug 2000.

[71] A. Pommer and A. Uhl. Wavelet packet methods for multimedia compression and encryption. In *Communications, Computers and signal Processing, 2001. PACRIM. 2001 IEEE Pacific Rim Conference on*, volume 1, pages 1–4 vol.1, 2001.

[72] S. Roche, J. Dugelay, and R. Molva. Multi-resolution access control algorithm based on fractal coding. In *Image Processing, 1996. Proceedings., International Conference on*, volume 3, pages 235–238 vol.3, Sep 1996.

[73] D.M. Thodi and J.J. Rodriguez. Prediction-error based reversible watermarking. In *Image Processing, 2004. ICIP '04. 2004 International Conference on*, volume 3, pages 1549–1552 Vol. 3, Oct 2004.

[74] R.Y.M. Li, O.C. Au, C.K.M. Yuk, Shu-Kei Yip, and Tai-Wai Chan. Enhanced image trans-coding using reversible data hiding. In *Circuits and Systems, 2007. ISCAS 2007. IEEE International Symposium on*, pages 1273–1276, May 2007.

[75] Zhicheng Ni, Yun-Qing Shi, N. Ansari, and Wei Su. Reversible data hiding. *Circuits and Systems for Video Technology, IEEE Transactions on*, 16(3):354–362, March 2006.

[76] A.M. Alattar. Reversible watermark using the difference expansion of a generalized integer transform. *Image Processing, IEEE Transactions on*, 13(8):1147–1156, Aug 2004.

[77] L. Kamstra and H.J.A.M. Heijmans. Reversible data embedding into images using wavelet techniques and sorting. *Image Processing, IEEE Transactions on*, 14(12):2082–2090, Dec 2005.

[78] D.M. Thodi and J.J. Rodriguez. Expansion embedding techniques for reversible watermarking. *Image Processing, IEEE Transactions on*, 16(3):721–730, March 2007.

[79] Guorong Xuan, Jiang Zhu, Jidong Chen, Y.Q. Shi, Zhicheng Ni, and Wei Su. Distortionless data hiding based on integer wavelet transform. *Electronics Letters*, 38(25):1646–1648, Dec 2002.

[80] Guorong Xua, Y.Q. Shi, Chengyun Yang, Yizhan Zheng, D. Zou, and Peiqi Chai. Lossless data hiding using integer wavelet transform and threshold embedding technique. In *Multimedia and Expo, 2005. ICME 2005. IEEE International Conference on*, pages 1520–1523, July 2005.

[81] Ching-Chiuan Lin, Nien-Lin Hsueh, and Wen-Hsiang Shen. High-performance reversible data hiding. *Fundam. Inf.*, 82(1-2):155–169, January 2008.

[82] Ju-Yuan Hsiao, Ke-Fan Chan, and J. Morris Chang. Block-based reversible data embedding. *Signal Process.*, 89(4):556–569, April 2009.

[83] Xianting Zeng A B, Lingdi Ping, and Zhuo Li. Lossless data hiding scheme using adjacent pixel difference based on scan path.

[84] Ching yu Yang A, Wu chih Hu A, and Chih hung Lin B. Reversible data hiding by coefficient-bias algorithm, 2009.

[85] Ching yu Yang A, Wu chih Hu A, and Chih hung Lin B. Reversible data hiding by adaptive iwt coefficient adjustment, 2011.

[86] G.C. Langelaar and R.L. Lagendijk. Optimal differential energy watermarking of dct encoded images and video. *Image Processing, IEEE Transactions on*, 10(1):148–158, Jan 2001.

[87] Ingemar J. Cox, Joe Kilian, F.T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia. *Image Processing,*

IEEE Transactions on, 6(12):1673–1687, Dec 1997.

[88] Image databases. available at. ImageProcessingPlace.com. `http://www.imageprocessingplace.com/root_files_V3/image_databases.htm`.

[89] A. Abrardo and M. Barni. Informed watermarking by means of orthogonal and quasi-orthogonal dirty paper coding. *Signal Processing, IEEE Transactions on*, 53(2):824–833, Feb 2005.

[90] M.L. Miller, G.J. Doerr, and Ingemar J. Cox. Applying informed coding and embedding to design a robust high-capacity watermark. *Image Processing, IEEE Transactions on*, 13(6):792–807, June 2004.

[91] Wei Wang, M. Hempel, Dongming Peng, Honggang Wang, H. Sharif, and Hsiao-Hwa Chen. On energy efficient encryption for video streaming in wireless sensor networks. *Multimedia, IEEE Transactions on*, 12(5):417–426, Aug 2010.

[92] Xiaotian Xu, Yong Liang Guan, and Kah Chan Teh. Performance analysis of binned orthogonal/bi-orthogonal block code as dirty-paper code for digital watermarking application. *Signal Processing Letters, IEEE*, 16(3):208–211, March 2009.

[93] J. Delgado, S. Llorente, and E. Rodriguez. Digital rights and privacy policies management as a service. In *Consumer Communications and Networking Conference (CCNC), 2012 IEEE*, pages 527–531, Jan 2012.

[94] R. Easley, Byung Cho Kim, and Daewon Sun. Optimal digital rights management with uncertain piracy. In *System Science (HICSS), 2012 45th Hawaii International Conference on*, pages 4525–4534, Jan 2012.

[95] Jung-Yoon Kim and Hyoung-Kee Choi. Improvements on sun 's conditional access system in pay-tv broadcasting systems. *Multimedia, IEEE Transactions on*, 12(4):337–340, June 2010.

[96] Lei Lei Win, T. Thomas, and S. Emmanuel. Privacy enabled digital rights management without trusted third party assumption. *Multimedia, IEEE Transactions on*, 14(3):546–554, June 2012.

[97] Bigstockphoto.com. `http://www.bigstockphoto.com/`.

[98] Fotomoto.com. `http://www.fotomoto.com/`.

[99] PlanetObserever.com. `http://www.planetobserver.com/`.

[100] B. Goldburg, S. Sridharan, and E. Dawson. Design and cryptanalysis of transform-based analog speech scramblers. *Selected Areas in Communications, IEEE Journal on*, 11(5):735–744, Jun 1993.

[101] M. Grangetto, E. Magli, and G. Olmo. Multimedia selective encryption by means of randomized arithmetic coding. *Multimedia, IEEE Transactions on*, 8(5):905–917, Oct 2006.

[102] Wenjun Zeng and Shawmin Lei. Efficient frequency domain selective scrambling of digital video. *Multimedia, IEEE Transactions on*, 5(1):118–129, March 2003.

[103] M.S. Kankanhalli and Teo Tian Guan. Compressed-domain scrambler/descrambler for digital video. *Consumer Electronics, IEEE Transactions on*, 48(2):356–365, May 2002.

[104] Jiangtao Wen, M. Severa, Wenjun Zeng, M.H. Luttrell, and Weiyin Jin. A format-compliant configurable encryption framework for access control of video. *Circuits and Systems for Video Technology, IEEE Transactions on*, 12(6):545–557, Jun 2002.

[105] American national standard x9.17: Financial institution key management (wholesale), 1985.

[106] W. Diffie and M.E. Hellman. New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6):644–654, Nov 1976.

[107] D. Naor and M. Naor. Protecting cryptographic keys: the trace-and-revoke approach. *Computer*, 36(7):47–53, July 2003.

[108] D. Diaz-Sanchez, A. Marin, F. Almenarez, and A. Cortes. Sharing conditional access modules through the home network for pay tv access. *Consumer Electronics, IEEE Transactions on*, 55(1):88–96, February 2009.

[109] Shyh-Yih Wang and Chi-Sung Laih. Efficient key distribution for access control in pay-tv systems. *Multimedia, IEEE Transactions on*, 10(3):480–492, April 2008.

[110] F. Dufaux and T. Ebrahimi. Scrambling for privacy protection in video surveillance systems. *Circuits and Systems for Video Technology, IEEE Transactions on*, 18(8):1168–1174, Aug 2008.

[111] Honggang Wang, M. Hempel, Dongming Peng, Wei Wang, H. Sharif, and Hsiao-Hwa Chen. Index-based selective audio encryption for wireless multimedia sensor networks. *Multimedia, IEEE Transactions on*, 12(3):215–223, April 2010.

[112] Shiguo Lian and Xi Chen. On the design of partial encryption scheme for multimedia content. *Mathematical and Computer Modelling*, 57(1112):2613 – 2624, 2013. Information System Security and Performance Modeling and Simulation for Future Mobile Networks.

[113] Wei Wang, M. Hempel, Dongming Peng, Honggang Wang, H. Sharif, and Hsiao-Hwa Chen. On energy efficient encryption for video streaming in wireless sensor networks. *Multimedia, IEEE Transactions on*, 12(5):417–426, Aug 2010.

[114] D. Kundur and K. Karthik. Video fingerprinting and encryption principles for digital rights management. *Proceedings of the IEEE*, 92(6):918–932, June 2004.

[115] A. Gupta, S. Sultana, M. Kirkpatrick, and E. Bertino. A selective encryption approach to fine-grained access control for p2p file sharing. In *Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2010 6th International Conference on*, pages 1–10, Oct 2010.

[116] A. Pande, P. Mohapatra, and J. Zambreno. Securing multimedia content using joint compression and encryption. *MultiMedia, IEEE*, 20(4):50–61, Oct 2013.

[117] Z. Shahid and W. Puech. Visual protection of hevc video by selective encryption of cabac binstrings. *Multimedia, IEEE Transactions on*, 16(1):24–36, Jan 2014.

[118] Fei Peng, Xiao wen Zhu, and Min Long. An roi privacy protection scheme for h.264 video based on fmo and chaos. *Information Forensics and Security, IEEE Transactions on*, 8(10):1688–1699, Oct 2013.

[119] Shujun Li, Guanrong Chen, A. Cheung, B. Bhargava, and Kwok-Tung Lo. On the design of perceptual mpeg-video encryption algorithms. *Circuits and Systems for Video Technology, IEEE Transactions on*, 17(2):214–223, Feb 2007.

[120] R. C. Gonzalez and R. E. Woods. *Digital Image Processing, Second ed.* Pearson Education, 2003.

[121] Albert J. Ahumada, Jr. and Heidi A. Peterson. Luminance-model-based dct quantization for color image compression. volume 1666, pages 365–374, 1992.

[122] C. C. Chang. Computer cryptography and information security, 1989.

[123] M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg, and K. Ramchandran. On compressing encrypted data. *Signal Processing, IEEE Transactions on*, 52(10):2992–3006, Oct 2004.

[124] Lintian Qiao and Klara Nahrstedt. Comparison of {MPEG} encryption algorithms. *Computers & Graphics*, 22(4):437 – 448, 1998.

[125] Yao Wang, S. Wenger, Jiantao Wen, and A.K. Katsaggelos. Error resilient video coding techniques. *Signal Processing Magazine, IEEE*, 17(4):61–82, Jul 2000.

[126] J. Wen, M. Muttrell, and M. Severa. Access control of standard video bitstreams. In *Int. Conf. Media Future, Florence, Italy*, May 2001.

[127] Nicholas Yeadon, Francisco Garca, David Hutchison, and Doug Shepherd. Continuous media filters for heterogeneous internetworking. In *In Proceedings of the Conference in Multimedia Computing and Networking*, 1996.

[128] S.J. Wee and J.G. Apostolopoulos. Secure scalable streaming enabling transcoding without decryption. In *Image Processing, 2001. Proceedings. 2001 International Conference on*, volume 1, pages 437–440 vol.1, 2001.

[129] Chun Yuan, B.B. Zhu, Yidong Wang, Shipeng Li, and Yuzhuo Zhong. Efficient and fully scalable encryption for mpeg-4 fgs. In *Circuits and Systems, 2003. ISCAS '03. Proceedings of the 2003 International Symposium on*, volume 2, pages II–620–II–623 vol.2, May 2003.

[130] Nicholas Paul Sheppard. On implementing mpeg-21 intellectual property management and protection. In *Proceedings of the 2007 ACM Workshop on Digital Rights Management*, DRM '07, pages 10–22, New York, NY, USA, 2007. ACM.

[131] Lei Tang. Methods for encrypting and decrypting mpeg video data efficiently. In *Proceedings of the Fourth ACM International Conference on Multimedia*, MULTIMEDIA '96, pages 219–229, New York, NY, USA, 1996. ACM.

[132] Wenjun Zeng and Shawmin Lei. Efficient frequency domain video scrambling for content access control. In *Proceedings of the Seventh ACM International Conference on Multimedia (Part 1)*, MULTIMEDIA '99, pages 285–294, New York, NY, USA, 1999. ACM.

[133] Tsung li Wu and S. Felix Wu. Selective encryption and watermarking of mpeg video (extended abstract). In *Proceedings of the International Conference on Image Science, Systems, and Technology, CISST 97, Las Vegas*, 1997.

[134] Min Wu and Yinian Mao. Communication-friendly encryption of multimedia. In *Multimedia Signal Processing, 2002 IEEE Workshop on*, pages 292–295, Dec 2002.

[135] Schneier. B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, 1996.

[136] W. Puech and J. M. Rodrigues. A new crypto-watermarking method for medical images safe transfer. In *in Proc. 12 th European Signal Processing Conference (EUSIPCO04*, pages 1481–1484, 2004.

[137] Knuth shuffling theory. `http://www.http:en.wikipedia.org/wiki/Random_permutation#Knuth_shuffles.htm`.

[138] John Black and Phillip Rogaway. Ciphers with arbitrary finite domains. In Bart Preneel, editor, *Topics in Cryptology CT-RSA 2002*, volume 2271 of *Lecture Notes in Computer Science*, pages 114–130. Springer Berlin Heidelberg, 2002.

[139] Mihir Bellare, Thomas Ristenpart, Phillip Rogaway, and Till Stegers. Format-preserving encryption. Cryptology ePrint Archive, Report 2009/251, 2009. `http://eprint.iacr.org/`.

[140] Yinian Mao and Min Wu. A joint signal processing and cryptographic approach to multimedia encryption. *Image Processing, IEEE Transac-*

tions on, 15(7):2061–2075, July 2006.

[141] Ci Wang, Hong-Bin Yu, and Meng Zheng. A dct-based mpeg-2 transparent scrambling algorithm. *Consumer Electronics, IEEE Transactions on*, 49(4):1208–1213, Nov 2003.

[142] Marc Van Droogenbroeck and Raphal Benedett. Techniques for a selective encryption of uncompressed and compressed images. In *Proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS) 2002*, pages 9–11.

[143] Hegui Zhu, Cheng Zhao, and Xiangde Zhang. A novel image encryptioncompression scheme using hyper-chaos and chinese remainder theorem. *Signal Processing: Image Communication*, 28(6):670 – 680, 2013.

[144] Guodong Ye. Image scrambling encryption algorithm of pixel bit based on chaos map. *Pattern Recognition Letters*, 31(5):347 – 354, 2010.

[145] Chengqing Li and Kwok-Tung Lo. Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. *Signal Processing*, 91(4):949 – 954, 2011.

[146] B. Goldburg, S. Sridharan, and E. Dawson. Cryptanalysis of frequency domain analogue speech scramblers. *Communications, Speech and Vision, IEE Proceedings I*, 140(4):235–239, Aug 1993.

[147] M. Ghanbari. *Standard Codecs: Image Compression to Advanced Video Coding*. Institution Electrical Engineers, 2003.

[148] Alexander Maximov and Dmitry Khovratovich. New state recovery attack on rc4. In David Wagner, editor, *Advances in Cryptology CRYPTO 2008*, volume 5157 of *Lecture Notes in Computer Science*, pages 297–316. Springer Berlin Heidelberg, 2008.