STATUS OF THESIS

Title of thesis | A Novel Joint Perceptual Encryption and Watermarking Scheme (JPEW) Within JPEG Framework

I MUHAMMAD IMRAN KHAN
(CAPITAL LETTERS)

hereby allow my thesis to be placed at the Information Resource Center (IRC) of Universiti Teknologi PETRONAS (UTP) with the following conditions:

1. The thesis becomes the property of UTP
2. The IRC of UTP may make copies of the thesis for academic purposes only.
3. This thesis is classified as

☐ Confidential

☒ Non-confidential

If this thesis is confidential, please state the reason:

_____

_____

The contents of the thesis will remain confidential for _____ years.

Remarks on disclosure:

_____

_____

Endorsed by

_____ Signature of Author

_____ Signature of Supervisor

Permanent address:
House No. 32, Street No. 53,
CAT-II, G-10/3,
ISLAMABAD, PAKISTAN.

Name of Supervisor
Assoc. Prof. Dr. Varun Jeoti

Date : 16-06-2011

Date : 16-06-2011

UNIVERSITI TEKNOLOGI PETRONAS

A JOINT PERCEPTUAL ENCRYPTION AND WATERMARKING SCHEME (JPEW) WITHIN JPEG FRAMEWORK

by

MUHAMMAD IMRAN KHAN

The undersigned certify that they have read, and recommend to the Postgraduate Studies Programme for acceptance this thesis for the fulfilment of the requirements for the degree stated.

Signature: _____

Main Supervisor: Assoc. Prof. Dr. Varun Jeoti

Signature: _____

Co-Supervisor: Dr. Aamir Saeed Malik

Signature: _____

Head of Department: Assoc. Prof. Dr. Nor Hisham Bin Hamid

Date: _____

A NOVEL JOINT PERCEPTUAL ENCRYPTION AND WATERMARKING SCHEME (JPEW) WITHIN JPEG FRAMEWORK

by

MUHAMMAD IMRAN KHAN

A Thesis

Submitted to the Postgraduate Studies Programme

as a Requirement for the Degree of

MASTER OF SCIENCE

ELECTRICAL AND ELECTRONIC ENGINEERING

UNIVERSITI TEKNOLOGI PETRONAS

BANDAR SERI ISKANDAR,

PERAK

JUNE 2011

DECLARATION OF THESIS

Title of thesis | A Novel Joint Perceptual Encryption and Watermarking Scheme (JPEW) Within JPEG Framework

I MUHAMMAD IMRAN KHAN
(CAPITAL LETTERS)

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

Witnessed by

Signature of Author

Signature of Supervisor

Permanent address:
House No. 32, Street No. 53,
CAT-II, G-10/3,
ISLAMABAD, PAKISTAN.

Name of Supervisor
Assoc. Prof. Dr. Varun Jeoti

Date : 16-06-2011

Date : 16-06-2011

DEDICATION

Again,

To Humanity.

ACKNOWLEDGEMENTS

First of all I would like to thank my Father (**Imtiaz Ahmad Khan**), my Mother, my Sister (**Dr. Amna**) and my Brother (**Farhan Khan, Engr.**) for their support, care, continuous guidance and advice.

I would also like to express my sincere gratitude to my supervisor (**Dr. Varun Jeoti**), for his guidance, nurturing and encouragements. He has been supportive as well as critical at every stage of my research work, and I have learnt a lot from his broad knowledge, insight, kindness and patience. He has been a mentor to me, for without his guidance this research work would not have yielded such positive results.

I owe a debt of gratitude to my co-supervisor (**Dr. Aamir Saeed Malik**), for his continuous help and guidance throughout my research work.

Further, I would also like to acknowledge the support of the **Post Graduate office and Department of Electrical and Electronics Engineering at Universiti Teknologi PETRONAS, MALAYSIA**.

I would also like to acknowledge all the authors of open source codes, as well as the authors of the research work with which the presented work is compared.

ABSTRACT

Due to the rapid growth in internet and multimedia technologies, many new commercial applications like video on demand (VOD), pay-per-view and real-time multimedia broadcast etc, have emerged. To ensure the integrity and confidentiality of the multimedia content, the content is usually watermarked and then encrypted or vice versa. If the multimedia content needs to be watermarked and encrypted at the same time, the watermarking function needs to be performed first followed by encryption function. Hence, if the watermark needs to be extracted then the multimedia data needs to be decrypted first followed by extraction of the watermark. This results in large computational overhead. The solution provided in the literature for this problem is by using what is called partial encryption, in which media data are partitioned into two parts - one to be watermarked and the other is encrypted. In addition, some multimedia applications i.e. video on demand (VOD), Pay-TV, pay-per-view etc, allow multimedia content preview which involves 'perceptual' encryption wherein all or some selected part of the content is, perceptually speaking, distorted with an encryption key. Up till now no joint perceptual encryption and watermarking scheme has been proposed in the literature.

In this thesis, a novel Joint Perceptual Encryption and Watermarking (JPEW) scheme is proposed that is integrated within JPEG standard. The design of JPEW involves the design and development of both perceptual encryption and watermarking schemes that are integrated in JPEG and feasible within the 'partial' encryption framework. The perceptual encryption scheme exploits the energy distribution of AC components and DC components bitplanes of continuous-tone images and is carried out by selectively encrypting these AC coefficients and DC components bitplanes. The encryption itself is based on a chaos-based permutation reported in an earlier work. Similarly, in contrast to the traditional watermarking schemes, the proposed watermarking scheme makes use of DC component of the image and it is carried out by selectively substituting certain bitplanes of DC components with watermark bits.

Apart from the aforesaid JPEW, additional perceptual encryption scheme, integrated in JPEG, has also been proposed. The scheme is outside of joint framework and implements perceptual encryption on region of interest (ROI) by scrambling the DCT blocks of the chosen ROI.

The performances of both, perceptual encryption and watermarking schemes are evaluated and compared with Quantization Index modulation (QIM) based watermarking scheme and reversible Histogram Spreading (RHS) based perceptual encryption scheme. The results show that the proposed watermarking scheme is imperceptible and robust, and suitable for authentication. Similarly, the proposed perceptual encryption scheme outperforms the RHS based scheme in terms of number of operations required to achieve a given level of perceptual encryption and provides control over the amount of perceptual encryption. The overall security of the JPEW has also been evaluated. Additionally, the performance of proposed separate perceptual encryption scheme has been thoroughly evaluated in terms of security and compression efficiency. The scheme is found to be simpler in implementation, have insignificant effect on compression ratios and provide more options for the selection of control factor.

ABSTRAK

Disebabkan pertumbuhan yang cepat teknologi internet dan multimedia, banyak aplikasi komersial yang baru seperti Video-on-Demand (VOD), bayar dan tonton, siaran multimedia masa sebenar dll, telah muncul. Untuk menjamin integriti dan kerahsiaan kandungan multimedia, kandungan biasanya di watermark dan kemudian disulitkan atau sebaliknya. Jika kandungan multimedia perlu di watermark dan disulitkan pada masa yang sama, fungsi watermarking harus dilakukan dahulu diikuti oleh fungsi penyulitan. Oleh kerana itu, jika watermark perlu diekstrak maka data multimedia mesti dinyahsulit dahulu diikuti oleh ekstraksi watermark. Ini akan menyebabkan overhead pengkomputeran yang besar. Penyelesaian yang diberikan di sastera untuk masalah ini adalah dengan menggunakan apa yang disebut penyulitan separa, di mana data media di bahagikan menjadi dua bahagian - satu untuk menjadi watermark dan yang lainnya disulitkan. Selain itu, beberapa aplikasi multimedia iaitu video-On-demand (VOD), TV berbayar, bayar dan tonton, membolehkan pratonton kandungan multimedia yang melibatkan penyulitan persepsi dimana semua atau beberapa bahagian yang dipilih daripada kandungan, di distorsi dengan kunci penyulitan. Sehingga ke hari ini tidak ada gabungan penyulitan persepsi dan skim watermarking telah dicadangkan dalam kesusasteraan.

Dalam tesis ini, satu baru Joint Perceptual Encryption and Watermarking skim (JPEW) telah dicadangkan yang diintegrasi dalam standard JPEG. Rekaan JPEW melibatkan reka bentuk dan pembangunan kedua-dua penyulitan persepsi dan skim watermarking yang diintegrasi dalam format JPEG dan munasabah dalam rangka kerja 'separa' penyulitan. Skim penyulitan persepsi mengeksploit pengedaran tenaga komponen AC dan komponen DC bitplanes dan dilakukan dengan penyulitan selektif pekali AC imej berterusan nada komponen DC bitplanes. Penyulitan itu sendiri berdasarkan pada permutasi kekacauan berpusat dilaporkan dalam sebuah karya sebelumnya. Demikian pula, kontras dengan skim watermarking tradisional, skim watermarking yang dicadangkan memanfaatkan komponen DC dan ia dilakukan

secara selektif menggantikan bitplanes tertentu komponen DC dengan bit watermark. Selain dari JPEW di atas, enkripsi skim tambahan persepsi, di integrasi dalam format JPEG, juga telah dicadangkan. Skim ini di luar gabungan rangka kerja dan melaksanakan penyulitan persepsi di Region Of Interest (ROI) dengan perawakan blok DCT dari ROI yang dipilih.

Prestasi kedua-dua, skim penyulitan persepsi dan watermarking dinilai dan dibandingkan dengan skim Quantization Index Modulation (QIM) berdasarkan watermarking dan skim Reversible Histogram Spreading (RHS) berdasarkan penyulitan persepsi. Keputusan kajian menunjukkan bahawa skim watermarking yang dicadangkan adalah tak terlihat dan kukuh, dan sesuai untuk pengesahan. Demikian pula, skim penyulitan persepsi yang dicadangkan melebihi skim berasaskan RHS dalam jumlah operasi yang diperlukan untuk mencapai tahap tertentu penyulitan persepsi dan memberikan kawalan ke atas jumlah penyulitan persepsi. Keselamatan secara keseluruhan JPEW juga telah dinilai. Selain itu, prestasi skim penyulitan persepsi berasingan yang dicadangkan telah dinilai sepenuhnya dalam hal keselamatan dan kecekapan pemampatan. Skim ini ditemui lebih mudah dalam pelaksanaan, berpengaruh kurang signifikan terhadap nisbah pemampatan dan memberikan lebih banyak pilihan untuk pemilihan faktor kawalan.

TABLE OF CONTENTS

APPENDICES

List of Tables

List of Figures

List of Abbreviations

AC	Alternating Current
AES	Advance Encryption Standard
CF	Control Factor
CWE	Commutative Watermarking and Encryption
DC	Direct Current
DCT	Discrete Cosine Transform
DES	Data Encryption Standard
DFT	Discrete Fourier Transform
DPCM	Differential Pulse-Code Modulation
DPV	Discontinuity Point Vector
DWT	Discrete Wavelet Transform
EPR	Electronic Patient Report
FFT	Fast Fourier Transform
FGS	Fine Granularity Scalability
FLC	Fixed-Length Codeword
HVS	Human Visual System
IDCT	Inverse Discrete Cosine Transform
IDEA	International Data Encryption Algorithm
IFC	Image Fidelity Criterion
ITU	International Telecommunication Union
I-VOP	Intra-coded Video Object Plane
JPEG	Joint Photographic Experts group
JPEW	Joint Perceptual Encryption and Watermarking
JWE	Joint Watermarking and Encryption
MPEG	Motion Picture Experts Group
MRI	Magnetic Resonance Imaging
MSE	Mean Squared Error

MS-SSIM	Multi Scale - Structural SIMilarity
MVD	Motion Vector Difference
NCC	Normalized Cross-Correlation
PSNR	Peak Signal-to-Noise Ratio
QCWE	Quasi-Commutative Watermarking and Encryption
QIM	Quantization Index Modulation
RHS	Reversible Histogram Spreading
ROI	Region Of Interest
S-box	Substitution-box
SMLFE	Scalable Multilayer FGS Encryption
SNR	Signal-to-Noise Ratio
SPIHT	Set Partitioning In Hierarchical Trees
SSIM	Structural SIMilarity
SSLFE	Scalable Single-Layer FGS Encryption
SVD	Singular Value Decomposition
TAF	Tampering Assessment Function
TSH	Tree-Structured Har transforms
UQI	Universal Quality Index
VEA	Video Encryption Algorithm
VIF	Visual Information Fidelity
VIFP	Pixel based Visual Information Fidelity
VoD	Video on Demand
VSNR	Visual Signal-to-Noise Ratio
WPSNR	Weighted Peak Signal-to-Noise Ratio
ZoE	Zone of Encryption

CHAPTER 1

INTRODUCTION

1.1 Introduction

Due to the wide spread of internet technologies, past decades have witnessed enormous transmission of the multimedia content over the internet. This multimedia content sometimes is sensitive, valuable and indented only to be transmitted to its legal owner, which generates the need for the protection of this multimedia data. Multimedia security, and issues related to it, has, therefore, attracted many researchers to it. A huge amount of work in securing the multimedia content has been reported during the past decade after the development of the image and video compression standards. There is an extensive use of multimedia content like images, videos and audio on the internet. Due to this increase in transferring of visual data, there is a need to make sensitive content secure against any potential adversary. The protection of the multimedia content involves two major issues, firstly the security of the content during transmission and secondly the authentication, copyright and ownership protection. Multimedia encryption deals with the protection of multimedia content during the transmission over insecure channel, while watermarking deals with the issues related to the authentication and copyright protection of the multimedia content.

Lately, this growth in the multimedia technologies has also resulted in the development of some unique commercial applications like video on demand (VoD), pay-TV, pay-per-view etc. [1] that allow the users a multimedia content preview. These applications allow the degraded quality of the content to be available and to be viewed freely to attract the consumers. For example, a video (i.e. audio visual data) is

degraded to a poor quality, in order to allow its preview free of charge. If the consumer wants to watch higher quality video (original video) then the consumer has to pay for watching it. Perceptual encryption deals with this degradation of quality of the multimedia content to certain predefined level. Applications for perceptual encryption are further discussed in section 2.2.4.1.

The transmission of large amount of visual data, e.g. images and videos, via the internet also allows the illegal distribution of copyrighted visual data, as well as tampering of visual data that is sensitive in nature. The illegal distribution and tampering of data needs serious considerations. Solutions are being put forward by many researchers. Watermarking techniques are one of the possible solutions to the copyright protection, owner identification and authentication. A large amount of work has been reported in the past years [2] resolving the issues related with watermarking and its application. Almost all of the reported work on watermarking in Discrete Cosine Transformation (DCT) based compression standards has been done by manipulating the AC[1] coefficients, particularly using mid frequency or low frequency components. Furthermore, the DC[1] component has also not been given its due importance, as it is considered unsuitable for embedding the watermark for the reason that it will degrade the quality of the image or video thus creating a checker board effect, as the DC component is a perceptually significant component.

Nowadays, as majority of the data are transmitted in compressed form so there is also a need to address the encryption and watermarking techniques combined with compression standard to reduce computational overhead. Some encryption and watermarking techniques combined with compression standard i.e. JPEG, JPEG 2000, have also been reported.

Watermarking and encryption of the multimedia content e.g. image/video/audio, are carried out using separate functions. If the multimedia content needs to be watermarked and encrypted at the same time, first the watermarking function needs to be performed, followed by the encryption function. In this scenario, if the watermark

[1] AC (Alternating Current) and DC (Direct Current), these names come from historical use of DCT in electrical current analysis.

is to be extracted, then the multimedia data need to be decrypted followed by the extraction of watermark. Intuitively, this will result in large computational burden. The computational burden can be minimized if the watermarking and encrypting were independent of each other. In other words, both the functions of watermarking and encryption were commutative. *Lian et al*. provided the solution for this problem in [3] using what is termed as 'partial encryption'. The main idea is to partition the media data into two parts, one part is watermarked while the other is encrypted. However, a detailed joint scheme within the given compression framework is still desirable.

1.2 Motivation

It is always desirable that new techniques are developed that can make watermarking and encryption functions independent of each other. The main idea is to design a Joint and commutative DCT based Perceptual Encryption and Watermarking scheme within the JPEG compression framework. A thorough literature survey shows that a very little work has been done in the area of Joint Encryption and Watermarking of multimedia content. Whatever little has been done uses already existing techniques that are made compatible to each other in order to achieve both watermarking and encryption. Designing simpler such schemes can result in increased efficiency of overall system, and, furthermore, if these schemes work within the popular JPEG framework, these techniques will be more valuable.

The motivation for joint encryption and watermarking can be explained from the following:

- **Avoid Key from being compromised:** On the receiver's end, if an extraction of watermark is required (in the scenario where encryption of the content is followed by watermarking) then a decryption key is required to decrypt the content first, and then to extract the watermark. This will obviously abate the confidentially of encryption key.

- **Prevent leakage of the Content:** Considering the scenario mentioned in the point above, while extracting the watermark from the decrypted content with the key, also the content itself will be revealed.

- **Simultaneous Operation on same Multimedia Content:** Joint architecture / scheme allows simultaneous operations meaning that now the watermarking and the encryption functions both can be carried out at the same time.

- **Direct Operation on Encrypted Domain:** Joint scheme also allows the extraction and embedding of watermark on the encrypted domain thus no need of a decryption key.

- **Desirable in Real-Time Applications:** Because joint scheme simultaneous operations of watermarking and encryption, thus saving the time and decreasing the delay; that is introduced by encrypting the content first and then watermarking it or vice-versa.

There is no reported work on Joint Perceptual Encryption and Watermarking despite its significance in several multimedia applications. The internet is going commercial and applications with unique requirement of multimedia content preview sometimes may require both perceptual encryption and watermarking to protect the confidentiality, integrity as well as the copyrights of the content. Thus, a design of Joint Perceptual Encryption and Watermarking Scheme will be highly suitable under this scenario. Motivated by the above discussed reasons, a Joint Perceptual Encryption and Watermarking Scheme is proposed, which is commutative and works within the framework of JPEG compression standard. The proposed scheme is abbreviated as **JPEW** (**J**oint **P**erceptual **E**ncryption and **W**atermarking scheme).

The motivation behind choosing to work within JPEG compression framework, while several other compression frameworks exist, is because JPEG compression standard is the most widely and commonly used compression standard for still image compression. Secondly, the most commonly and widely used video compression

standard (i.e. MPEG 1, 2 and 4) are built upon JPEG, by including some special features to deal with other attributes in video (i.e. Motion Vector). The intra-frame coding in the MPEG which removes the spatial redundancies is, however, the same as JPEG. MPEG additionally performs inter-frame coding which removes temporal redundancies from the sequence of frames. The proposed joint scheme of perceptual encryption and watermarking is based on intra-frame coding, thus making the proposed scheme easily deployable on MPEG compression standard as well.

1.3 Objectives of the Research Work

The initial objective for the research work is to conduct a thorough literature survey on Joint Encryption and Watermarking Schemes, Perceptual Encryption Schemes and DC component based Watermarking Schemes. After completing the survey and identifying the potential work to be done, the objectives of the research work has been chosen to be the following two:

1. Designing a Joint Perceptual Encryption and Watermarking Scheme within the framework of JPEG compression standard. This Joint design can be further categorized as follows,

    A. To suggest a joint framework for commutative perceptual encryption and watermarking within the overall framework of JPEG.

    B. To design a novel Perceptual Encryption scheme that works within JPEG framework and is also compatible with joint watermarking scheme of item A.

    C. To design a novel Watermarking scheme that works within JPEG framework and is compatible with joint perceptual encryption scheme of item A.

2. Developing stand-alone Region-Of-Interest (ROI) based Perceptual Encryption schemes similar to the one designed for the joint scenario and having the same characteristics.

1.4 Scope and Methodology

The main aim of the conducted research work is to present the design of a Joint Perceptual Encryption and Watermarking technique on the popular image and video compression standards. The methodology followed in the development of the entire joint perceptual encryption and watermarking scheme can be split into three phases:

The first phase is focused on developing a joint framework that allows commutative design of perceptual encryption and watermarking within JPEG requirements. This is done by intelligently splitting the DCT data into two independent parts and carrying out perceptual encryption on one and the watermarking on another. In the second phase, the perceptual encryption scheme and also watermarking schemes are so designed that they contain an element of novelty. The third phase is where the performance of the proposed scheme is evaluated. This is preceded by a thorough literature survey on the methodologies of performance evaluation of both the perceptual encryption and watermarking schemes individually.

While presenting the existing schemes in this thesis, the variable names are kept same as in the corresponding publication for better understanding. For compatibility with JPEG compression architecture, the joint commutative design selects the data splitting at DCT level. The actual DCT data partitioning is, however, carried out by statistical analysis of continuous-tone still images. For the purpose of simplicity and better understanding, and to mimic the still frames of videos, continuous-tone grey scale still images are used in the experiments. Based on the outcomes of the statistical analysis certain AC coefficients and most significant DC components bit-planes are selected for perceptual encryption, and for watermarking, certain least significant bit-planes of DC coefficients are selected. Thus, a perceptual encryption scheme is

designed, utilizing the AC coefficients and most significant bit-planes of the obtained media data. The scheme is so designed that it allows for controlled amount degradation in the content using a control factor. A design-curve is developed using Objective Image Quality Assessment Metrics (IQA's) – the newly emerging metric for measuring degradation. The proposed scheme strives to achieve linear progressive degradation by using the proposed control factor. The perceptual encryption itself is based on a chaotic scrambler that acts like a key-enabled S-Box proposed in the literature. After that, a watermarking scheme is formulated by exploiting the fact that DC coefficient has the largest energy in the DCT block, which means more choice of media data that can be manipulated in order to insert a watermark.

For the performance evaluation of this type of joint scheme, no standard way has been chalked out yet as there are very few joint encryption and watermarking schemes proposed in literature. However, the performance evaluation of the separate schemes has been discussed in the literature. Thus, for the proposed scheme, its performance is evaluated from watermarking perspective and perceptual encryption perspective. For the watermarking scheme, the imperceptibility, payload and robustness need to be assessed. And for perceptual encryption scheme, security and compression efficiency are the most important attributes in the proposed scheme that need to be assessed. Compression Efficiency or compression analysis in encryption scheme was not given much of importance in literature. However, it is necessary to assess the compression efficiency of an encryption scheme when it is integrated in compression standard. The most important aspect of the proposed scheme is the security that is evaluated differently as compared to plain schemes. All of these aspects are discussed in this thesis. The thesis is focused on perceptual aspects as it is dealing with multimedia content rather than the cryptographic aspects. Other main concern of the thesis is the perceptual security which is also discussed; the cryptographic security that is associated with the adapted chaotic scrambler is not discussed in detail. As for watermarking, the robustness is assessed by placing the watermarked image under common image processing attacks i.e. salt & pepper noise, Gaussian noise etc. The imperceptibility of the Watermarking scheme is measured using IQA’s.

All the obtained results of experiments and the evaluation are carried out at simulation level using MATLAB and the hardware validation is kept out of the scope of the proposed work.

1.5 Thesis Structure / Outline

The conducted research work is consolidated in two parts: part I comprising chapters 3 and 4 concentrates on the joint perceptual encryption and watermarking scheme, and part II consisting of chapters 5 and 6 mainly focuses on the a separately proposed stand alone perceptual encryption scheme.

The thesis is organized in the following manner: Chapter 1 introduces the thesis, presenting the motivation behind this research work, the objectives of the proposed research work, the brief methodology and scope.

Chapter 2 is focused on introducing the field of multimedia security, followed by the detailed background and preliminaries of the research work which paves the path to understand the work presented in later chapters. A through critical literature survey within the scope of this research work is presented that highlights the general academic issues that need to be addressed in order to realize the design of the proposed schemes.

Chapter 3 proposes the joint and commutative framework for Perceptual Encryption and Watermarking which complies with JPEG compression standard. It is followed by the presentation of the design of individual schemes themselves in detail.

Chapter 4 presents the results of the proposed joint perceptual encryption and watermarking scheme proposed in the previous chapter. Performance evaluation for the entire scheme is also presented in this chapter. Both chapters 3 and 4 cover the first part of the presented work.

In chapter 5, a separate design for the Perceptual Encryption Scheme is presented. The scheme is Region of Interest based on DCT block scrambling.

In chapter 6, the performances of the perceptual encryption scheme presented in chapter 5 is evaluated, as well as the results of this scheme is also presented and discussed in this chapter. Chapters 5 and 6 cover the second part of the research work.

Lastly, chapter 7 concludes all the presented work and also outlines the direction for future work.

Appendix A demystifies the proposed chaotic scrambler used in the research work and presents the working of the scrambler.

In Appendix B, brief interpretations of the used Objective Image Quality Assessment metrics are presented.

Appendix C shows the examples of the popular Continuous-Tone Grey-Scale Standard Test Images used in this work.

This page is intentionally left blank Chapter 2 starts from next page.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

To facilitate further discussion on Multimedia Content Encryption, Watermarking, and Joint / Commutative Encryption and Watermarking schemes and on their architecture, methodologies and techniques, a brief introduction and background about Multimedia Content Encryption and Watermarking, their classification, usage / applications and some popular techniques along with the feature and requirements to design new schemes and the issues related to them is presented in later sections of this chapter. The literature review thoroughly covers the schemes based on DCT in order to relate the proposed schemes with the previously reported work in the literature although the other transformation based schemes are discussed also for better understanding of the ideas.

2.2 Multimedia Content Encryption

Multimedia Content Encryption techniques provide ways to secure the transmission of the multimedia content over the insecure channel or in other words the challenge of keeping the multimedia content out of the reach of eavesdroppers. Usually the insecure channel or media is the internet or any other multimedia network. The general scenario of the multimedia encryption is shown in Fig. 2.1.

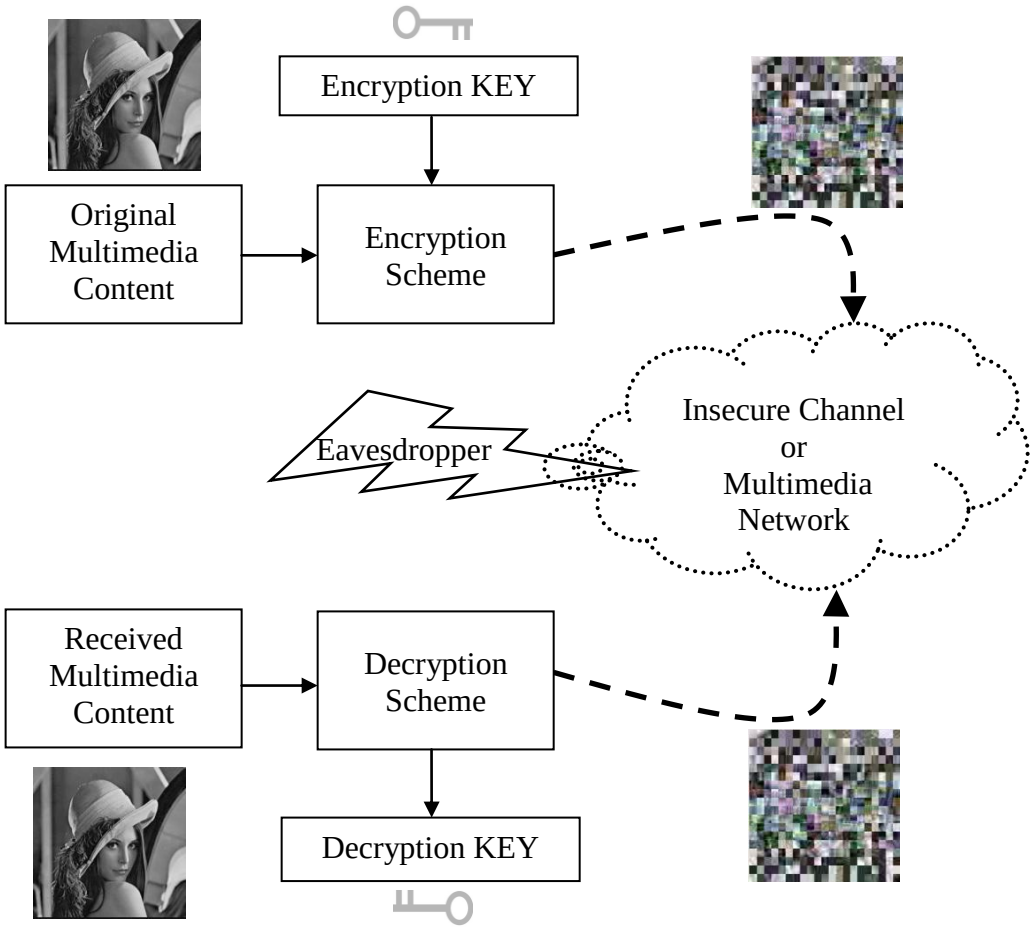


Figure 2.1: A Typical Multimedia Encryption and Decryption Scenario

2.2.1 Classification

The multimedia encryption schemes can be classified into different categories depending upon how the encryption is being done and under what constraints it is being done. Also the encryption schemes can be differentiated according to their properties, i.e. the domain in which the encryption is carried out, and the application for which the multimedia content is being encrypted.

To clarify the classifications, a classification tree for the multimedia content encryption is presented as shown in Fig. 2.2.

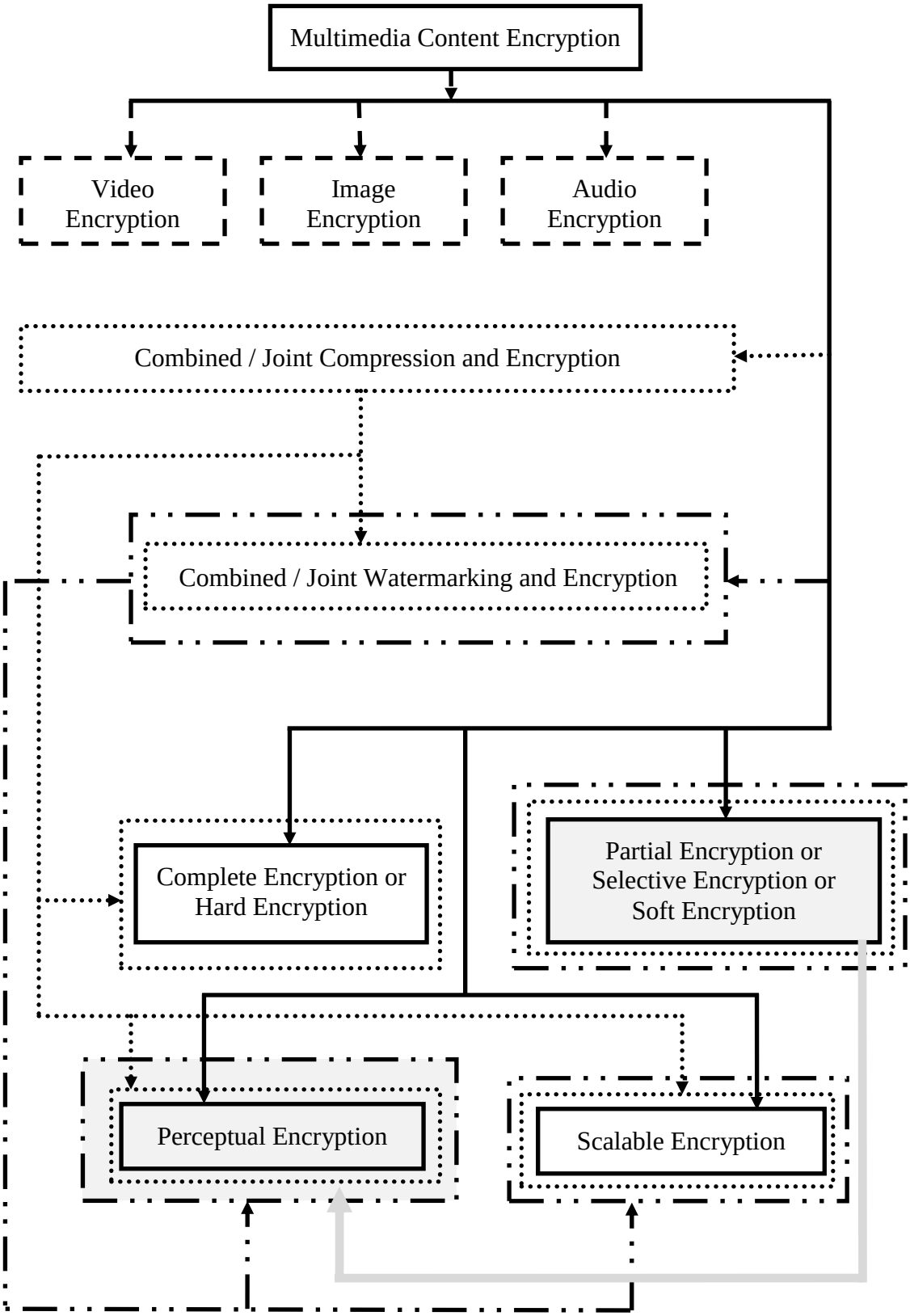
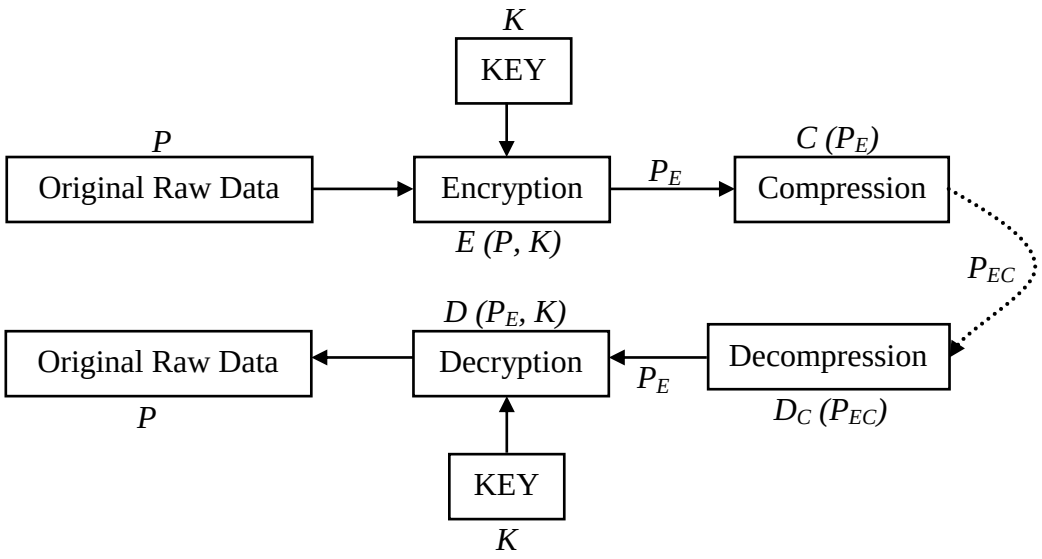


Figure 2.2: Classification of Multimedia Content Encryption Schemes

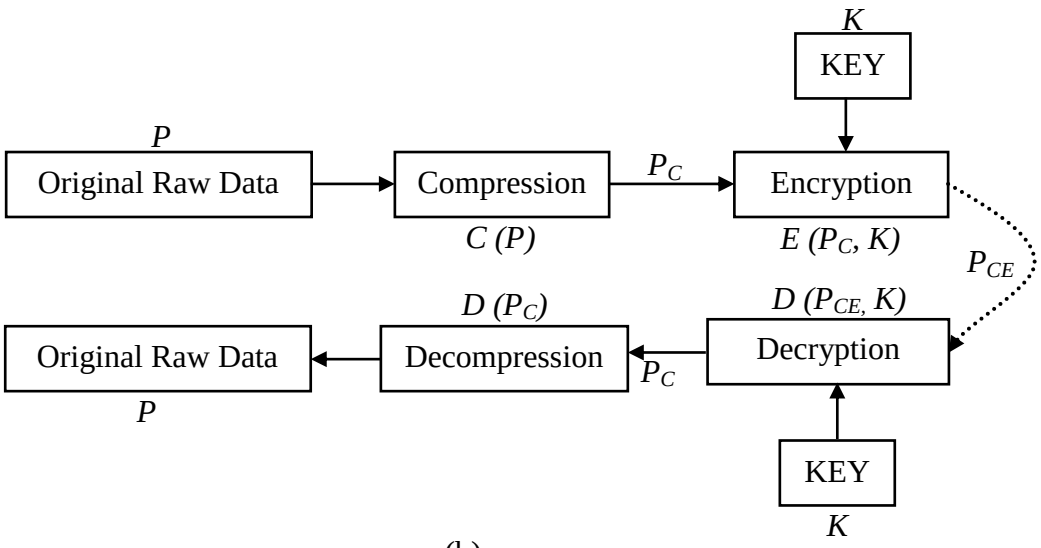
2.2.2 Complete / Hard Encryption

Multimedia content (audio, video or image) is encrypted using traditional ciphers like Advance Encryption Standard (AES) [4], Data Encryption Standard (DES) [5] and International Data Encryption Algorithm (IDEA) [6] etc. irrespective of the format of the data that has to be encrypted [7-11]. This can also be referred as naïve approach. However, complete encryption can be performed in various ways either first the raw data is encrypted and then compressed or the compressed data is encrypted. Albeit computationally costly, complete encryption schemes are more secure.

Complete encryption can be conceptualized from the block diagram shown below in Fig 2.3. In Fig 2.3(a) the original raw multimedia data (P) first undergo encryption using encryption function (E) to get encrypted data (P_E) using the key (K) and then compression function (C) is applied on the encrypted data to get compressed data (P_{CE}). Similarly, to get original data, first the compressed data needs to be decompressed using function (D_C), to get encrypted data (P_E). Then using decryption function (D) and the key (K), the decompressed data is decrypted to get the original multimedia raw data (P). Fig 2.3(b) shows the case where compression is done prior to encryption.



(a)



(b)

Figure 2.3: A scenario for (a) Encryption before Compression
(b) Compression before Encryption, of Multimedia Content

2.2.2.1 Draw Backs of Complete Encryption Schemes

Considering the first case in which the raw data is first encrypted and then compressed, an encryption operation will change the location or values of the pixels which will result in the change of correlation between the pixels. This change in statistical distribution of the pixel values affects the compression ratios. Therefore compression after encryption is not considered suitable keeping inconsideration the compression efficiency. On the other hand if the data compression is performed first and followed by encryption, although the bit stream that needs to be encrypted will be reduced but it will offer less secrecy [12].

2.2.3 Partial / Selective / Soft Encryption

Partial Encryption[2] schemes are the algorithms that only encrypt some selected part of the multimedia data and the rest of the data remains unchanged. The encryption

[2] The term partial encryption, selective encryption and soft encryption are interchangeable in literature.

algorithm used to encrypt the selected part of the data can be any traditional encryption algorithm or can be a specifically designed algorithm for multimedia data. Nowadays partial encryption schemes are mostly used in multimedia encryption which will be discussed in further sections. Fig. 2.4 presents the basic idea of partial encryption scheme for multimedia content. As shown in the Fig 2.4, only the significant data is selected and encrypted the rest of the data is unchanged. Similarly, when decrypting the content only the selected encrypted data is decrypted.

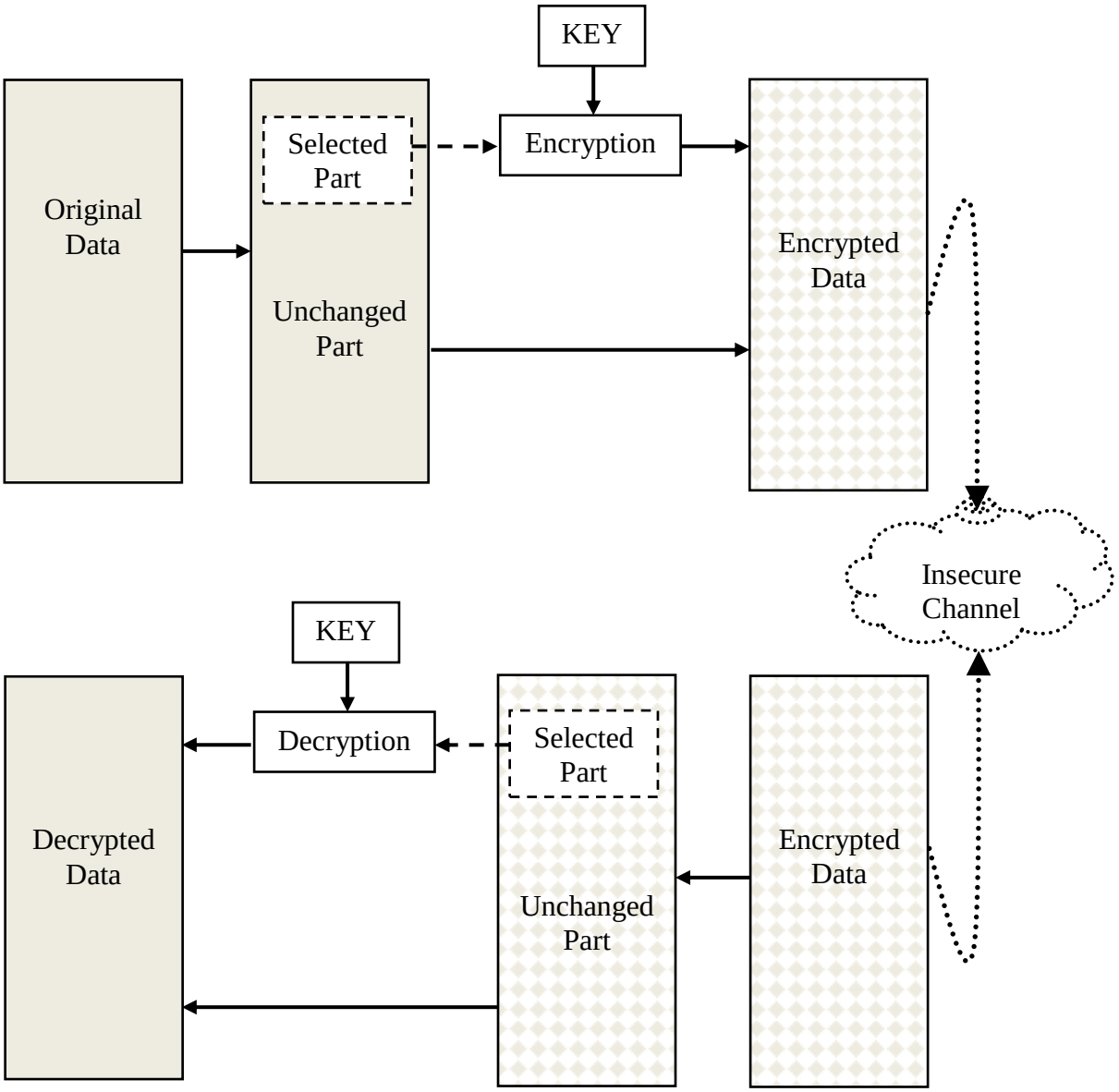


Figure 2.4: The Partial Encryption and Decryption Process for Multimedia Content

Mathematically partial encryption can be realized as follows, let M be the multimedia content, where M can be partitioned in to n parts i.e. M_0, M_1, M_2, M_3... M_n. For the encryption of the content,

$C_i = E_i (M_i, K_i)$, where $i = 0, 1, 2, 3, 4 \ldots n$. (2.1)

In the case where the same key is used to encrypt all the part of the multimedia data then
$K_i = K$. Similarly for the decryption process the equation will be,

$M_i = D_i (C_i, K_i)$, where $i = 0, 1, 2, 3, 4 \ldots n$. (2.2)

C_i, E_i, D_i, K_i are the encrypted i^{th} part of the multimedia content, the cipher used to encrypt the portioned (M_i) media data, the decryption algorithm used to decrypt the partitioned media data and the key used to encrypt and decrypt the media data, respectively.

2.2.3.1 Selection and Partitioning of the Multimedia Content

The identification of the part that needs to be encrypted needs serious consideration, while keeping the security aspects in view which includes the perceptual security, parametric security and the cryptographic security. The issue is that the encrypted data should be sufficient to make the content unintelligible. The remaining data / unencrypted part should be insufficient and should not aid in the recovery of the encrypted data. The other aspect is the trade-off between the amount of data encrypted (efficiency) and the security. Although the main objective of partial encryption is to reduce the overhead of encrypting the whole content, by only encrypting some of the parameters / parts of the content, in particular some specific significant part, to achieve the goal and to make the content secure and fulfilling the requirement of perceptual security. Other than these aspects the independence of the unencrypted part on the encrypted part is also necessary.

Another issue that arises is: how to partition the data? The partitioning of the data is subjected to the compression standard used and which multimedia content

needs to be encrypted. The partitioning is based on the compression standard used to compress the content and also the type of content i.e. Audio, Video and Images.

Table 2.1: Table showing which part of the content that can be Partially Encrypted (Partitioning of the Content) in different compression schemes and types of multimedia data

Mutimedia Content/ Domain	**Compressed**	**Uncompressed**
Image	AC Coefficients, Sign of AC Coefficients, DC Coefficients (in DCT Based Compression standard - JPEG) Sign of the Coefficients, Coefficients in each frequency sub-band [13] (in Wavelet based codecs i.e. JPEG 2000, SPIHT[3])	Bitplanes and Foreground / Background Objects [14]
Video	I-Frames, Motion Vector Difference (MVD), Intra-frame Encryption same as Encryption of DCT based compressed images	Usually Transferred in compressed domain to save bandwidth
Audio	FFT parameters, Huffman codes	Usually Transferred in compressed domain to save bandwidth

2.2.3.2 Review of Partial / Selective / Soft Encryption Schemes

In the literature there are many proposed encryption schemes with their pros and cons depending upon the application for which they are used. Here we have evaluated some of the partial encryption schemes that fall under the scope of the conducted research work.

[3] Set Partitioning in Hierarchical Trees (SPIHT) for more information on this compression standard see [15] and [http://www.cipr.rpi.edu/research/SPIHT/].

Scheme 1: Authors: This Encryption Algorithm was developed by Marc Van Droogenbroeck and Raphaël Benedett at Montefiore B-28, Department of Electricity, Electronics and Computer Science, Sart Tilman, B-4000 Liège, Belgium and was published in [Techniques for a Selective Encryption of Uncompressed and Compressed Images – Year 2002], [16].

The Proposed Scheme: A selective[4] encryption or soft encryption scheme for uncompressed images is proposed, in which the image is decomposed into 8 bitplanes (i.e. i_7, i_6, i_5, i_4, i_3, i_2, i_1, i_0). One by one, starting from the least significant bitplane up to the most significant bitplane, is encrypted. Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) is used as a metric to measure the distortion introduced in the encrypted images. Linear relationship has been shown between the PSNR values and the number of encrypted bitplanes. Also a method to encrypt JPEG compressed images is proposed in this paper, where the appended bits (specify the sign and magnitude of non-zero coefficients) of selected AC coefficients are encrypted. In JPEG compression standard, the appended bits are the bits that are representing the (AMPLITUDE) symbol followed by (RUNLENGTH, SIZE) symbol. The metrics used to measure the encrypted image quality are only MSE and PSNR. Classical encryption algorithms, like DES, triple DES and IDEA, are used to encrypt selected data.

Scheme 2: Authors: This Encryption Algorithm was developed by Martina Podesser, Hans-Peter Schmidt and Andreas Uhl at School of Telematics & Network Engineering Carinthia Tech Institute, Klagenfurt, AUSTRIA and was published in [Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environments – Year 2002], [14].

The Proposed Scheme: In this paper, another selective encryption approach is proposed to secure uncompressed image data transmission in mobile environment. In the proposed scheme the image is divided into 8 bitplanes, and starting from the most significant bitplane, each bitplane is encrypted. As stated, the minimum of

[4] The term selective encryption is sometimes interchangeable with partial encryption as the idea behind these techniques is the same.

12.5% of the data, which is equivalent to one bitplane, needs to be encrypted, to distort the image. PSNR is again used as a metric to measure the level of encryption and classical encryption algorithm like AES (Advanced Encryption Standard) is used for encryption purposes. The proposed scheme is designed for partially encrypting uncompressed images.

Scheme 3: Authors: This Encryption Algorithm was developed by Wenjun Zeng and Shawmin Lei at Sharp Laboratories of America, Inc. 5750 NW Pacific Rim Blvd. Camas, WA 98607 and was published in [Efficient frequency domain selective scrambling of digital video – Year 2002], [13].

The Proposed Scheme: A number of simple and efficient frequency domain encryption techniques like selective bit scrambling, block shuffling and block rotation for videos are proposed in this paper. The proposed techniques are for both, wavelet based system and DCT based system. For DCT based system the techniques includes sign bit encryption and motion vector scrambling. One of the advantages of the proposed methods is that they have an insignificant effect on compression ratio.

Scheme 4: Authors: This Encryption Algorithm was developed by J.M. Rodrigues, W. Puech at Laboratory LIRMM, UMR CNRS 5506, University of Montpellier II 161, rue Ada, 34392 MONTPELLIER CEDEX 05, FRANCE and A.G. Bors at Dept. of Computer Science, University of York, YORK YO10 5DD, U.K. and was published in [Selective Encryption of Human Skin in JPEG Images – Year 2006], [17].

The Proposed Scheme: In this paper, a selective encryption of human skin in JPEG compressed images is proposed. In the proposed technique, firstly the skin is detected in the image, then the amplitude part of the selected number of AC coefficients corresponding to the skin part in the DCT Blocks is encrypted with AES cipher.

Scheme 5: Authors: This Encryption Algorithm was developed by Li Weng and Bart Preneel at Department of Electrical Engineering, Katholieke Universiteit Leuven, 3001 Heverlee, Belgium and was published in [On Encryption and Authentication of the DC DCT Coefficient – Year 2007], [18].

The Proposed Scheme: It is showed in this paper that, about 60% of the information is guaranteed by authenticating the DC coefficient and 80% of the information can be hindered by encrypting the DC coefficient. A set of experiments was performed in this paper to show that how much information the DC coefficient possesses. The paper states that the SSIM score was 0.7 when leaving the first AC coefficient and DC coefficient together, and setting all the coefficients equal to zero. Another experiment was done by randomly flipping the sign bits of the DCT coefficients which resulted in SSIM value of 0.5.

Scheme 6: Authors: This Encryption Algorithm was developed by C. Narsimha Raju, Kannan Srinathan and C. V. Jawahar at International Institute of Information Technology Hyderabad, India – 500032 and was published in [A Real-Time Video Encryption Exploiting the Distribution of the DCT coefficient – Year 2008], [19].

The Proposed Scheme: A real-time video encryption scheme is proposed in frequency domain. Where the first 10 DCT coefficients in 8×8 DCT block (DC and first 9 AC's), are first XOR with the random numbers generated by Pseudo-Random Number Generator (PRNG). For DC coefficients, the PRNG generated values fall in the range of 50 to 255, because DC coefficient has higher values and for AC coefficients the values fall in between 0 to 30. After that in the next step, a 1×64 vector is generated by PRNG to permute the DCT coefficients within the macro block. In this paper, the experiment showed that 86.53% of the DC values fall in 50-255 and 96.94% of the AC values fall in 0-30. A maximum of 23.41% of increase in the video size was introduced by the proposed encryption scheme, and it encrypted

one frame in average of 7.2 milliseconds. The proposed scheme encrypts the whole DC coefficient and also the perceptual quality has not been measured.

2.2.4 Perceptual Encryption

Perceptual Encryption deals with the degradation of the quality of multimedia content according to desired requirements. Traditional cryptographic schemes or encryption schemes do not provide the perceptual degradation, they deal with the complete encryption / complete degradation of the content. Perceptual encryption in other words is generalization of partial encryption and is carried out by encrypting selected sensitive parameters of the media data. The selection of the parameter in the media data such that it introduces gradual degradation in the content is also an issue. The notion for the design of the perceptual encryption scheme was first presented in [20] as shown in the Fig. 2.5.

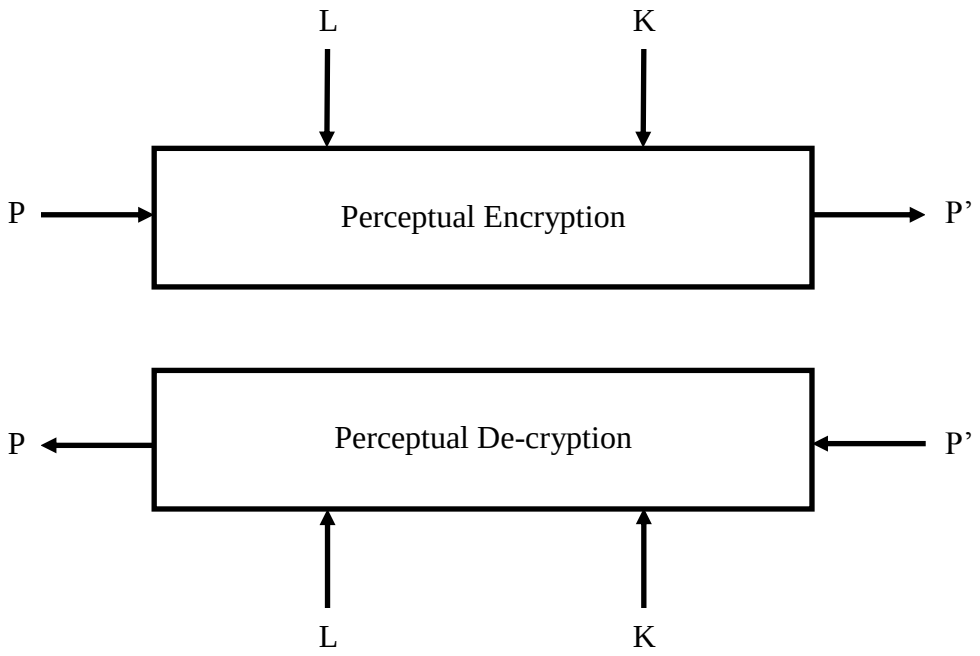


Figure 2.5: Perceptual Encryption and Decryption Process for Multimedia Content

where *P*, *L*, *K* and *P'* are the multimedia data, quality loss factor, the key used and the encrypted multimedia data, respectively. The quality loss factor or the level of encryption controls the amount of degradation in the content. In the literature, at some places, perceptual encryption is referred to as transparent encryption but transparency in actuality refers to the property of the format-compliance [21]. So a perceptual encryption algorithm should be transparent encryption algorithm for the particular codec.

2.2.4.1 Applications of Perceptual Encryption/Cryptography

The immense growth in multimedia technologies has resulted in many commercial applications. Many of these commercial applications involve perceptual encryption. Some of the applications are stated below:

- Live Video Broadcasting.
- Publishing Encrypted Images (Art-Work Image Vending).
- Recording encrypted bit-streams on CD-ROM or DVD-ROM.
- Video / Audio on Demand systems.
- Pay-TV (Pay per view) / Pay-Music / Interactive TV
- Wireless / Mobile Multimedia.
- Confidential Video Conferencing.
- Preview from the physical media (DVD, CD-ROM) when used in an unauthorized device [20].

Perceptual encryption schemes, those are published in the literature are presented in next section. These are the available perceptual encryption scheme for audio, video and images up to date, to the best of our knowledge. Some of the selective encryption schemes can also be considered as generalized idea for perceptual encryption. However, for these selective encryption schemes the control factor which controls the level of the degradation is not discussed.

2.2.4.2 Review of Perceptual Encryption Schemes

A survey on available perceptual encryption schemes is presented. Up to the best of our knowledge these are all the schemes within our scope of research work, published in the literature.

Scheme 1: Authors: This Perceptual Encryption Algorithm was developed by Andres Torrubia at Trymedia Systems, Inc. and Francisco Mora at Universidad Politecnica de Valencia and was published in [Perceptual Cryptography of JPEG Compressed Images on the JFIF Bit-Stream Domain – Year 2003], [20].

Codec Compliance: **JPEG/JFIF compressed bit-streams (JPEG Compressed Images)**

The Proposed Scheme: In this paper, a notation for perceptual cryptography[5] is presented that is compliant with JPEG compression standard. The parameter, quality loss factor (that is also referred as the control factor in the further presented perceptual encryption schemes), was introduced. The idea was to selection a *ZoE* (Zone of Encryption), which is encrypted using a key *k*. This encryption is carried out by selecting the AC coefficients that fall in *ZoE* and the alternating Huffman codewords are encrypted using the key '*k*'. Although a complete explanation on how these code words are encrypted and how the quality is measured are not discussed in the publication.

However the main idea proposed is to encrypt the selected part in the content to degrade its quality instead of degrading its quality as a whole. A complete design is not given which enables the selection of the control or quality loss factor.

[5] The terms perceptual encryption and perceptual cryptography are interchangeable.

Scheme 2: Authors: This Perceptual Encryption Algorithm was developed by Shiguo Lian, Jinsheng Sun, Zhiquan Wang at Department of Automation Nanjing University of Science and Technology, Nanjing, P.R China and was published in [Perceptual Cryptography on SPIHT Compressed Images or Videos – Year 2004], [22].

Codec Compliance: **SPIHT Compressed Images or Videos**

The Proposed Scheme: The proposed scheme is for SPIHT (Set Partitioning in Hierarchical Trees) compression standard, is wavelet based standard and is an upgraded form of EZW (Embedded Zerotree Wavelet). The proposed scheme consists of three steps: first after the wavelet decomposition, a number of coefficients are selected to be confused. Secondly, the selected coefficients are confused, and thirdly, the coefficient's signs are encrypted using chaotic cipher. The security analysis along with the analysis of compression efficiency have been carried out and found to change the compression ratio slightly and was secure.

Scheme 3: Authors: This Perceptual Encryption Algorithm was developed by Shiguo Lian, Jinsheng Sun, Zhiquan Wang at Department of Automation Nanjing University of Science and Technology, Nanjing, P.R China and was published in [Perceptual Cryptography on JPEG2000 Compressed Images or Videos – Year 2004], [23].

Codec Compliance: **JPEG2000 Compressed Images or Videos**

The Proposed Scheme: The proposed scheme is compliant with the JPEG2000 compression standard. The scheme consists of four steps which are Encryption strength computing (Control Factor / Quality loss factor), Sign encryption, Bitplane permutation and Inter-block permutation. In step one, the quality factor is determined using the equations given in [23]. In the second step, the sign of the transformed wavelet coefficients are encrypted using a chaotic stream cipher. The signs of the wavelet coefficients forming a sequence of bits are XORed (modulated)

with the sequence generated by the chaotic cipher. In the third step, the bitplanes are permuted using column as a unit (see [23] for more details of the generation of the bitplanes). In the last step, the code blocks are permuted. These code blocks are generated by partitioning the sub-bands; the purpose of generating these code blocks is to perform the coding process individually on each code block. Also, the proposed scheme was found to be robust under brute force attack.

The proposed scheme involves three parameters to degrade the quality of the content which increases the computational cost of the algorithm. Nevertheless the degradation in the content can be introduced using lesser number of parameters to obtain similar results.

Scheme 4: Authors: This Perceptual Encryption Algorithm was developed by Shiguo Lian, Jinsheng Sun, Zhiquan Wang at Department of Automation Nanjing University of Science and Technology, Nanjing, P.R China and was published in [Perceptual Cryptography on MPEG Compressed Videos – Year 2004], [24].

Codec Compliance: **MPEG Compressed Videos**

The Proposed Scheme: Like the previously discussed schemes, this scheme also consists of five steps. The first step is the encryption strength control in which the number of parameters to be encrypted is determined in order to get the desired level of encryption. In the second step, the DCT coefficients are divided into subsections, and then are encrypted within each subsection. This is done to avoid the increase in compression ratio, as small coefficients and coefficients with large value will not intermix. The DC coefficient is not included in any subsection of DC coefficients, and is excluded from the encryption process. The encryption of DCT is carried out for I-frame and intra-macro block of P/B frames. In the third step, similar to the previously proposed scheme, the signs of the DCT coefficients are encrypted using a chaotic cipher. This step is carried out for I-frame and intra-macro block of P/B frames. In step four, for I-frames the luminance plane and chrominance planes is confused (see [24] for more details). In the last step, the sign of the motion

vector is encrypted. The proposed scheme is shown secured on the point that the multimedia encryption scheme is considered secure if the time required to break the encryption scheme is more than the time for which the multimedia content is valuable.

In the proposed scheme, the perceptual quality of the content is not measured which results in undefined level of perceptual encryption. Although the quality factor (strength control of encryption) is determined but the degradation using that control factor may not always be gradual.

Scheme 5: Authors: This Perceptual Encryption Algorithm was developed by Shiguo Lian, Jinsheng Sun, Zhiquan Wang and was published in [Perceptual MPEG4 Video Encryption and Its Usage in Video-on-Demand Systems – Year 2004], [25].

Codec Compliance: **MPEG 4 Compressed Videos**

The Proposed Scheme: Similar to previously discussed schemes, a perceptual encryption scheme is proposed in this publication. Again the strength of encryption is determined in the beginning. In MPEG 4 each I-VOP (Intra-coded Video Object Plane) is decomposed into code blocks where each code block is coded from least significant bitplane to most significant bitplane. These bitplanes are also encrypted partially along with the encryption of the signs of the motion vector. The performance is then analysed in terms of Security in general, Computational Complexity and Direct Bit-Rate Control. The other aspects of security (perceptual and parametric security) were not discussed. However, the scheme is said to be suitable for real-time applications.

Scheme 6: Authors: This Perceptual Encryption Algorithm was developed by Shujun Li, Guanrong Chen, Albert Cheung, Bharat Bhargava, and Kwok-Tung Lo and was published in [On the Design of Perceptual MPEG-Video Encryption Algorithms – Year 2007], [21].

Codec Compliance: **MPEG Compressed Videos**

The Proposed Scheme: The proposed scheme is the extension of Video Encryption Algorithm (VEA) [26], and is known as perceptual Video Encryption Algorithm (PVEA). In the proposed scheme, FLC data elements are selectively encrypted. The last four data elements in FLC are selected only, to be encrypted and these correspond to the intra DC coefficients, sign bits of non-intra DC coefficients and AC coefficients, ESCAPE DCT coefficients and sign bits, and residuals of motion vectors. The proposed scheme is found secure.

Another perceptual scheme is proposed for audio in [27], following the same concept of perceptual encryption as proposed in [20].

2.2.5 Scalable Encryption

Encryption algorithms those support bit rate conversion, in other words those encryption algorithms which allows direct operation on the bit stream without decoding and decrypting the bit stream in order to adjust according to the bit rate. This happens when the multimedia content is transmitted on a bandwidth-limited network then the bit stream is cut down to adopt the bitrate. A few of the scalable encryptions schemes in the literature are [28-30].

In the scheme proposed in [28], the content in the transform domain was divided into three layers i.e. base layer, middle layer, enhancement layer. The middle layer and the enhancement layer were encrypted in the scheme based on the assumption that the base layer is granted to be delivered. In [29], two scaleable encryption algorithms are proposed i.e. Scalable Single-Layer FGS Encryption (SSLFE), Scalable

Multilayer FGS Encryption (SMLFE). First scheme encrypts Fine Granularity Scalability (FGS) stream using both selective encryption as well as complete encryption. In the second scheme, the FGS stream is partitioned in to multiple layers and then encrypted.

2.3 Watermarking

"Watermarking" ensures the integrity of the multimedia content. It is also used for hiding copyright messages in the multimedia content, as well as to detect illegal tampering. Watermarking is a newly emerging field, but because of increasing multimedia communications over the internet (which is an insecure medium of transmission), the heavy demands of industries, the need of multimedia security and to protect intellectual property, watermarking is attracting the attention of the researcher community.

A general watermarking framework consists of two main steps: i) Watermark embedding and ii) watermark extraction. Other steps that are involved are generation of watermark, distribution of watermarked content and the comparison (decision) stage. First the watermark is generated, in some cases, using pseudo number generator. Then in watermark embedding process, the watermark is inserted into the host image. After that, the watermarked image is distributed over the network. Then the watermark extraction process occurs in which the watermark is recovered. The recovered watermark is then compared with the already existing watermark to see if both watermarks match or not. A typical watermarking scenario is shown in Fig. 2.6.

2.3.1 Applications of watermarking

There are several applications which involve watermarking. Each watermarking application has its own requirements. Some of the popular watermarking applications are as follows.

2.3.1.1 Multimedia Content Authentication

In the digital world it is easy to tamper an image using the modern image processing tools, which are widely available. The problem is how to make sure that the multimedia content is not being tampered? Watermarking can be a solution to detect if any modification has been made in the multimedia content. In other words, watermarking guarantees the genuineness of the image. In this case, a fragile watermarking technique (described in section 2.3.3.6) should be used so that if a modification is made, the watermark will be destroyed or altered which will indicate the corresponding changes.

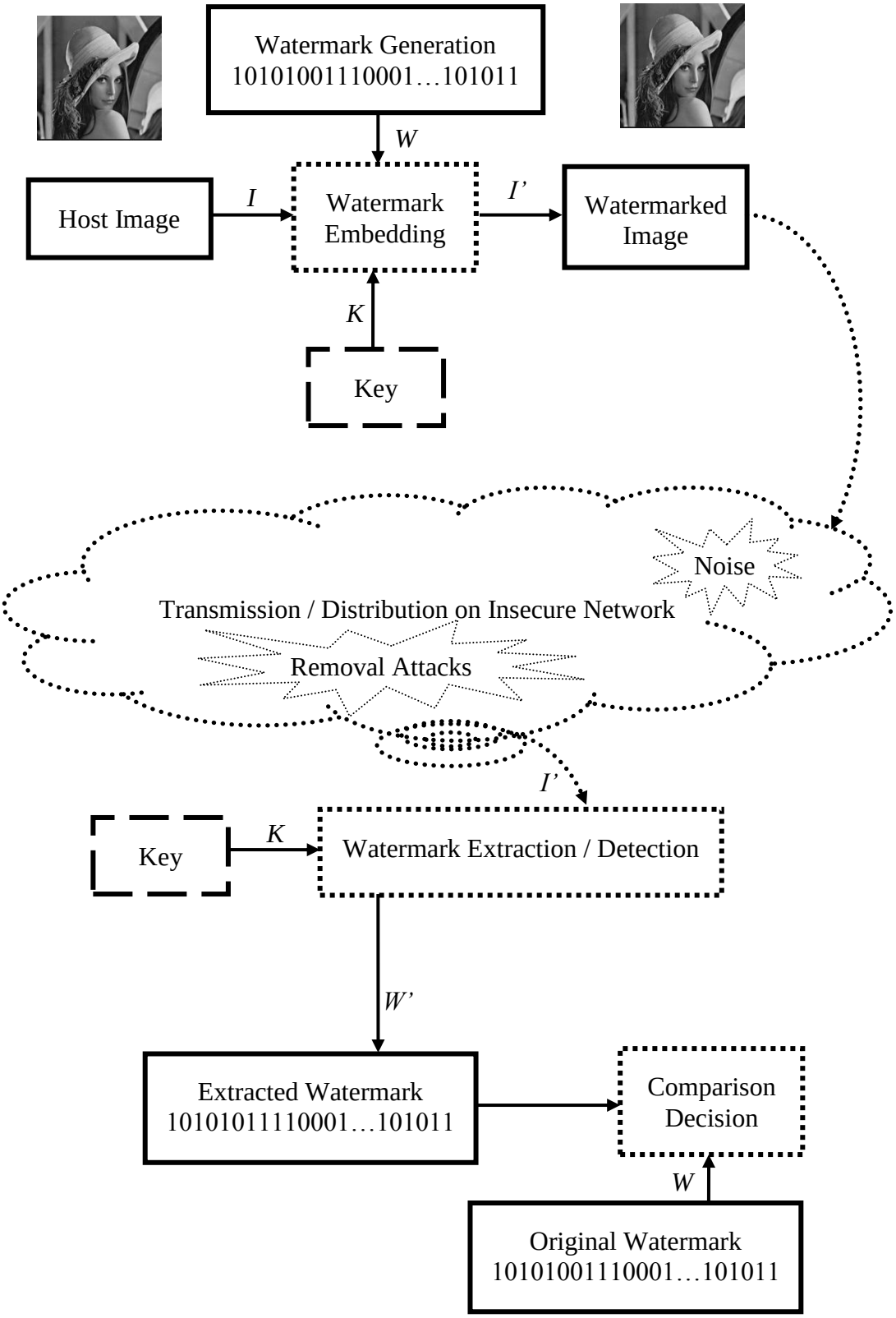


Figure 2.6: A Typical Watermarking Embedding and Extracting Scenario – in which the Watermarked Image is Transferred / Distributed on Insecure Network

2.3.1.2 Broadcast Monitoring

Watermarking can be used as an active technique to monitor the broadcast on the television networks in order to verify if the commercials are aired for the time that they have been paid for. Even though it is possible to engage a human observer who will monitor the number of time the commercial has been on aired, this method is costly and prone to human error. A better alternative is to use computer based monitoring system, which is further categorized into passive monitoring and active monitoring. In passive monitoring systems, the transmitted signal is compared with the signals (commercials) that already exist in the database. But maintaining a database is an expensive task and also the comparison is a computationally expensive task due to the large volume of multimedia contents. Another problem is that the transmitted signal is degraded to some level during the transmission process so an exact match search will not work in this case, one should perform a nearest neighbour search which will increase the computational cost. In the active monitoring system, a signal (or identification code) is embedded in the transmitted signal and that signal is compared. Watermarking is an alternative in the active monitoring systems, where the watermarks can be compared and counted in the broadcast.

2.3.1.3 Copyright protection

The most common of the watermarking application is the copyright protection. The watermark for copyright protection is used to identify the original owner of the multimedia content. This is done by embedding secret information in the multimedia content that can be retrieved only by the entity having the key.

2.3.1.4 Fingerprinting (Transaction Tracking)

Fingerprinting deals with the hiding of a serial number or any message that enables one to distinguish an object from other similar objects. For example if there is a DVD of some movie, the watermark will indicate the copyright holder of that DVD

and fingerprinting enable the identification of the individual buyer. Every buyer will have a unique fingerprint with the same watermark. This can ensure the tracking of pirated or illegally distributed copies of the multimedia content.

2.3.1.5 Copy Control

The main idea of 'Copy Control' is to restrict the recording (which can be distributed illegally) of the purchased multimedia content. A watermark detector needs to be embedded in every recording device which will prevent the recording of any copyright material.

2.3.1.6 Device Control

Device Control allows the interaction between devices through a signal in which a watermark is embedded. This is done in order to access the resources.

2.3.2 Design Aspects of Watermarking Schemes

To design a new watermarking scheme four features should be taken into consideration namely,

- Robustness: The ability of the watermark to be detected after attacks and must be robust under intentional and unintentional image processing attacks.

- Imperceptibility / Fidelity: The watermarked image and the original image should be identical and for the ideal design of a watermarking scheme there should be no distortion introduced in the content while embedding the watermark.

- Security: The embedded watermark is unrecoverable. However the security of the watermarking scheme is also dependent on the key used.

- Capacity / Data Payload: The amount of bits inserted in form of watermark in the image.

2.3.3 Classification of Watermarking Techniques

A huge amount of work has been done in this field; in order to understand how the watermarking schemes are different from each other it is necessary to classify them. They can be classified according to their characteristics and also depending on the application.

2.3.3.1 Spatial domain watermarking

The watermark is directly embedded / inserted into the pixel values of the host image. Inserting a watermark in spatial domain is easy to implement and results in less computational complexity. However watermark inserted in the spatial domain is not robust to common image processing attacks and can be removed with the help of some image analysis operations.

2.3.3.2 Frequency domain watermarking

An alternative for inserting the watermark in the multimedia content is in transformed domain. Transformed domain can be Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT). The watermarking in transformed domain is performed by inserting the watermark in the transformed coefficients (i.e. DCT coefficients). However the insertion of watermark in transformed domain can introduce noise or distortion in the quality of image / video or audio. So a reasonable amount of payload should be kept.

2.3.3.3 Blind watermarking

A watermarking technique is considered to be blind if in that particular technique, the original image is not required to recover the watermark in the extraction process. Some of the blind watermarking schemes are presented in [31-32, 36-38].

2.3.3.4 Non-blind watermarking

Contrary to blind watermarking techniques, in non-blind watermarking techniques the original multimedia content is required to recover the watermark in the watermark extraction process. Non-blind schemes are presented in [30, 33].

2.3.3.5 Robust watermarking

As mentioned in the above section, robust watermarking techniques are those which can resist against the common efforts to remove the watermark.

2.3.3.6 Fragile watermarking

In this type of watermarking techniques, the watermark inserted in the multimedia content is very sensitive to any kind of intentional or unintentional efforts to remove the watermark. A slight modification in image / video can result in damaging the watermark.

2.3.3.7 Semi Fragile watermarking

These techniques fall in between robust and fragile watermarking techniques. These techniques are designed to survive common image processing operation such as compression etc. But they are sensitive toward the intentional attacks to remove watermark.

2.3.3.8 Perceptible watermarking

Also known as visible watermarks are those which are intended to be visible on the multimedia contents, like video or images. These watermarks are easy to remove as compared to imperceptible watermarks (discussed in the next section).

2.3.3.9 Imperceptible watermarking

In contrast to the perceptible watermarks, imperceptible watermarks are those which are not visible in the multimedia content. They are embedded in the content in such a way that the quality of the content is not disturbed. The watermarking schemes reviewed in the following section 2.3.4 fall under the umbrella of imperceptible watermarking.

2.3.4 Review of Common Watermarking Schemes

In order to understand the methodology followed in designing the watermarking scheme, some popular watermarking schemes are reviewed in this section.

Scheme 1: Authors: This Watermarking Algorithm was developed by Weili Tang and Yoshinao AOKI at Graduate School of Electronics and Information Engineering, Hokkaido University, Japan and was published in [A DCT-based Coding of Images in Watermarking – Year 1997], [31].

- **Application:** Proof of ownership (copyright protection)**.**
- **Domain:** Transformed Domain Algorithm.
- Non-Blind (Original Image required for the watermark extraction).
- **Watermark:** A grey-scale image, half the size of the original image.
- **Payload** $= \frac{M \times N}{2}$, where M is the number of rows in the image and N is the number of columns in the image.
- Imperceptible.

The Technique: The main idea is to embed the watermark in the middle-band frequency. The authors selected grey scale images, both the original image and the watermark. Let the original image be D and the watermark to be W, and the watermarked image will be $W_d = W (+) D$. [(+) refers to the operation of modulation]. The watermark used is half of size of the original image.

Embedding process: The original image is divided in to 8×8 blocks of pixels and then these 8×8 blocks are transformed using DCT. A zig-zag scan is performed to select the middle-band coefficients as shown in Fig. 2.7. Using DPCM method, the watermark image is permuted. A residual pattern is obtained by modulation and the selected coefficients are modified using the residual pattern. The process of watermark embedding into selected coefficients is unclear as either additive or scaling method is used or some other functions. However, the main purpose is to show the useability of middle-band frequency coefficients for watermark embedding.

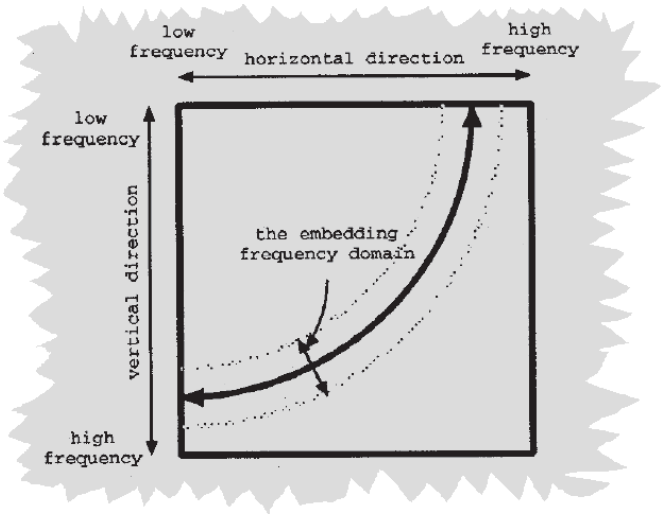


Figure 2.7: Selection of Middle Frequency Band. Picture cropped from [A DCT-based Coding of Images in Watermarking by Tang and AKOI], [31].

Extraction Process: The original image is also required to get the watermark. First the watermarked image is divided into 8×8 blocks and then the DCT is performed. The DCT coefficients are selected where the watermark is embedded (the middle-

band). An XOR operation and inverse permutation are performed to recover the watermark.

Discussion: The technique was proposed when the watermarking theory was in the state of emergence and not many techniques had been put forward then. One of the drawbacks of this technique is that one can easily modify the middle-band coefficients, and the watermark can get distorted. However, the recovery of AC coefficients are not possible from the unencrypted one; so this proposed scheme is still considered secure for copyright protection.

Scheme 2: Authors: This Watermarking Algorithm was developed by Mohamed Al Baloshi and Mohammed E. Al-Mualla at Multimedia Communication and Signal Processing Research Group, Etisalat University College, P.O.Box: 573, Sharjah, United Arab Emirates and was published in [A DCT-Based Watermarking Technique for Image Authentication – Year 2006], [32].

- **Application:** Authentication
- **Domain:** Transformed Domain Algorithm
- Blind
- **Watermark:** Binary image / logo of size equal to the number of 8×8 blocks of pixels in the image.
- **Payload** = $\frac{M}{8} \times \frac{N}{8}$, where M is the number of rows in the image and N is the number of columns in the image.
- Imperceptible
- Fragile

The Technique: The idea presented in this paper is to randomly select the DCT coefficient and embed exactly one watermark bit in it. DCT is performed on blocks

of size $n \times n$ pixels, thus meaning that the size of the watermark should be equal to the number of the DCT block. **Embedding process**: For an image I of size $M \times N$, where M is the number of rows and N is the number of columns. To embed the watermark

of the size $J \times L = (M/n \times N/n)$, DCT is performed on the block of size $n \times n$. Let us refer to these blocks as B_i where $1 \leq i \leq B$, B is the number of blocks. The corresponding DCT blocks are represented as C_i , where $1 \leq i \leq C$, C is the number of DCT blocks. A key k is used to randomly select the coefficients vector $S = \{s1 \ldots\ldots sB\}$, and W_i is the watermark bit in the coefficient C_{si} then the watermarked coefficient C_{si}' is expressed by equation. 2.3,

$$C'_{si} = \begin{cases} C_{si} \quad , & if \quad Q(C_{si}) = w_i \\ C_{si} + \Delta, & if \quad Q(C_{si}) \neq w_i \quad and \quad C_{si} \leq 0 \\ C_{si} - \Delta, & if \quad Q(C_{si}) \neq w_i \quad and \quad C_{si} > 0 \end{cases} \qquad (2.3)$$

Delta is the quantization parameter and $Q(.)$ is a coefficient-binary function which is shown in the next equation.

$$Q(c) = \begin{cases} 0, & if \left\lfloor \frac{c}{\Delta} \right\rfloor \ is \ \ even \\ 1, & if \left\lfloor \frac{c}{\Delta} \right\rfloor \ is \ \ odd \end{cases} \qquad (2.4)$$

The watermarked image is referred as *I'*. **Extraction Process:** The watermarked image *I'* is first divided into two $n \times n$ block, DCT is performed on these $n \times n$ blocks and the output is referred to as C_i. The same key is used to generate the vector *S*. By using equation 2.5 the watermark is extracted.

$$W_i'' = Q(C_{si}'') \qquad (2.5)$$

Discussion: PSNR is used to measure the degradation introduced in the watermarked image and to assess the level of tampering, a tampering assessment function is used

(TAF). The above scheme had undergone some attacks, and as stated in the paper it was effective against those attacks and had provided exact and selective authentication depending upon the attack.

Scheme 3: Authors: This Watermarking Algorithm was developed by Chun-ChingWang and Yu-Chang Hsu at Department of Electronic Engineering, National Changhua University of Education, No. 2, Shi-Da Road, Changhua, Taiwan and was published in [Fragile Watermarking Algorithm for DCT-Domain Image Authentication and Recompression– Year 2007], [33].

- **Application:** Authentication
- **Domain:** Transformed Domain Algorithm (With Compression)
- Blind
- **Watermark:** Sequence of Bits (1's or 0's). The watermark used in the given example is 6.5 times smaller than the original image. (Payload / size requirement is explicitly not mentioned).
- Imperceptible
- Fragile

The Technique: The idea in this paper is to embed the watermark during the compression process. For this purpose, the last non-zero DCT coefficients according to the zig-zag scan are selected and the watermark is embedded into that coefficients. **Embedding process**: The watermark is also permuted before the embedding process. The embedding process has been simplified and is explained as follows, Let the last non-zero coefficient in which the watermark bit need to be embedded be *Ø* and the watermark bit be *w*. *E*(*a*) = (*a+1*) *mod* 2, where '*a*' is the number of odd coefficients in the block. The watermark is embedded using the equation below,

$$\bar{\varphi} = \begin{cases} S(\varphi)(|\varphi| - 1) & ,if \quad w \otimes E(\Lambda) = 0 \\ \varphi & ,if \quad w \otimes E(\Lambda) = 1 \end{cases} \tag{2.6}$$

Extraction Process: The extraction of the watermark bit takes place according to the following given equation.

$$\bar{w} = \begin{cases} 0, & if \quad E\left(\bar{q}^{w}\right) = 1 \\ 1, & if \quad E\left(\bar{q}^{w}\right) = 0 \end{cases} \tag{2.7}$$

Where $\bar{q}^{w}$ is the watermark DCT block.

Discussion: The proposed scheme uses the last non-zero coefficient in the DCT block. As removing or modifying that coefficient will not significantly affect the image quality, so the watermark can be removed easily. Also the authors state that there is an improvement of 5% (increase) in the compression ratio. (The change can be variable, not necessarily only increasing)

Scheme 4: Authors: This Watermarking Algorithm was developed by Neminath Hubballi at Department of Computer Science, Indian Institute of Technology Guwahati and Kanyakumari D. P. at Department of Information Science, GMIT, Davanagere, Karnatakaand and was published in [Novel DCT based watermarking scheme for digital images – Year 2009], [34].

- **Application:** Copyright protection or proof of ownership (not mentioned explicitly in the paper)
- **Domain:** Transformed Domain Algorithm
- Non-Blind
- **Watermark:** The Watermark is generated by the image itself in the spatial domain. The watermark consists of binary digits. The generation of watermark involves the histogram of the original image. Then the mean of that histogram is calculated (H_m) along with the grey level threshold (G_t). The mean of histogram is then downscaled by multiplying H_m and G_t ($T_h = H_m \times G_t$). Then the original image is divided into the blocks of 8×8 pixels.

The mean of these blocks were calculated. If the mean of the block is greater than 'T_h' then the watermark gets the value 0 other wise 1.

- Imperceptible
- Robust

The Technique: The technique is similar to the middle band techniques discussed above. The original image is divided into blocks size of 8×8 pixels and the DCT is performed on these blocks. **Embedding process**: The middle frequency coefficients are selected. The authors state that mid frequency coefficients are taken because they are less Vulnerable to common image processing attacks like filtering and compression. The selected coefficients are modified using an additive method. **Extraction Process:** The original image is required in the extraction process thus making this technique non-blind. The watermark is calculated from the original image using the abovementioned technique for the generation of watermark.

Discussion: The proposed technique is placed under few image processing attacks like filtering and compression. The authors use three different quantization matrices in the compression process. The proposed scheme inherits the drawbacks of middle-band frequency selection technique. In the paper PSNR and Normalized Cross Correlation (NCC) are used to measure the distortion.

2.3.5 Watermarking Techniques Using DC Component

Some of the existing watermarking techniques that uses DC component in DCT domain are described below.

Scheme 1: Authors: This Watermarking Algorithm was developed by Jiwu Huang at Department of Electronics, Zhongshan University, Guangzhou, 510275, China and also with the Institute of Automation, Chinese Academy of Science and Y. Q. Shi and Y. Shi at the Department of Electrical and Computer Engineering, New Jersey

Institute of Technology, Newark, NJ 07102 USA and was published in [Embedding Image Watermarks in DC Components – Year 2000], [35].

- **Application:** Not Defined
- **Domain:** Transformed Domain Algorithm
- Blind
- **Watermark:** Random number sequence
- Imperceptible

The Technique: In this paper the authors argued that DC component is a more suitable place to embed watermark than any other in DCT domain. As in previous literature the researcher explicitly excluded DC component to embed the watermark. Since it was considered that by embedding a watermark in the DC component will cause block artefacts. The authors established some arguments which states that it is not necessarily that in every case the block artefacts are introduced in the content. Some of the experimental results reported in the paper, that justify that the watermark embedded in DC component is more robust than the watermark cast in lower AC frequency component.

In this proposed watermarking technique the image is divided into of 8×8 pixels of non-overlap blocks. Then on the basis of texture the blocks are categorized into two categories, one for weak texture (*S1*) and the other for blocks with strong texture (*S2*). The Human Visual System (HVS) is more sensitive to the changes made in *S1* than *S2*; that is why *S2* is considered more suitable for watermark embedding. The watermark is embedded in the DC components that fall in *S1* and *S2*, both using additive approach by keeping the scaling factor 0.006 for *S1* and 0.015 for *S2*. For the purpose of experiment, a Lena and a Baboon, image of size 256×256 were taken and after embedding a watermark the resulting PSNR values were 44.1 and 42.62 dB. The robustness of the proposed watermarking algorithm was also tested using low pass filtering, clipping and sub-sampling.

Scheme 2: Authors: This Watermarking Algorithm was developed by Haiping Lu, Xuxia Shi, Alex C. Kot and Lihui Chen at School of EEE, Nanyang Technological University, Singapore 639798 and Yun Q. Shi at Department of ECE, New Jersey Institute of Technology, Newark, NJ07102, USA and was published in [Watermark Embedding in DC Components of DCT for Binary Images – Year 2002], [36].

- **Application:** For binary images
- **Domain:** Transformed Domain Algorithm (DCT)
- Non-Blind
- **Watermark:** Random Number Sequence with Gaussian Distribution
- Imperceptible

The Technique: The technique proposed by the authors in this paper is for binary images. In the proposed technique, in [36], the image is subjected to pre and post processing. The pre-processing operation consists of blurring the image, and the post processing consists of binarizing the image after the embedding process into binary image. The embedding process begins by passing the image through a low pass Gaussian filter of size 5×5 to introduce blurring. Then the image is divided into non-overlapping blocks of 8×8 pixels. Non-uniform blocks are then identified and the blocks which are totally black or totally white are then skipped. DCT is performed on each block and the watermark is embedded using additive approach into DC component. IDCT is performed and those blocks are binarized. The watermarked blocks (non-uniform) are replaced in the original image to obtain the resultant watermarked image.

For the extraction process of watermark, the original image is required which makes this proposed scheme non-blind. The non-uniform blocks are then identified and blurred using the same Gaussian filter used in the embedding processing, to extract the watermark.

Scheme 3: Authors: This Watermarking Algorithm was developed by Fengsen Deng and Bingxi Wang at No 306, P.O. Box 1001, Information Engineering University Zhengzhon, Henan, 450002 China and was published in [A Novel Technique for Robust Image Watermarking in the DCT Domain – Year 2003], [37].

- **Application:** Not Specified (Assumption: Copyright Protection)
- **Domain:** Transformed Domain Algorithm (DCT)
- Blind
- **Watermark:** Binary data
- Imperceptible

The Technique: The proposed technique is similar to the technique in [36] described earlier, where the image is first divided into non-overlapping blocks of 8×8 pixels. Then these blocks are categorized into two categories, one for weak texture (*S1*) and other for strong texture (*S2*). The classification is made based upon edge point density. The binary watermark data (*W*) of size $M \times N$ is then permuted. DCT is performed on the 8×8 blocks and watermark bits are embedded such as if the watermark bit is '0' then that DC coefficients are quantized to the nearest even value, and if the watermark bit is '1' it is rounded to the nearest odd value. The quantization is done using a scaling factor that is different to *S1* and *S2*. IDCT is performed to get the watermarked image. Alike embedding process, in the extraction process, first the watermarked image is divided into blocks of size 8×8 pixels then the classification of texture is made using edge point density. The obtained coefficients are then quantized using the 'Δ'; if the quantized coefficient is even then the watermarking bit is '0' else it is '1'.

Scheme 4: Authors: This Watermarking Algorithm was developed by Ming-Harng Lee, Mong-Fong Horng and Bo-Chao Chang at Department of Computer Science and Information Engineering Shu-Te University, Kaohsiung, Taiwan, ROC and was published in [A DC-based Approach to Robust Watermarking with Hamming-Code – Year 2007], [38].

- **Application:** Ownership Identification
- **Domain:** Transformed Domain Algorithm (DCT)
- Blind
- **Watermark:** A binary image of 44×44 for 512×512 images.
- Imperceptible

The Technique: In the proposed technique, the watermark is embedded in the DC component. The embedding process is as follows, the image is first divided into blocks of *n*×*n* pixels. The size of the blocks varies and is adjustable according to the number of bits that need to be embedded into the image. Then these blocks are transformed into frequency domain by performing the DCT operation. The watermark, that needs to be embedded, is recoded with 16 bit hamming code and is embedded into the DC component by using the addictive approach as shown in the equation below.

$$dct\_C'(x,y) = \begin{cases} dct\_C\ (x,y) + \alpha, & if \quad HW(k) = 1 \\ dct\_C\ (x,y) - \alpha, & if \quad HW(k) = 0 \end{cases} \tag{2.8}$$

Where *dct_C (x,y)* is the DC component of the particular block and α is the offset value that is needed to be adapted accordingly. Finally, the IDCT is performed to get the watermarked image. The extraction process is as follows, first the DCT is performed on the image blocks of size defined in the embedding process, and the watermark bits are extracted using the equation 2.9.

$$HW(i,j) = \begin{cases} 1, & if \quad dct\_C'(i*k, j*k) > dct\_C\ (i*k, j*k) \\ 0, & if \quad otherwise \end{cases} \tag{2.9}$$

$$for \quad 0 \le i, j \le ceil\left(\frac{n}{k}\right)$$

Similarity is measured between the original and recovered watermark. The watermarked image was also tested under few attacks and found to be robust i.e. the watermarked image was placed under cutting attack and it was found that cutting up to 10% of the image still gave the similarity score above 70% between original watermark and the extracted watermark.

Scheme 5: Authors: This Watermarking Algorithm was developed by Gaorong Zeng at Institute of Information Science, Beijing Jiaotong University, Beijing, P. R. China and Section of Computer Science Teaching, Shangrao Normal University, P.R. China and Zhengding Qiu at Institute of Information Science, Beijing Jiaotong University, Beijing, P. R. China and was published in [Image Watermarking Based on DC Component in DCT – Year 2008], [39].

- **Application:** Ownership Identification (Assumed, as it is not mentioned in the publication)
- **Domain:** Transformed Domain Algorithm (DCT)
- Blind
- **Watermark:** A binary image of 64×64 for 512×512 images.
- Imperceptible
- Robust

The Technique: In the proposed technique, the watermark is placed under pre-processing step in which an Arnold transform is carried out on the watermark and the 2-D watermark is converted in to 1-D binary array. In the embedding phase, the original image / Host Image is divided into non-overlapping blocks of 8×8 pixels and 2-D DCT is performed on each block separately. The watermark bit is embedded in the DC coefficient of every block using QIM technique. Then inverse DCT is performed to get the watermarked image. In the extraction process, first, the watermarked image is divided into blocks of size 8×8 pixels and DCT is performed on them. The watermark bits are extracted from the DC component of each block using the equation given below,

$$\tilde{v}(k) = \mathrm{mod}(ceil(\frac{\tilde{F}(0,0)}{\Delta}), 2) \qquad (2.10)$$

Where 'Δ' is the step size used in the generation of quantization vector, $\tilde{F}(0,0)$ is the watermarked DC coefficient and $\tilde{v}(k)$ is the embedded information. All watermark bits are extracted from the DC components and the 1-D array of watermark bits is then converted into 2-D matrix. Arnold back transform is carried out to get the watermark. An experiment was performed in which the watermark was embedded into middle frequency and higher frequency. It was found that the robustness of DC was higher than any other coefficient. Also, the watermarked image was placed under several attacks (i.e. compression, median filtering, resizing, salt & pepper noise and Gaussian noise) and the technique was found to be robust under these attacks.

2.4 Commutative / Joint Watermarking and Encryption (CWE) / (JWE)

The purpose of watermarking is to ensure the authenticity of the multimedia content and also to protect the copyrights. On the other hand encryption is used to secure the multimedia content from any kind of adversaries. Encryption and watermarking both are separate functions. So watermarking and encryption operations can be performed in two steps, either watermarking operation followed by encryption of the watermarked data or encryption of the multimedia data first then followed by watermarking the encrypted data. But these approaches are not commutative. In order to extract the watermark from encrypted data, first the data should be decrypted, contradicting the commutative property, this means the watermark should be extracted without any decryption, in other words directly from the encrypted data. The question that arises here is 'why does one need this commutative watermarking and encryption?' The answer is simple; intuitively the commutative watermarking and encryption will result in less computational cost and allow signal processing in the encrypted domain. For example, if in one application

the multimedia is encrypted as well as watermarked, the CWE/JWE will allow direct extraction or embedding of the watermark in the encrypted content. Which means the knowledge of the decryption key is not required. This concept of watermarking in encrypted domain was first discussed in [3]. According to [3], four properties must be satisfied in case of watermarking the encrypted data. The four properties (variable names are kept same as in original publication) as adopted from [3] are:

I. A watermark (m) can be embedded using the watermarking embedding function (W) into the encrypted image (I

$$I_K' = M(I_K, m) \tag{2.11}$$

II. The watermark extracting function (V) should be able to extract the watermark (m) from the encrypted image, when the watermark was embedded in the encrypted domain.

$$V(M(E_K(I), m)) = m \tag{2.12}$$

Where E_K is the encryption function with key K.

III. The watermark extraction function should be able to extract the watermark from the encrypted image, when the watermark was embedded in clear (unencrypted) domain.

$$V(M(I, m)) = m \tag{2.13}$$

IV. The decryption function should not affect the integrity of the watermark.

$$V(D(M(E_K(I), m))) = m \tag{2.14}$$

Where D is the decryption function.

All of these properties have been satisfied by Lian *et al*. in [3], the architecture for joint watermarking and encryption is described in the next section.

2.4.1 General Framework for JWE/CWE

The general framework for CWE / JWE is shown in the figure below, where,

P = Original multimedia content

C = Encrypted multimedia content

M = Watermarked multimedia content

E ( ) = Function for Encryption Algorithm

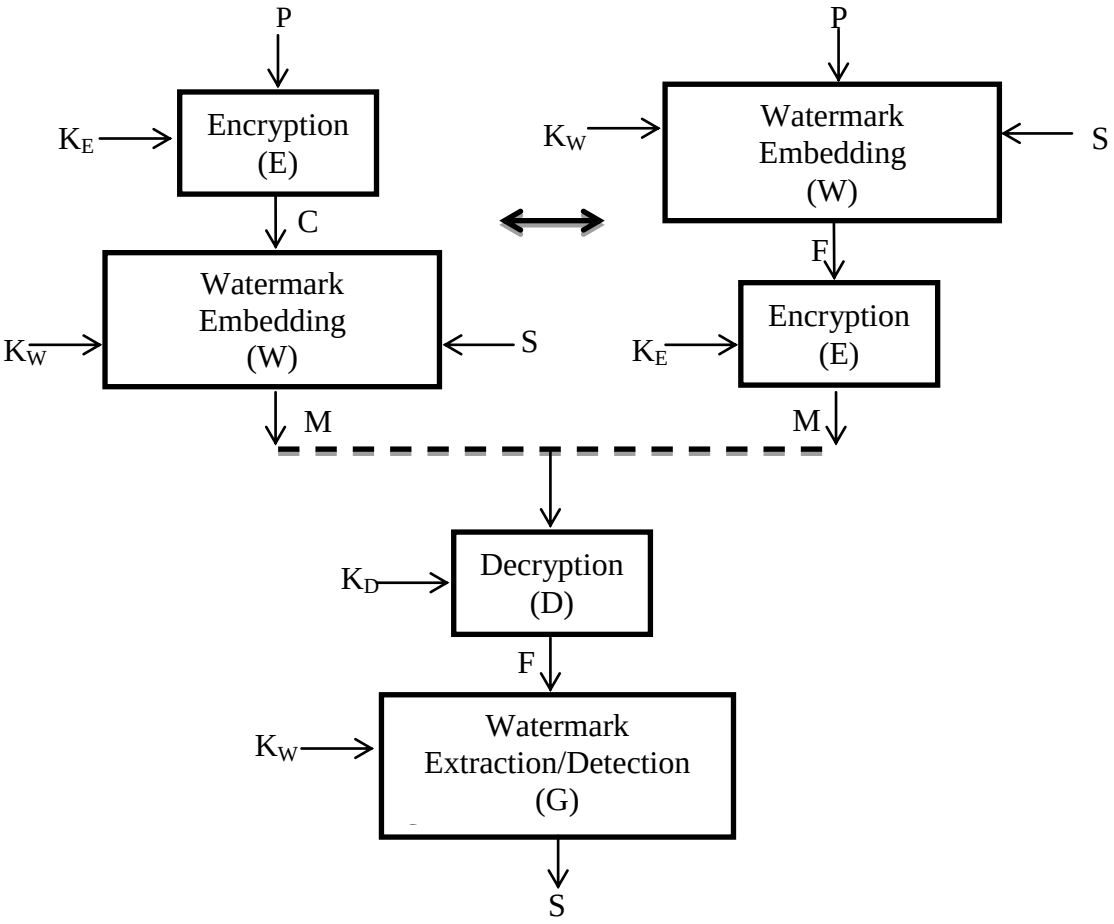


Figure 2.8: The Joint Encryption and Watermarking Framework

The framework is borrowed from the book "Multimedia Content Encryption: Techniques and Applications", by Shiguo Lian), [40].

W ( ) = Function for Watermarking Algorithm for embedding the watermark

K_E = Encryption Key

K_W = Watermark Key

S = Watermark

D ( ) = Function for Decryption Algorithm

G ( ) = Function for Watermark Extraction / Detection Algorithm

K_D = Decryption Key

The above framework can be described mathematically as:

$$W\left(E\left(P, K_E\right), W, K_W\right) = E\left(W\left(P, S, K_W\right), K_E\right) = M \qquad (2.15)$$

And for the detection/extraction of watermark,

$$\begin{aligned} G\left(D\left(M, K_D\right), K_W\right) &= G\left(D\left(E\left(W\left(P, S, K_W\right), K_E\right), K_D\right), K_W\right) \\ &= G\left(W\left(P, S, K_W\right), K_W\right) = S \end{aligned} \qquad (2.16)$$

As it can be observed that, by changing the order of watermarking operation and encryption operation, the encryption/decryption and watermarking extraction/embedding processes are not affected. A watermarking and encryption scheme is commutative if it follows the above expressions.

2.4.2 The CWE / JWE Problem

The main issue of concern is how to achieve this CWE for image and video data. One possible way is that the watermarked portion and encrypted portion of the visual data must be independent of each other in order to achieve the goal of CWE / JWE. Partial encryption is one of the possible solutions and has also been reported in the literature. The idea is to partition the data into two portions, one portion is watermarked and the other one is encrypted, in order to make both operations independent of each other. As complete encryption is not performed on the data, so the portion where the watermark is embedded is unprotected or unencrypted, which can cause a security breach.

2.4.3 CWE / JWE Schemes Based on Partial Encryption

Not substantial or significant amount of literature has been published in the area of joint watermarking and encryption. Recently *Lian et al*. [3] put forward a general architecture for CWE / JWE. Some of the implementations on different codecs have also been reported in the literature after the emergence of CWE / JWE architecture. The main idea of partitioning the data for CWE and the complete architecture was introduced in [3]. First, the proposed architecture and its practical implementation on wavelet based codecs are described. Then some other proposed schemes are discussed.

(Note: The variables used in the schemes described below are kept same as those published in the paper/letter for simplicity)

Scheme 1: Authors: The CWE Scheme was developed by Shiguo Lian, Zhongxuan Liu, Ren Zhen, and Haila Wang at France Telecom Research & Development Beijing, China and was published in [Commutative Watermarking and Encryption for Media Data – year: 2006], [3].

Codec on which the scheme is implemented: JPEG 2000 (DWT domain)

The CWE/JWE Scheme: In the proposed scheme the original multimedia data is partitioned into two parts. One of these two partitioned parts is regarded as the significant part of the multimedia data while the other is considered as less significant.

Block diagram of Commutative Encryption and Watermarking Solution based on Partial Encryption is shown on next page.

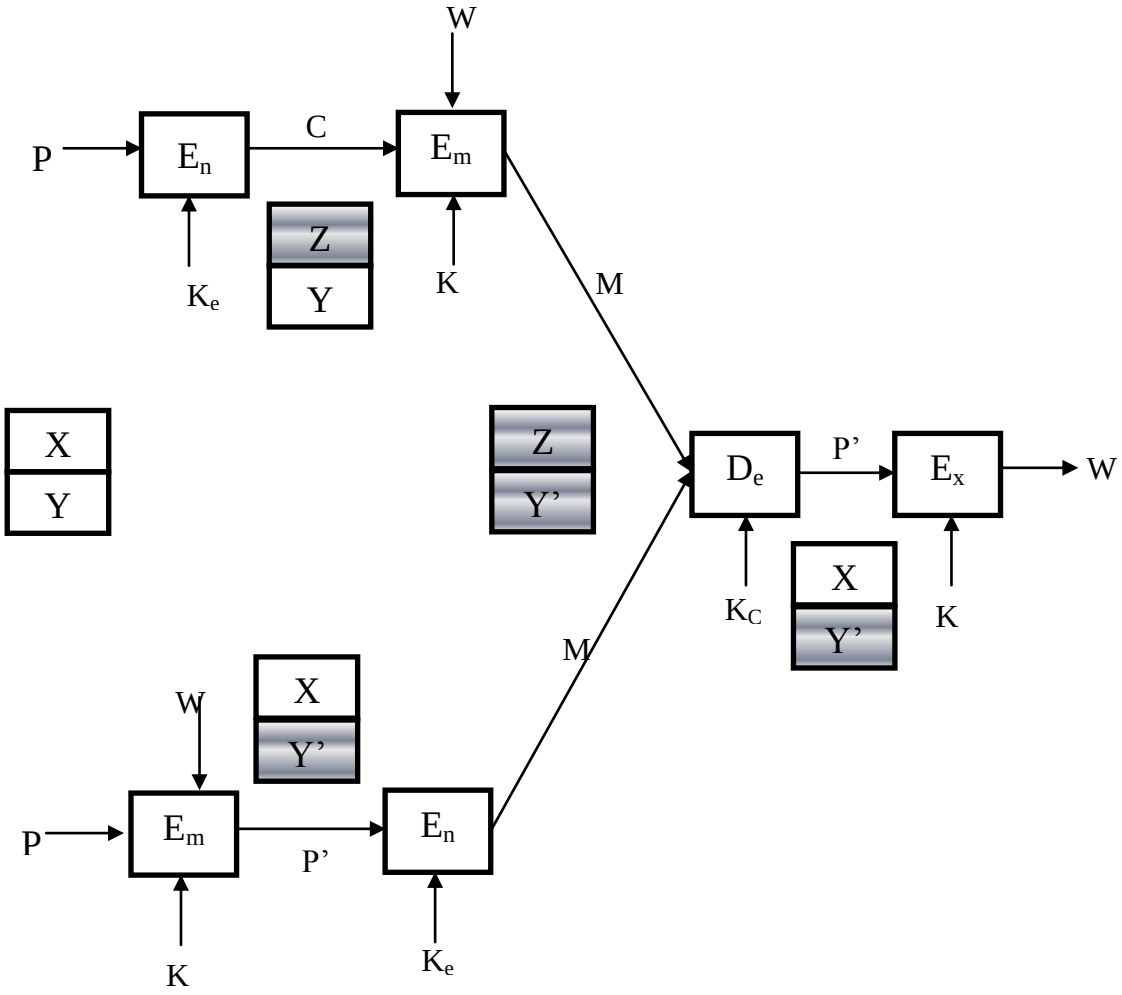


Figure 2.9: Block diagram of Commutative Encryption and Watermarking Solution based on Partial Encryption.
(Figure adopted from the letter [Commutative Watermarking and Encryption for Media Data] [3])

Referring to Fig. 2.9, the definitions of the symbols are given below,

P = Original multimedia content

X = Significant part of the content (to be encrypted)

Y = Other part of the content (to be watermarked)

C = Encrypted content

M = Watermarked cipher content

P' = Watermarked content

W = Watermark

K_C = Encryption key

K_W = Decryption key

E_n ( ) = Encryption function

D_e ( ) = Decryption function

E_m ( ) = Function for Watermarking Algorithm for embedding the watermark

E_x ( ) = Function for Watermark Extraction / Detection Algorithm

Referring to the diagram, when either X is encrypted first or Y is watermarked, it will not interfere with the any of the processes thus both the operations are independent of each other. The watermark is embedded or extracted without decrypting the content or in other words without the knowledge of the decryption key. Reversely, the content can be encrypted and decrypted without damaging the watermark. Mathematically, the commutative watermarking and encryption is defined as,

$$M = E_m[E_n(X||Y,K_c),\ W,K_w] = E_m(Z||Y,W,K_w) = Z||Y' \qquad (2.17)$$

$$M = E_n[E_m(X||Y,W,K_w),K_c] = E_n(Z||Y',K_c) = Z||Y' \qquad (2.18)$$

The scheme was implemented on Wavelet based codecs, where $M \times N$ image was transformed by a four-level wavelet. Complete Encryption was performed on low level sub-bands (LL_3, LH_3, HL_3, *and* HH_3). Sign encryption was performed in the sub-bands in high level (LH_1, HL_1, HH_1, LH_0, HL_0, *and* HH_0). The sub bands in mid-levels (LH_2, HL_2, and HH_2) were both encrypted and watermarked, using sign encryption technique and QIM technique for watermarking.

Scheme 2: Authors: The CWE Scheme was developed by Shiguo Lian, Zhongxuan Liu, Ren Zhen, and Haila Wang and was published in [Commutative Encryption and Watermarking in Video Compression – year: 2007], [41].

Codec on which the scheme is implemented: H.264/AVC

The CWE/JWE Scheme: The concept/architecture of the proposed scheme is the same as in the previous paper which was based on partial encryption, but the codec on which the scheme is implemented is different. Here MVD, IPM and sign of DCT coefficients (first eight) are encrypted and the middle frequency coefficients are watermarked.

Scheme 3: Authors: The JWE Scheme was developed by M. Cancellaro, F. Battisti, M. Carli A. Neri at Applied Electronics Department, Universit`a degli Studi Roma TRE, Roma, Italy and G. Boato, F.G.B. De Natale at Department of Information Engineering and Computer Science, University of Trento, Trento, Italy and was published in [A Joint Digital Watermarking and Encryption Method – year: 2008], [42].

Codec on which the scheme is implemented: Tree-Structured Haar Transform (TSH)

The CWE/JWE Scheme: The scheme employs the same architecture as described in [3]. The domain chosen is the Tree-Structured Haar Transform. In TSH the image is decomposed using Discontinuity Point Vector (DPV). The sizes of sub-bands are dependent on DPV. So DPV acts as a key for the decomposition of the image and it is kept secret in the proposed scheme.

The proposed scheme can be explained as follows: Suppose X is the original image and $\times$ is the third order TSH decomposition. $\times$ will be characterized by 10 sub-bands (i.e. LL_3, HL_3, LH_3, HH_3, HL_2, LH_2, HH_2, HL_1, LH_1, HH_1) after decomposition. A binary watermark W of the same size as the image is selected. The coefficients obtained in the transform domain are then converted from analog to digital, meaning that they are represented as B bits. Thus forming a bitplane matrix BP_l, where $1 \leq l \leq$

B. BP_B is the least significant bitplane and is replaced by the matrix containing sign of the TSH coefficients. The significant bitplanes are encrypted using AES cipher. The remaining bitplanes are then used for watermark insertion. The binary to decimal conversion is performed on these remaining bitplanes. Also, TSH transform is performed on the watermark W resulting in the w by using the same DPV as used for transforming the original image. QIM is used to embed the watermark into the converted coefficients. Finally, digital to analog conversion is carried out followed by the inverse TSH transform to obtain the encrypted and watermarked image $X_{W,E}$.

The watermark extraction and decryption process is as follows: a third order TSH transform is performed on $X_{W,E}$ to obtain $\chi_{W,E}$, using the same DPV used in the encryption and watermarking process. The transformed coefficients are then converted into digital, from analog, thus forming matrices of bitplanes. The selected most significant bitplanes are decrypted using AES. The bitplanes that have been watermarked are then converted into decimal form and are arranged in a matrix. The watermarked w' is recovered using the QIM recovery formula stated in the paper. The watermark is then converted to spatial domain and represented as *W'*. A comparison between the original watermark and the extracted watermark was performed. The invisibility of the watermark was measured using PSNR and WPSNR. The proposed scheme was subjected to several image processing attacks (i.e. sharpening, blurring, addition of Gaussian noise and JPEG compression) and was found to be robust against those attacks.

Scheme 4: Authors: The JWE Scheme was developed by F. Battisti, M. Cancellaro, M. Carli A. Neri at Applied Electronics Department, Universit`a degli Studi Roma TRE, Roma, Italy and G. Boato at Department of Information Engineering and Computer Science, University of Trento, Trento, Italy and was published in [Watermarking and Encryption of color images in the Fibonacci domain – year: 2008],[43].

Codec on which the scheme is implemented: Fibonacci-Haar Wavelet Transform

The CWE/JWE Scheme: In this scheme the architecture for CWE / JWE as proposed by *lian et al*. was followed and implemented in the domain of Fibonacci-Haar Wavelet Transform. Fibonacci-Haar Wavelet Transform is a generalization of Haar Transform and it uses a Fibonacci *p-sequence* into decompose the image in to sub-bands. The encryption and embedding procedure is as follows: let the original image be *X*, and as the image is colored so X_C represents its color components where $C = R, G, B$. Let a watermark be *W* having only binary values. As this watermark has to be embedded into the color component of image so it is also partitioned in to three parts represented by W_C**.** A first order Fibonacci-Haar transfom is performed on the image X_C using a Fibonacci sequence P_C and the resulting transformed image is represented by $\mathcal{X}_C$. The first order transformation results in four sub-bands (i.e. LL_C, LH_C, HL_C, HH_C). The LL_C sub-band is then encrypted using AES cipher. The rest of the sub-bands are partitioned into *B* blocks, in order to embed the watermark. The watermark is embedded into the blocks using a Singular Value Decomposition (SVD) watermarking method. Finally the inverse of Fibonacci-Haar Wavelet transform is carried out to get the encrypted and watermarked image $\mathcal{X}'_C$.

The extraction and decryption procedure is as follows: First the watermarked and encrypted image $\mathcal{X}'_C$ is transformed into Fibonacci-Haar Wavelet domain using the same Fibonacci p-sequence P_C as used in the encryption process. The LL'_C sub-band is then deciphered using AES with the key sent by the sender to receiver. The rest of the three sub-bands (LH'_C, HL'_C, HH'_C) are then partitioned into *B* blocks, and the watermark is extracted using SVD method. Finally the original and the extracted watermarked are compared.

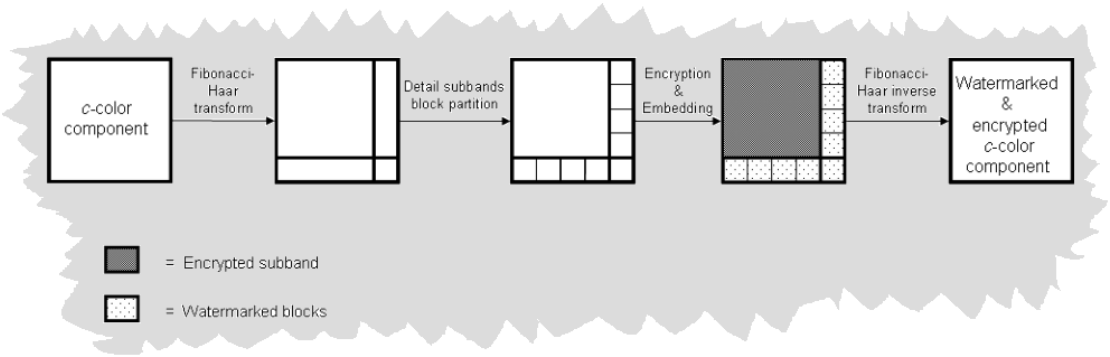


Figure 2.10: Diagram of Commutative Encryption and Watermarking Scheme in [43].
(Figure cropped from original publication in [43])

PSNR and WPSNR are used to measure the distortion between the watermarked and the original image. The proposed scheme was also subjected to some attacks and its robustness was verified.

Scheme 5: Authors: The JWE Scheme was developed by Federica Battisti, Michela Cancellaro, Marco Carli, Alessandro Neri at Applied Electronics Department, Universit`a degli Studi Roma TRE, Roma, Italy and Giulia Boato at Department of Information Engineering and Computer Science, University of Trento, Trento, Italy and was published in [Joint Watermarking and Encryption of Color Images in the Fibonacci-Haar Domain – year: 2009], [44].

Codec on which the scheme is implemented: Fibonacci-Haar Wavelet Transform

The CWE/JWE Scheme: This paper is an extension of the previously described paper by the same authors. The extension includes the increment of the image database evaluation of performance in terms of mutual information between the original watermark and the recovered one.

Scheme 6: Authors: The CWE Scheme was developed by Shiguo Lian at France Telecom R&D (Orange Labs) Beijing, Bejing 2 Science Institute South Rd., Haidian District, Beijing, People's Republic of China and was published in [Quasi-commutative watermarking and encryption for secure media content distribution – year: 2009], [45].

Codec on which the scheme is implemented: MPEG 2

The CWE/JWE Scheme: In this paper the author introduces another solution for CWE / JWE other than partial encryption; a new homogenous watermarking-encryption scheme which is quasi commutative is proposed. In the proposed scheme, watermarking and encryption can be done on the same part of the multimedia content. The scheme is referred as a Quasi-Commutative Watermarking and Encryption (QCWE) scheme and it uses homogenous operations. A possibility of security breach in the previously proposed architecture for CWE / JWE based on partial encryption is also pointed out. It is stated that an attack can be carried out on the watermarked-encrypted content by replacing the watermarked part with some other data, and the same can be done to the encrypted part. Thus the content will lose its originality.

The encryption and watermarking process is described as follows: Suppose,

$P = p_0, p_1 \ldots p_{n-1}$ (Original content)
$C = c_0, c_1 \ldots c_{n-1}$ (Encrypted content)
$M = m_0, m_1 \ldots m_{n-1}$ (Watermarked content)
$P' = p'_0, p'_1 \ldots p'_{n-1}$ (Decrypted content)
K_E = Encryption key
K_W = Watermarking key
Z = Detected Watermark

The encryption and watermarking embedding is described as follows: Before the encryption and watermarking process, the data is pre-processed to avoid overflow. For the encryption process, the data is modulated by a secret pseudorandom sequence $X_0 = x_{0,0}, x_{1,0}, \ldots, x_{0,n-1}$, using the key K_E. Again a secret pseudorandom sequence $X_1 = x_{0,0}, x_{1,1}, \ldots, x_{1,n-1}$, is generated using the key K_w and additive watermarking is

performed on the data. Decryption and watermarking extraction is described as follows: For the purpose of decryption, a secret pseudorandom sequence $X_0 = x_{0,0}, x_{1,0}, \ldots, x_{0,n-1}$, is generated using the key K_E to decrypt the data and again a secret pseudorandom sequence $X_1 = x_{0,0}, x_{1,1}, \ldots, x_{1,n-1}$, is generated using the key K_w to extract the watermark from the data.

The proposed scheme was also applied to MPEG 2 codec, where DC coefficients in the intra-encoded Luma blocks were chosen to be encrypted along with independently encrypting the DC coefficients in Chrom blocks, or inter-encoded blocks and the signs of AC coefficients. Only intra-encoded Luma blocks were chosen to be watermarked. Also, performance evaluation of the scheme was carried out; this scheme is not considered to be robust as compared to other schemes falling under joint scenario and also pre-processing of the data is required.

Table 2.2 (a): A consolidated presentation of all the Commutative Watermarking and Encryption schemes (CWE), proposed in Literature.

Scheme (Author Name's)	**Target Codec**	**Transf-ormation**	**Data Splitting**		**Encryption Scheme Used**	**Water-marking Scheme Used**
			Encryption	**Water-marking**		
Lian *et al*. (2006) [3]	JPEG 2000	DWT	Complete Encryption on Lower Level Sub-band. Sign Encryption on High and Mid-level, Sub-bands.	Mid-level Sub-bands.	AES	QIM
Lian *et al*. (2007) [41]	H.264/ AVC	DCT	MVD, IPM and sign of DCT coefficients	Middle frequency coefficients	Selective Encryption Scheme for H.264/AVC [81]	Watermarking Technique for H.264 [82]
Cancellaro *et al*. (2008) [42]	----	TSH	MS Bitplanes	Decimal value of Mid-Bitplanes	AES	QIM

Cancellaro *et al*. (2008) [43]	----	Fibonacci-Haar transfom	LL_C sub-band	Block Based Partitioning of LH_C, HL_C and HH_C Sub-bands	AES	SVD Watermarking Method
Battisti *et al*. (2009) [44]	----	Fibonacci-Haar Wavelet transform	LL_C sub-band	Block Based Partitioning of LH_C, HL_C and HH_C Sub-bands	AES	SVD Watermarking Method
Shiguo Lian (2009) (QCWE) [45]	MPEG 2	DCT	DCs in the intra-encoded Luma blocks and sign of AC Coefficients	DCs in intra encoded Luma blocks	Stream Cipher (Using XOR Function)	Method Discussed in [45]

Table 2.2 (b): Strengths and Drawbacks/Weaknesses of the presented Commutative Watermarking and Encryption schemes (CWE).

Scheme (Author Name's)	**Strengths**	**Drawbacks /Weaknesses**
Lian *et al*. (2006) [3]	• Within DWT based codec. • Perform complete encryption.	• Cannot be extended to DCT based codecs. • Does not deal with perceptual encryption.
Lian *et al*. (2007) [41]	• Complete Encryption for H.264/ AVC	• Cannot be implemented on Image compression codecs. • Does not deal with perceptual encryption.
Cancellaro *et al*. (2008) [42]	• Perform complete encryption on the content.	• Cannot be extended to DCT based codecs. • Not in scenario of compression. • Does not deal with perceptual encryption.
Cancellaro *et al*. (2008) [43]	• Perform complete encryption on the content.	• Cannot be extended to DCT based codecs. • Not in scenario of compression. • Does not deal with perceptual encryption.
Battisti *et al*. (2009) [44]	• Perform complete encryption on the content.	• Cannot be extended to DCT based codecs. • Not in scenario of compression. • Does not deal with perceptual encryption.
Shiguo Lian (2009) (QCWE) [45]	• Perform complete encryption on the content. • Using same data.	• Cannot be implemented on Image compression codecs. • Does not deal with perceptual encryption. • Pre-processing required. • Relatively less robust.

Table 2.2(a) shows the attributes associated with the joint scheme described in the above sections and Table 2.2(b) shows the pros and cons of these joint schemes. It can be noticed from Table 2.2 that still there is no joint scheme proposed for JPEG, beside the fact that JPEG is the most commonly used image compression standard. The proposed schemes in [41-43] are also not integrated in the any compression system. Similarly the most recently proposed scheme, in [45], is not suitable in real-time multimedia applications as it required pre-processing of the data that need to be encrypted and watermarked. Each multimedia data compression standard requires a dedicated encryption scheme or watermarking scheme or a dedicated joint encryption and watermarking scheme, which still haven't been reported yet in the literature. Thus there is a need of a joint encryption and watermarking scheme integrated in JPEG compression standard. However, the proposed work is on joint perceptual encryption and watermarking scheme, as perceptual encryption is more sophisticated derivation of multimedia encryption schemes. The proposed scheme can also be moulded into complete encryption scheme by ignoring the gradual encryption or the control factor, and encryption all the selected data (selected AC coefficients) together.

2.5 Summary

A detailed literature review has been presented in this chapter. The chapter is partitioned into three main parts. The first part covers the covers the brief introduction and background of encryption techniques and its classifications followed by multimedia content encryption schemes specifically with the focus on perceptual encryption schemes. Also some of the popular perceptual encryption schemes have been discussed.

In the second part of this chapter, a brief introduction and background of watermarking is presented. Few watermarking schemes are discussed to learn the basics of watermarking framework. Although the focus is on the issue of watermarking, the DC component and the DC component based watermarking schemes are presented as well.

In the third part of the chapter, the problem of joint watermarking and encryption are discussed, followed by a presentation of, to the best of our knowledge, all joint watermarking and encryption schemes existing in the literature.

This page is intentionally left blank Chapter 3 starts from next page.

CHAPTER 3

THE DESIGN OF JOINT PERCEPTUAL ENCRYPTION AND WATERMARKING SCHEME (JPEW)

3.1 Introduction

In the previous chapter the architecture of Joint Encryption and Watermarking schemes proposed in the literature up till now, has been reviewed. Also the basic concepts involved in encryption and watermarking of multimedia content that can further facilitate the discussion on the proposed scheme, were discussed together with the review of several encryption and watermarking schemes. In this chapter, a novel architecture of a Joint Perceptual Encryption and Watermarking Scheme (JPEW) is proposed that is commutative and integrated within the JPEG compression framework. It is followed by the methodology to evaluate the performance of the proposed scheme. Up till now, no scheme has been reported in the literature which addresses the design of a joint perceptual encryption and watermarking scheme. The proposed design not only involves the design of a commutative architecture for perceptual encryption and watermarking but also a new design of both the perceptual encryption scheme and watermarking scheme. These two schemes are also so designed that they are easily integrated with JPEG compression standard individually.

Firstly the proposed architecture for the Joint Perceptual Encryption and Watermarking scheme that is easily integrable with DCT based JPEG standard is described to clarify the main idea of the proposed scheme.

3.2 Architecture for the proposed Joint Perceptual Encryption and Watermarking Scheme (JPEW)

The architecture of the proposed scheme is based on intelligently splitting the multimedia content within the JPEG framework and partially encrypting and watermarking selected components of the multimedia content. This intelligent splitting of data is preferable in the transform domain. Since in transform domain, a clearer representation of energy distribution of the content is visible and can be manipulated according to given requirements. In pixel domain the only available information is pixel itself that at most can be further split into bitplanes but those bitplanes do not provide sufficient levels of gradual degradation in the content, which is the fundamental requirement of perceptual encryption. Additionally, if the data is required for the embedding the watermark then only a limited amount of data is available for it. Secondly, to further allow the design to be commutative as well as within compression framework, more limitations are imposed on the available parameters for each function of watermarking and encryption. So there is a trade off between limitation of data parameters and level of degradation to be introduced in the content for perceptual encryption scheme, and payload for watermarking scheme. One further drawback of manipulating the content for the watermark embedding and encryption is that the scheme will no longer be integrable within compression framework. In this case the watermarking and the encryption have to be done before compressing the content. Thus these mentioned constraints must be kept in consideration while designing commutative joint perceptual encryption and watermarking scheme in framework of compression.

The architecture of the proposed scheme is shown in Fig. 3.2. The DCT coefficients obtained after the quantization process in the JPEG compression standard are chosen for splitting the data. The DCT coefficients are categorized as AC coefficient (AC component) and DC coefficient (DC component). The DC component is further divided into DC bitplanes. Some coefficients from the AC component and few DC bitplanes from the DC component are selected to serve the purpose of perceptual encryption, and the remaining bitplanes of the DC component are selected for watermarking. The selection criterion of these components is based on a statistical

analysis and is discussed in section 3.3.1.3.

3.2.1 Format Compliance

For the scheme to be called a Joint Encryption and Watermarking Scheme it is necessary that the operation of watermarking and encryption should be independent of each other as discussed in the previous chapter. But if the joint scheme in the scenario of the compression then the property of Format Compliance which means that even if the content is encrypted or watermarked, it can be decompressed at the decoder as well as it can be recompressed on the encoder. Simply the decoder and encoder must be able to understand the encrypted and/or watermarked bit stream. The proposed scheme which can be regarded as Joint Perceptual Encryption-Watermarking-Compression Scheme is format complaint or transparent to JPEG compression standard. In this whole process the encrypted data can be decrypted and the watermark can be extracted at any stage, thus making compression, encryption and watermarking independent of each other, as shown in the block diagram in Fig. 3.1.

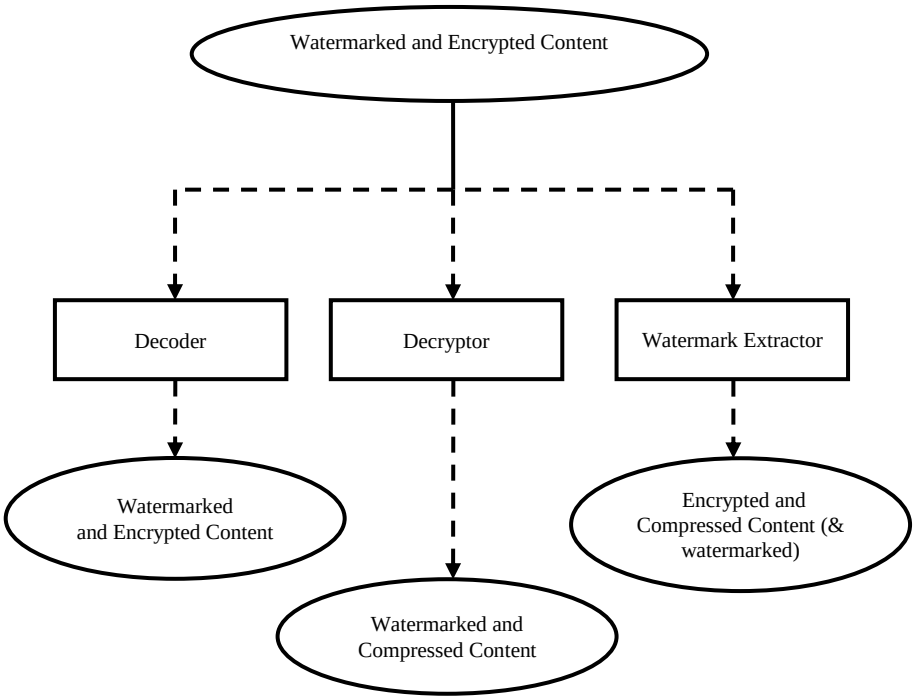
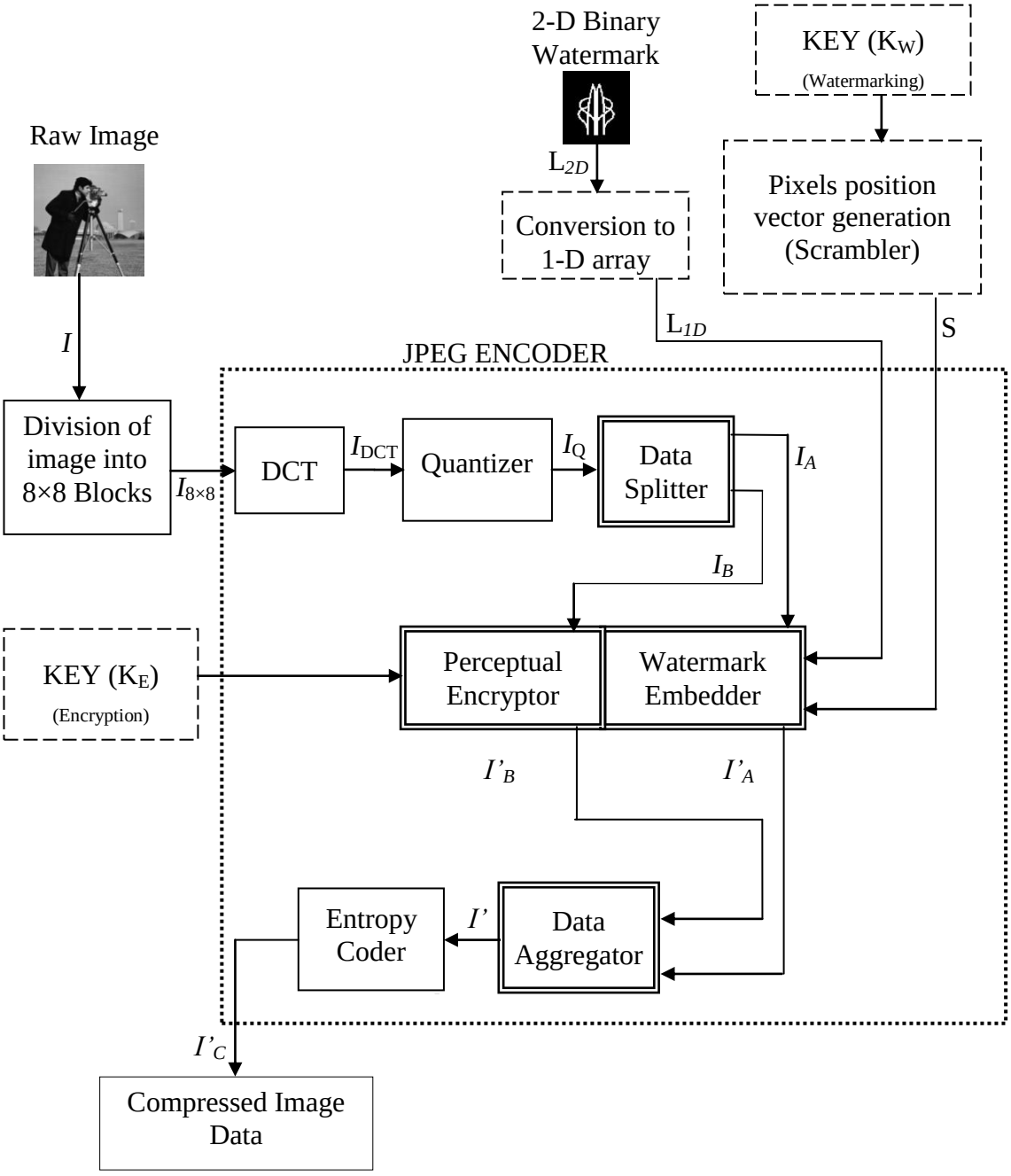
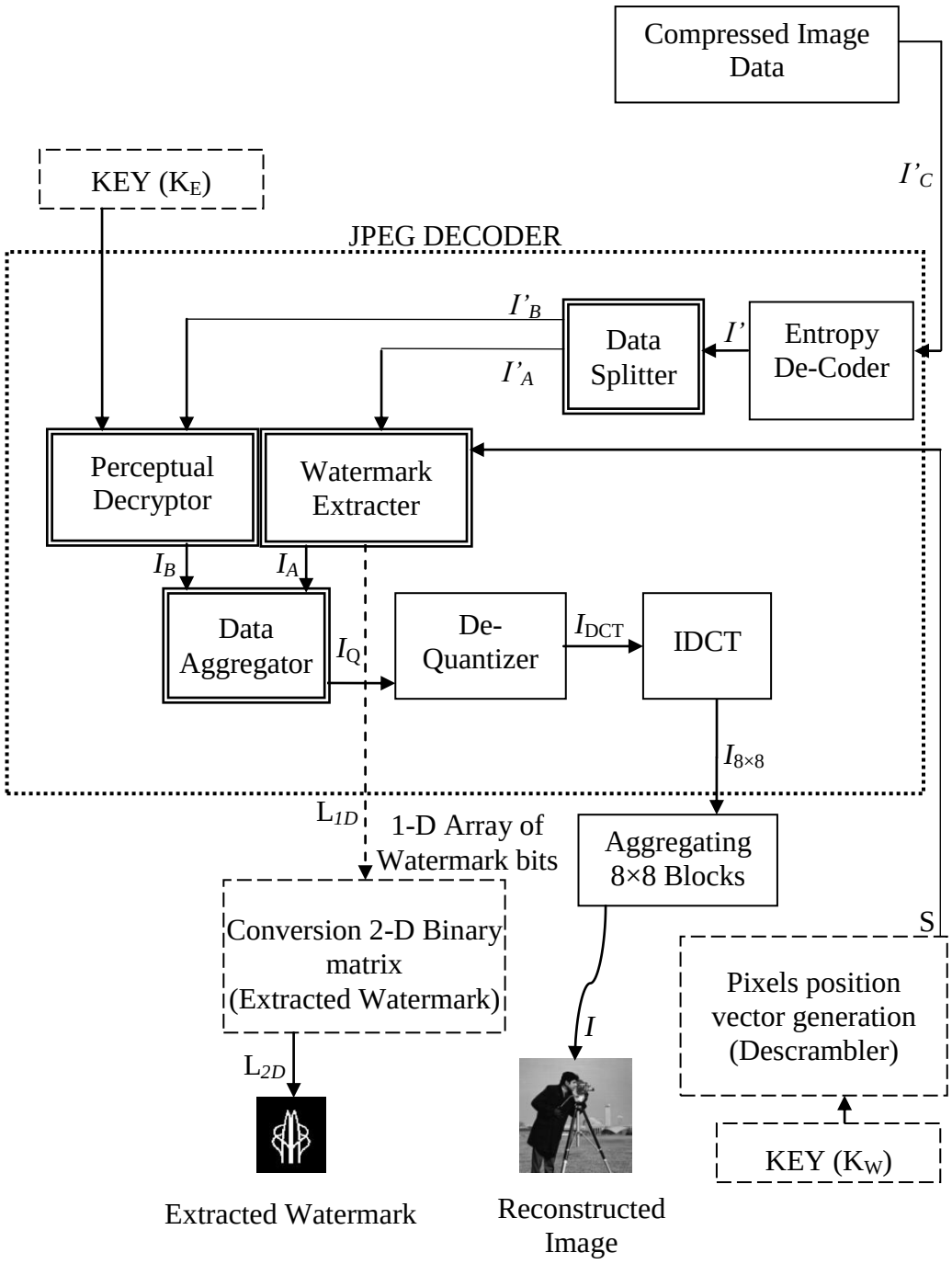


Figure 3.1: Independence diagram which shows the independence of watermarking, encryption and compression operation from each other.


2-D Binary Watermark
KEY (K_W)
(Watermarking)
Raw Image
L_{2D}
Conversion to 1-D array
Pixels position vector generation (Scrambler)
L_{1D}
S
I
JPEG ENCODER
Division of image into 8×8 Blocks
$I_{8\times8}$
DCT
I_{DCT}
Quantizer
I_Q
Data Splitter
I_A
I_B
KEY (K_E)
(Encryption)
Perceptual Encryptor
Watermark Embedder
I'_B
I'_A
Entropy Coder
I'
Data Aggregator
I'_C
Compressed Image Data

(a)



(b)

Figure 3.2: Architecture of the proposed Joint Perceptual Encryption and Watermarking (JPEW) Scheme (a) The Encoder Part of the JPEG Compression standard with Encryptor and Watermark Embedder Block incorporated in it. (b) The Decoder part of the JPEG Compression Standard with the Watermark Extractor and Decryptor Block incorporated in it.

3.3 Proposed System

Block-diagram of the proposed system within the commutative framework for perceptual encryption and watermarking is presented in Fig.3.2. Various blocks of the system are described below.

3.3.1 JPEG Encoder / Decoder

JPEG is a lossy/lossless compression standard. Lossy compression is achieved by first transforming the pixel domain image data using DCT and quantizatizing the same afterwards. But it can achieve much higher compression ratio as compared to the simple lossless compression schemes. The main components of the JPEG compression standard are the DCT / IDCT, Quantizer / Dequantizer and Entropy Coder / Decoder. For the encoder part, first DCT is carried out for continuous-tone still image that needs to be compressed. Then the obtained DCT coefficients are quantized (see [46] for detailed working of JPEG compression standard). Then these quantized DCT coefficients are fed into the Watermark Embedder + Perceptual Encryptor Block based on simple Scrambler. Here the content is watermarked and encrypted to the required perceptual quality. After that, the obtained scrambled and watermarked coefficients are passed through the entropy coder which uses runlength and Huffman coding techniques to reduce the size of the bitstream, which is to be further transmitted. The reverse of the encoder process is adopted in the JPEG decoder part.

3.3.1.1 Block Based DCT / IDCT

DCT step can be regarded as the most important step in the JPEG compression standard. Besides JPEG, other compression standards like MPEG 1, MPEG 2, MPEG 4 and H.264 also utilize DCT in intra-frame coding because of its energy compaction

property. In order to understand the proposed scheme it is necessary to discuss DCT and its characteristics which will be exploited to design the scheme. After DCT operation, the obtained data can be categorized as AC and DC Coefficients. DC carries the highest energy in the DCT block and it is the average of all the pixels in that block. It is also known as low frequency component. On the other hand, AC coefficients are known as high frequency components and less amount of energy is compacted in the AC coefficients as compared to the DC coefficients. This is also shown in section 3.3.1.3 (for the mathematical equations of 2-D DCT see [46]).

3.3.1.2 Quantizer / De-Quantizer

Another important step in JPEG, to achieve higher level of compression, is quantization. The main idea behind quantization is to discard redundant data. Mostly high frequency component i.e. AC coefficients in the lower right corner in a DCT block, are considered to be redundant information. In the JPEG implementation, quantization is carried out by dividing the DCT coefficients with corresponding values in quantization matrix. A commonly used quantization table is shown in Fig.3.3 below. The values in the lower right corner are large as compare to the rest of the values in it, because their lies spatially redundant information.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Figure 3.3: A Commonly Used Quantization Table.
Picture cropped from [46].

Similarly, in de-quantization process, in JPEG implementation, the DCT coefficients are multiplied by the corresponding values in the quantization table (for more details see [46]).

3.3.1.3 Data Splitter

Data Splitter block in Fig 3.2, is the primary component of the proposed scheme that allows the joint framework for perceptual encryption and watermarking. In this block, the obtained DCT data are split into two parts. The basic idea is to manipulate the energy contained in the DCT coefficients. As reported in [19] and [47], most of the energy is present in the DC and the first few AC coefficients. An analysis has also been carried out in this work to examine the percentage of energy distribution among the DCT coefficients of continuous-tone images. The graph shown in Fig.3.4 is plotted by going through the following steps: first, a large database of continuous-tone grey-scale still images is taken, which also includes commonly used standard test images. These images are then transformed into frequency domain using DCT. After that, absolute values of AC coefficients, from every DCT block of each image, are summed up. The reason for taking absolute values of AC coefficients is because AC coefficients can also have negative values. Similarly, DC values are also added but absolute operation is not required as DC is always positive. In the next step, the 64^{th} AC coefficient is plotted, and then the sum of the 64^{th} and 63^{rd} AC coefficients is plotted. This goes on until the sum of the entire AC coefficients has been plotted.

In the last step, the sum of all AC coefficients and DC coefficient is plotted or in other words the sum of all the DCT coefficients in the DCT block is plotted. These plotted values are then normalized to the scale of 0-100. As seen from the graph in Fig. 3.4, approximately 0.4235 % of the energy is compacted in the last 54 DCT coefficients, and approximately 99.5765 % of the total energy is compacted in the first 10 DCT coefficients. As expected, most of the energy is in the DC coefficient which is approximately 93.484 % according to the performed analysis.

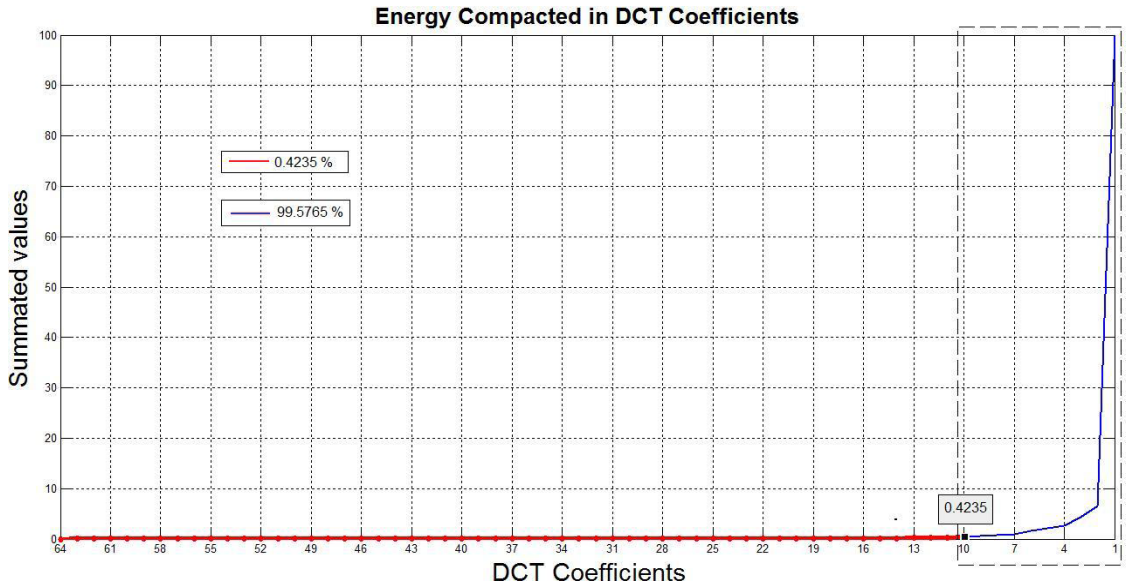


Figure 3.4: Graph showing the Energy Distribution among the DCT coefficients.

Also to determine the energy retained by each AC coefficient individually, a statistical analysis of the distribution of the energy present in the AC coefficients has been carried out. The normalized graph is plotted in Fig. 3.5 which shows the average values of the AC coefficients in the DCT block. A set of images were taken and their absolutes AC coefficient values are summed up. The DC value is not plotted in the graph shown in Fig. 3.5 as it will overshadow the remaining energy distribution in the AC coefficients because of its large value. Fig. 3.5 provides a clearer view of the energy contained in each AC coefficient.

Since the DC is always a large value thus it would be beneficial to split the DC coefficients into bitplanes. This can be done as follows: the DC coefficient from each DCT block is collected such that it forms of matrix. Then this DC matrix is transformed into binary representation thus forming bitplanes as shown in Fig. 3.6. Analysis to see the visual degradation caused by each bitplane is carried out. This analysis is as follows: first starting from the least significant bitplane each bitplane along with the previous bitplanes is set to zero. In other words, first least significant bitplane (DC1 = 0) is set zero and then second to the least significant bitplane along with the least significant bitplane (DC1 = 0 and DC2 = 0) is set to zero.

This continues until all the bitplanes are set to zero. After each step the similarity is measured between the obtained image and the original image. This similarity is the converted to percentage of dissimilarity and is plotted as shown in Fig. 3.7.

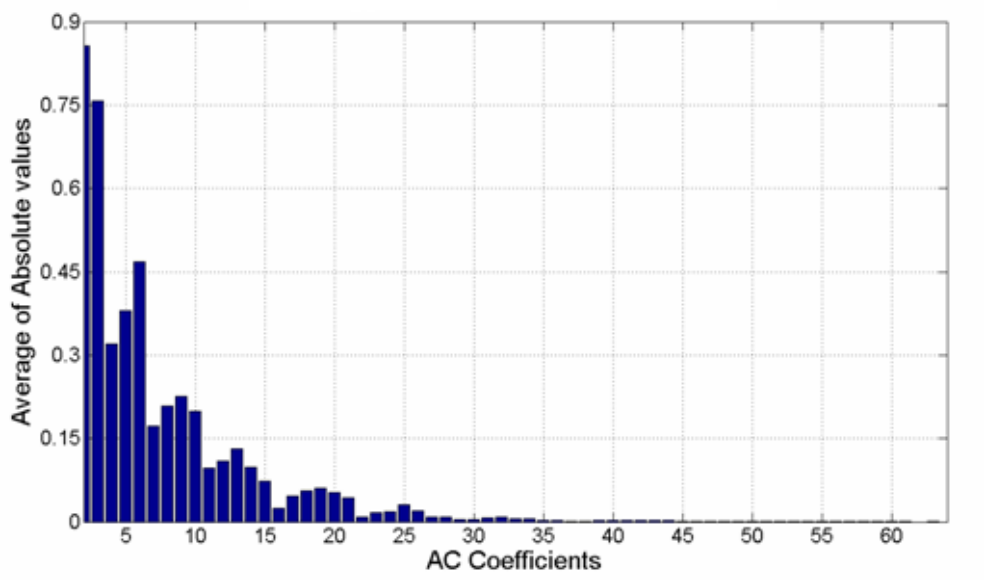


Figure 3.5: The graph shows the average normalized values of AC coefficients.

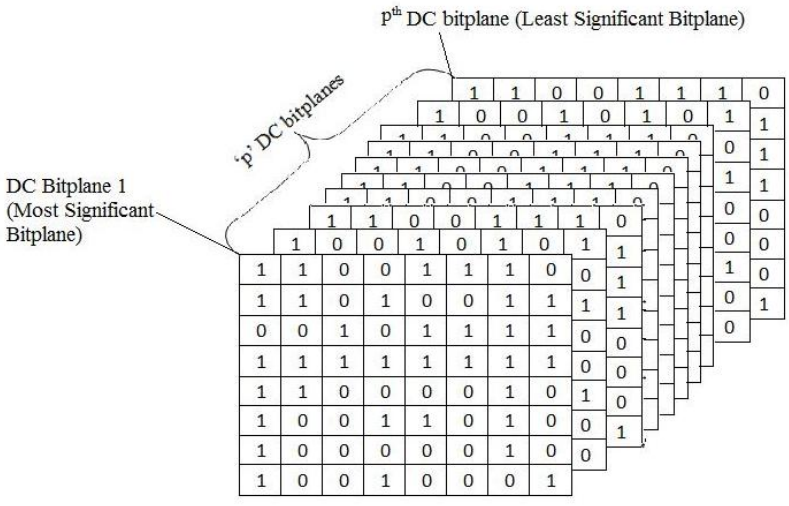


Figure 3.6: Collection of DC coefficient bitplanes.

It is clear from Fig. 3.4 that most of the energy is concentrated in between the first 30 values of the DCT block. Logically, manipulating the higher AC coefficient values can give a good level of perceptual encryption. Also, it is suggested in [47] that the encryption of the first few coefficients is sufficient to distort the content. Thus, based on these observations, AC coefficients are selected for carrying out perceptual encryption because of the gradual increase in the energy from 9th AC coefficient toward the 1st AC coefficient. Also from Fig. 3.7 one can see that fourth DC bitplane and on words can degrade the content up to 90%. Thus along with the AC coefficients the last four bitplanes of DC component are also selected to be scrambled to increase the degradation in the content. The remaining DC components bitplanes are selected for embedding the watermarking as only on average about 3% of the visual degradation can be caused by them.

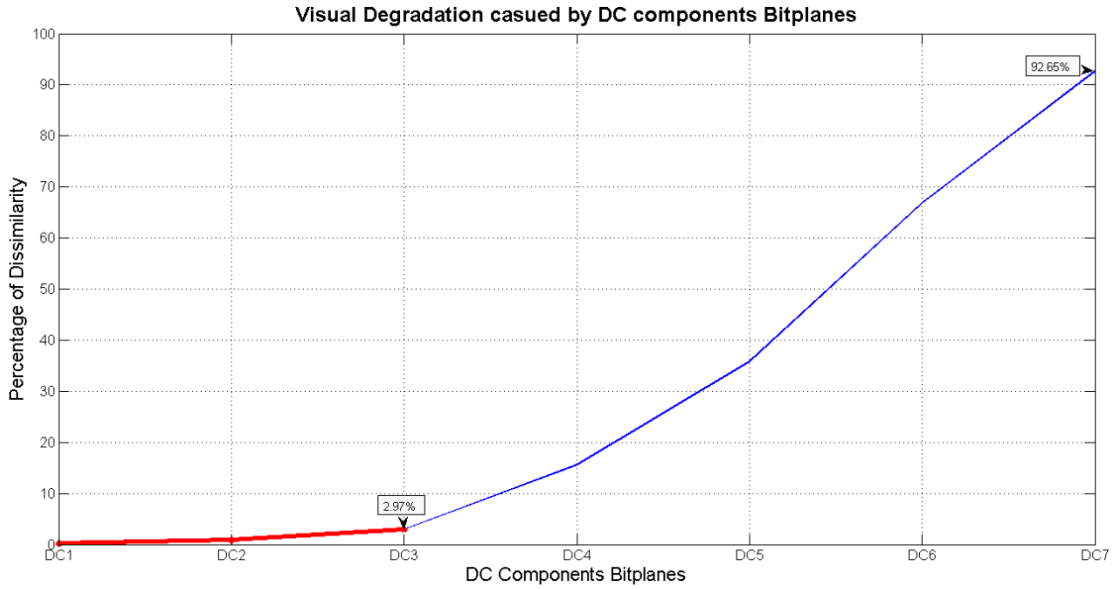


Figure 3.7: The graph shows the average percentage of dissimilarity after the DC component bitplanes are set to zero.

As seen from Fig. 3.7, for the case of perceptual encryption, if the first 9 AC coefficients are used, the amount of degradation can reach 72%. This amount of degradation can be increased to 93% if the last DC bitplanes are also used in perceptual encryption. For the purpose of watermarking, the remaining least important

bitplanes are used to embed the watermark. The choice of how many least significant bitplanes to be used from the remaining bitplanes is left to user.

3.3.1.4 Perceptual Encryption Using DCT Coefficients (Scrambler/ Descrambler)

Selected quantized AC coefficients and DC bitplanes are fed into a scrambler which encrypts the content to the required perceptual quality. Similarly the descrambler decrypts the content and brings the content to its original perceptual quality.

- **KEY (K_E)**: This key is provided to the scrambler to encrypt the AC coefficients and DC bitplanes to a certain perceptual quality requirement. The same key will be used to decrypt the encrypted data at the receiver's end. Thus this key needs to be transmitted on a secure channel; this will bring in the key management protocols into action.

How this perceptual encryption is carried out is as follows: Based on the conclusion from section 3.3.1.3 that the first 9 AC coefficients and last four DC bitplanes compact large energy in the DCT block and can be used for perceptual degradation in the image. In order to scramble the quantized DCT coefficients, the scrambler is placed after the quantization block in the JPEG image compression standard. The DCT coefficients are numbered according to zigzag order as shown in Fig. 3.8.

The DC coefficient of each block of 8×8 pixels is collected and these DC coefficients are arranged in the form of matrix. After that a binary conversion is performed on these DC coefficients to obtain '*p*' number of binary matrices or bitplanes as shown in Fig. 3.6.

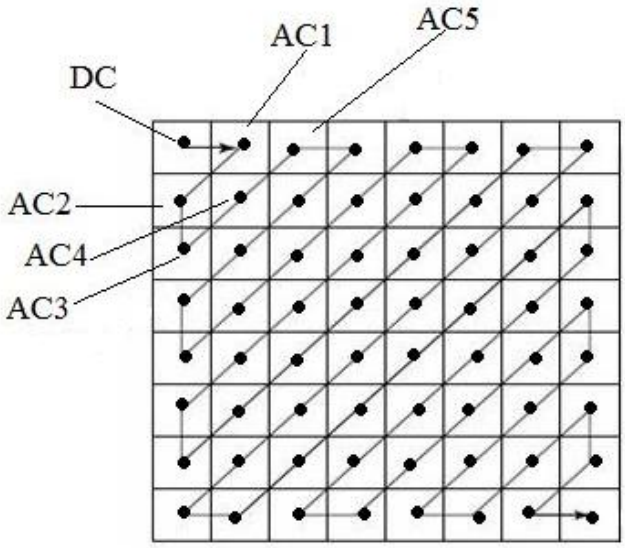


Figure 3.8: DCT Coefficient numbered according to Zigzag order.

The scrambling process is initiated by scrambling the last selected AC coefficient (9^{th} AC) followed by scrambling of the second to last AC coefficient (8^{th} AC). This process continues until all the selected AC coefficients have been scrambled. Then the scrambling of the DC bitplanes is initiated in the same order. First, 4^{th} DC bitplane is scrambled along with first nine AC coefficients then 4^{th} and 3^{rd} bitplanes are scrambled along with first nine AC coefficients and so on untill all the last four DC bitplanes are scrambled. After every step of scrambling the values of Objective Image Quality Assesment Metrics are measured which are required for the development of design curve to enables the selection of control factor or quality loss factor.

For the purpose of scrambling, any scrambler having an acceptable cryptographic security in scenario of media data encryption can be used. In this work, a chaotic scrambler adopted from [57-58] is used. The working of this scrambler is described in Appendix A.

3.3.1.4.1 Level of Perceptual Encryption - Control Factor

It is desirable to have control over then level of degradation. The Control / Quality loss Factor (CF/QF) is the factor that controls the amount of degradation in the content. The proposed perceptual encryption scheme enables one to degrade the quality of the content to a pre-determined level. The following quoted points from [21] regarding control factor should be kept in consideration in establishing the basis for selection of control factor,

> " *1) since there does not exist a well-accepted objective measure of visual quality of digital images and videos, the control factor is generally chosen to represent a rough measure of the degradation; 2) the visual quality degradations of different frames may be different, so the control factor works only in an average sense for all videos; 3) the control factor is generally selected to facilitate the implementation of the encryption scheme, which may not have a linear relationship with the visual quality degradation (but a larger value always means a stronger degradation); 4) when the control factor p = 1, the strongest visual quality degradation of the specific algorithm (i.e., of the target application) is reached, but it may not be the strongest degradation that all algorithms can produce (i.e., all visual information of the video is completely concealed).* "
>
> Text quoted from [21],
> Shujun Li, Guanrong Chen, Cheung, A., Bharat Bhargava,
> Kwok-Tung Lo, "On the Design of Perceptual MPEG-Video
> Encryption Algorithms".

The selection of control factor in the proposed scheme is made possible by the development of design curves using Objective Image Quality Assessment metrics that allows the flexible selection of control factor to degrade the quality of the content to required level.

3.3.1.5 Watermarking using DC components Bitplanes (Watermark Embedder / Extractor)

The quantized DC coefficient is watermaked in a DCT block using bitplane approach that will be described in later sections. Similarly, the watermark is extracted from the DC coefficients in the decoder part in the Watermark Extractor block.

- **KEY (K_W):** This is used to generate a random scrambler. The proposed scrambler of Appendix A generates a random position vector using the key as an initial condition for the chaotic map. The generated vector can be understood as indices of the pixel position where the watermark bits need to be embedded, usually in the least significant bitplane. The same key will be used in the decoder part where again the same position vector needs to be generated to extract the watermark bits from those locations. Like the key (K_E) used for scrambling in the perceptual encryption, K_W is also transferred on a secure channel.

- **Pixels position vector generation (Scrambler / Descrambler):** In this block the scrambler is used to generate the random position vector to embed the watermark bits in those positions. On the decoder part, the scrambler generates the same position vector using the same key used in the encoder part, to extract the watermark bits.

- **1-D to 2-D / 2-D to 1-D conversion:** A 2-D logo is converted into 1-D array of binary vector. Now as a 1-D array it is embedded as the watermark. Similarly, on the decoder end, the extracted watermark 1-D vector is converted into 2-D logo. As such, the technique allows not only 2-D logo, but also 1-D copyright information or data which identifies the creator of the content.

The basic idea for watermarking is to embed information (watermark) into DC component. Majority of the work that has been reported up till now has been done by manipulating the AC component [31-32], particularly using mid frequency or low frequency components in transformed domain. Because the DC component was not considered suitable for embedding the watermark, it was supposed that embedding the

watermark in it will degrade the quality of the image or video. The DC component is perceptually significant component and mostly, scaling and additive techniques were used to embed watermark bits which may cause some unwanted distortion in the content.

The emphasis of traditional frequency domain watermarking techniques is on AC component. Although DC component is perceptually significant, but it is argued and shown in [35, 39] that embedding a watermark in DC component can also be imperceptible and robust. Only few of the DC component based watermarking schemes have been reported [35-39]. The proposed watermarking technique combined with JPEG compression standard is based on using DC component that is decomposed into bitplanes [59]. In contrast to additive and scaling methods, in the proposed method the watermark bits are embedded into bitplanes using substitution technique. The proposed scheme is classified as blind watermarking because it does not require the original image on the receiver's end to extract the watermark.

3.3.1.5.1 Embedding Process

The embedding of watermark is carried out after the quantization process in JPEG compression standard as shown in Fig. 3.2. The embedding of watermark can be split into the following steps.

- **STEP 1:** After the quantization step in JPEG compression standard, the DC coefficient of each block of 8×8 pixels is collected. These DC coefficients are arranged in the form of $N \times N$ matrix. Then binary conversion is performed on these $N \times N$ DC coefficients to obtain 'p' number of binary matrices or bitplanes as shown in Fig. 3.6 in section 3.3.1.3.

- **STEP 2:** Least Significant Bitplanes (LSB planes) are then selected to embed the watermark bits. For experimental purposes, two least significant bitplanes are selected as a trade-off between imperceptibility, capacity and robustness to substitute the watermark on them.

The selection of bitplanes is discussed in section 4.3.1. The watermark of size $N \times N$, that is to be embedded which can either be a logo or any other information, is converted into binary representation and arranged in 1-D array such that $1 \leq L \leq N \times N$.

- **STEP 3:** *N/2* random positions are selected from each DC component bitplane to embed the watermark bits. For the purpose of selecting the random positions, any scrambler with a key which generates random positions can be used. The proposed watermarking scheme adopts a Chaotic Seed Based Scrambler [57-58], the same scrambler as used in the proposed perceptual encryption scheme to scramble AC coefficients and DC bitplanes as described in previous sections. This scrambler has optimal property of spread and dispersion. Spread measures the distance between the elements that are near to each other before permutation. Dispersion measures the randomness in spread. These two properties are of great significance to ensure that the recovery of watermark is not possible without the knowledge of the correct key.

- **STEP 4:** The watermark bits are then substituted in place of random positions generated for each DC component bitplane, and the compressed watermarked data is obtained. If the JPEG decoder is used without the watermark extraction block a watermarked image is obtained, then the watermark can also be independently extracted from the watermarked image.

In implementation the selected bitplanes are converted and concatenated into 1-D array and is represented by P_{DCb}. Where $P_{DCb}(i)$ is the coefficient bit at location i. Mathematically the embedding process is as follows,

$$P_{DCb}(i) = \begin{cases} W_{(k)} & if \quad (i) = S_p(k) \\ P_{DCb}(i) & if \quad (i) \neq S_p(k) \end{cases} \tag{3.1}$$

Where $1 \leq i \leq$ *(Number of DC coefficients* $\times$ *Number of Selected bitplanes)*. S_p is the generated position vector using the key K_W and $W_{(k)}$ is the watermark bit. k is the number of bits in watermark when it is converted into 1-D array.

3.3.1.5.2 Extraction Process

The watermark extraction process at the decoder side consists of the following simple steps.

- **STEP 1:** DC coefficients are separated from the data obtained from the entropy decoder. These coefficients are arranged in the form of the $N \times N$ matrix as done in the embedding process, and binary conversion is performed to get the DC component bitplanes.
- **STEP 2:** Random positions are then generated by the scrambler using the same key as used in the watermark embedding process, and then the watermark bits are collected from the corresponding positions in that particular bitplanes, where the watermark is embedded.
- **STEP 3:** The obtained watermark bits are in 1-D array. The collected bits are then transformed from 1-D array to 2-D matrix to get the extracted binary watermark.

Mathematically the extraction process is as follows,

$$if \quad i = S_p(k) \quad then \quad W_{exb(k)} = P_{DCb}(i) \tag{3.2}$$

Where W_{exb} is the extracted watermark bit. The watermark extraction takes place only from the positions generated by the scramble. The proposed scheme is classified as frequency domain, blind and imperceptible watermarking technique.

3.3.1.6 Data Aggregator

The functionality of this block is to combine the data which have been watermarked and encrypted in the encoder part. Similarly, in the decoder part, again its function is to combine the data after the data have been decrypted and the watermark is extracted from it.

The rest of the JPEG Encoder and Decoder blocks are the common operations carried out in JPEG compression standard and their working is described in [46].

3.4 Methodology for Performance Evaluation

The performance of the proposed scheme needs to be evaluated more carefully as compared to other schemes which are generally not developed for joint scenario. One of the important issues involved in the evaluation as well as the design of JPEW is the difficulty to measure similarity between two images. One of the most commonly used metric to measure the degradation in multimedia content is PSNR (peak signal-to-noise ratio). PSNR, in fact measures the number of errors introduced in the multimedia content. The reason behind its intensive use is the unavailability of more accurate measure but still PSNR is in use. The proposed design requires the involvement of objective metrics to measure the,

- Level of degradation in the image so that an accurate estimation of range could be provided.
- Level of perceptual security (discussed in later sections).
- Level of imperceptibility in the watermarking scheme.
- Similarity between the original and extracted watermarks.

To accomplish the abovementioned tasks, newly designed Objective Image Quality Assessment Metrics (IQAs) are used along with PSNR [48]. Since these IQAs have emerged only recently, thus they have not been used much widely but are gaining popularity. These IQAs includes,

- Structural SIMilarity (SSIM) [49].
- Multi-Scale Structural SIMilarity (MS-SSIM) [50].

- Visual Information Fidelity (VIF) [51].
- Pixel-Based Visual Information Fidelity (VIFP) [51].
- Visual Signal-to-Noise Ratio (VSNR) [52].
- Universal Quality Index (UQI) [53].
- Image Fidelity Criterion (IFC) [54].
- Weighted Signal-to-Noise Ratio (WSNR) [56].

The usage of these IQAs i.e. SSIM, MS-SSIM, VIF, VIFP and UQI, can also be regarded as one of the novel aspect of the proposed design because these IQAs are used in the proposed design intensively for the first time. Detailed functionality of these IQAs can be found in corresponding publications (also see Appendix B for their interpretation).

The performance of perceptual encryption scheme is evaluated in terms of measuring the perceptual degradation caused in the images by the encryption of the selected parameter and the security. To measure the degradation in the content the abovementioned IQA's are used. Security of the scheme is ensured by assessing the strength of the proposed scheme against image restoration techniques, Attack-Zero which falls under ciphertext-only attack, key recovery and rearrangement attack. For image restoration techniques the perceptually encrypted image was placed under common filtering techniques i.e. wiener filtering etc and is presented in section 4.4.1.1. Then another attack was done on the perceptual encrypted image in which it is assumed that attacker has the knowledge of the data that has been encrypted and the attacker sets the encrypted data equal to zero. This attack is named as Attack-Zero and is presented in section 4.4.1.2. The next possible attack on the perceptually encrypted image in then when attacker fails to recover good quality image from the abovementioned attacks is Rearrangement attack on the perceptually encrypted image.

A case of Rearrangement attack has also been discussed and presented in section 4.4.2. A discussion on key size and key management has been made in section 4.4.5 & section 4.4.5.1, respectively. The performance of the watermarking scheme is assessed in terms of imperceptibility and robustness. Imperceptibility involves measurement of similarity between original image and watermark image, this similarity is measured using the abovementioned IQA's. A study has been carried out in section 4.3.1 to determine the imperceptibility of the scheme. Robustness of the scheme is measured by placing the watermarked image under common signal processing modifications caused during the transmission and storage of the image, and comparing similarities. This is presented in section 4.4.4. An attack on watermarking scheme known as watermark replacement attack has also been discussed within the scope if the attacker tries to replace the embedded watermark, and is presented in section 4.4.3.

Another important factor in performance evaluation of the proposed scheme is the effect of perceptual encryption on compression ratio. This has not been given its due importance in the literature. However, its importance cannot be denied when the schemes are integrated with compression standard, and the compression efficiency must be determined in the case of encryption scheme. The compression analysis is basically the comparison between the compression ratios obtained before any encryption process and the compression ratios obtained after encrypting the selected data. The compression analysis of the proposed encryption scheme is presented in detail in section 4.2.3.

3.5 Summary

In this chapter, a Joint Perceptual Encryption and Watermarking Scheme is presented. The joint architecture is the combination of a perceptual encryption scheme and a watermarking scheme. Both of these schemes are integrable with JPEG compression standard. The perceptual encryption scheme is presented in the first half

of the chapter, and the selection of control factor discussed. The proposed perceptual encryption scheme is based on AC coefficients. The scheme provides certain levels of encryption that degrades the content according to one's own quality requirement. Later on, a DC component bitplanes based watermarking scheme is presented, and the embedding and extraction process are discussed in detail.

CHAPTER 4

PERFORMANCE EVALUATION OF JPEW

4.1 Introduction

In the previous chapter, a Joint Perceptual Encryption and Watermarking scheme (JPEW) is proposed and its design methodology and the design components involved are discussed. In this chapter, the results of performance evaluation of the proposed scheme are presented and explained. Performance evaluation of JPEW consists of Performance Evaluation of Perceptual Encryption Scheme and Performance Evaluation of Watermarking Scheme, and is presented in this chapter accordingly. Additionally, these proposed schemes are compared with corresponding existing scheme in the literature. Lastly, the overall security of JPEW is analyzed in detail.

4.2 Performance Evaluation of Perceptual Encryption scheme

The results of perceptual encryption scheme are discussed in the upcomming sections. In addition, the selection of the control factor / quality loss factor is explained with respect to the design curve. Compression analysis of the proposed perceptual encryption scheme is also carried out. Additionally, a comparison of the designed perceptual encryption scheme with an existing Reversible Histogram Spreading Technique (RHS) based perceptual encryption scheme proposed by Yang *et al*. [60] in 2009 is also carried out.

4.2.1 Perceptual Degradation using AC coefficients and DC Bitplanes

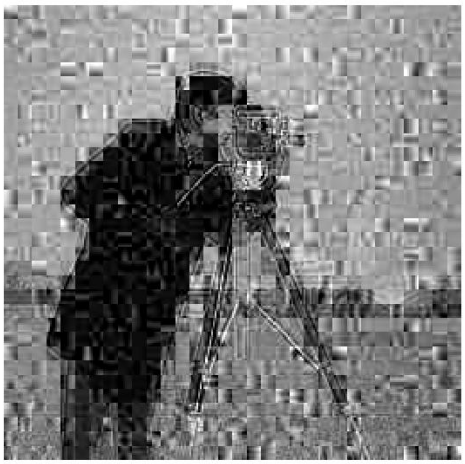
The first 9 AC coefficients and last 4 DC bitplanes are selected to be scrambled to carry out perceptual encryption. The AC coefficients are read in zig-zag order from the DCT block. The first 9 AC coefficients represent progressively lowest to higher high frequency coefficients. Using all the first 9 AC coefficients give rise to a fixed but largest amount of quality degradation and the DC componant bitplanes further increase the level the of degradation. However, if one carries out perceptual encryption for the nineth coefficient alone, the amount of degradation is least. This process of encryption, nineth coefficient then nineth and eighth and so on, can thus give rise to a design curve explained in section 4.2.2. The process is commenced by encrypting only the 9^{th} AC coefficient, then 9^{th} with 8^{th} AC coefficient are encrypted together. As mentioned earlier, encryption is implemented through the process of scrambling, so the words 'encryption' and 'scrambling' are used interchangeably. Then 9^{th}, 8^{th} and 7^{th} AC coefficients are scrambled together, this goes on up to the 7^{th} DC bitplane. So that the entire first 9 AC coefficients and last 4 DC bitplanes are scrambled. After every step of scrambling the AC coefficient and DC bitplane, the values of SSIM, MS-SSIM, VIF, VIFP, UQI, IFC, VSNR and PSNR are calculated and are shown in Table 4.2.

Fig. 4.1(a, b and c), are the resultant images after undergoing the degradation when only first 9 AC coefficients are scrambled. It can be seen that the minor details in the image are no more visible, and still the image as a whole is meaningful. Here it is noticed that as we increase the number of AC coefficients and DC bitplanes in the scrambling process, the level of visible information through the content decreases. After encrypting all 9 AC coefficients, one can hide 48% to 72%, (estimated in terms of SSIM) and 22% to 44% (estimated from MS-SSIM) of perceivable information in the image. On average, 62.9% and 37.3% of the information is hidden as estimated by SSIM and MS-SSIM, respectively. The estimated ranges of percentage of hidden information measured from the other metrics are shown in Table 4.1.

Table 4.1: Estimated Ranges of Percentage of Hidden Information after Encrypting First 9 AC Coefficients

Metric	Range
VIF	89.1% to 95%
VIFP	83.6% to 94.2%
UQI	63.6% to 89.7%

The percentage of the perceivable hidden information varies from image to image. Most of the continuous-tone still images fall in this estimated range. Here it is worth mentioning that the proposed scrambling scheme only scrambles the coefficients in its own orbit or in other words if AC 9 of any quantized DCT block is scrambled then that AC 9 can only replace AC 9 in any other quantized DCT block, it cannot take place of AC 4 or AC 3 or any other DCT coefficient.



(a)

(b)

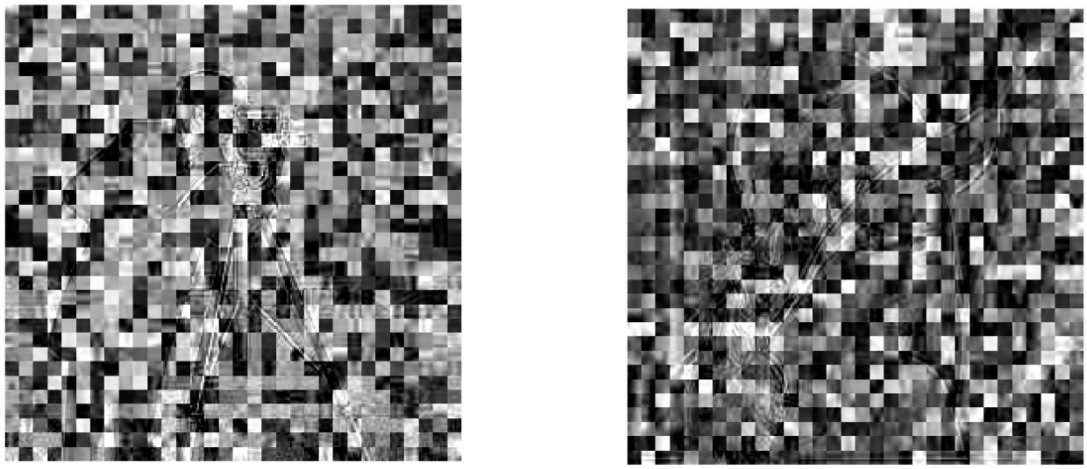
(c)

Figure 4.1: (a) 256 × 256 Cameraman image with its first nine AC coefficients scrambled. (PSNR = 17.52, SSIM = 0.2977, MS-SSIM = 0.5448, VSNR = 6.6485, VIF = 0.0629, VIFP = 0.0707, UQI = 0.1709, MSE = 1095.09, IFC = 0.3703, WSNR = 15.6407, SNR = 11.9458).
(b) 256 × 256 Lena image with its first nine AC coefficients scrambled. (PSNR = 17.86, SSIM = 0.2973, MS-SSIM = 0.6233, VSNR = 8.1683, VIF = 0.05919, VIFP = 0.0866, UQI = 0.2301, MSE = 1063.52, IFC = 0.3760, WSNR = 13.8646, SNR = 10.6474).
(c) 512 × 512 Fishing boat image with its first nine AC coefficients scrambled. (PSNR = 19.86, SSIM = 0.3280, MS-SSIM = 0.5888, VSNR = 6.9162, VIF = 0.0654, VIFP = 0.0734, UQI = 0.2076, MSE = 671.1398, IFC = 0.4480, WSNR = 18.0747, SNR = 14.5201)

Table 4.2: The Corresponding Metrics Average Values Against Each Level of Perceptual Encryption (From AC9 to DC1).

No. of Coefficient / IQA Metric	AC 9	AC 9 ↓ AC 8	AC 9 ↓ AC 7	AC 9 ↓ AC 6	AC 9 ↓ AC 5	AC 9 ↓ AC 4	AC 9 ↓ AC 3	AC 9 ↓ AC 2	AC 9 ↓ AC 1	AC9 ↓ DC4	AC9 ↓ DC3	AC9 ↓ DC2	AC9 ↓ DC1
PSNR	31.8820	30.3391	29.1753	28.2322	26.4211	25.3154	24.3928	21.9117	20.2384	19.6017	18.7351	15.9059	12.8113
SSIM	0.8654	0.8196	0.7762	0.7366	0.6699	0.6155	0.5640	0.4603	0.3709	0.3598	0.3282	0.2743	0.2159
MS-SSIM	0.9755	0.9588	0.9420	0.9299	0.8895	0.8581	0.8246	0.7229	0.6267	0.5917	0.5472	0.4562	0.2776
VSNR	27.8294	24.290	22.0990	20.8882	18.0091	16.4971	15.2276	12.1003	10.0456	9.8006	8.5187	5.9207	2.0554
VIF	0.5752	0.5104	0.4265	0.3654	0.2859	0.2376	0.1881	0.1236	0.0731	0.0696	0.0620	0.0571	0.0483
VIFP	0.5089	0.4513	0.4075	0.3779	0.3103	0.2607	0.2275	0.1431	0.0905	0.0892	0.0781	0.0608	0.0493
UQI	0.7004	0.6431	0.5970	0.5600	0.4967	0.4448	0.3995	0.2975	0.2126	0.1983	0.1764	0.1495	0.1248
IFC	3.9629	3.3941	2.7098	2.2769	1.7479	1.4249	1.1063	0.7157	0.4218	0.4084	0.3519	0.3195	0.2738

Note: Measured values for individual image in the database are not presented in the thesis due to limited space.



(a) (b)

Figure 4.2: (a) 256 × 256 Cameraman image with its first nine AC coefficients and last 4 DC bitplanes scrambled. (PSNR = 8.5107, SSIM = 0.1183, MS-SSIM = 0.0794, VIF = 0.0312, VIFP = 0.0219, UQI = 0.0764, IFC = 0.1830). (b) 256 × 256 Lena image with its first nine AC coefficients and last 4 DC bitplanes scrambled. (PSNR = 9.6455, SSIM = 0.1315, MS-SSIM = 0.1009, VIF = 0.02554, VIFP = 0.0176, UQI = 0.0843, IFC = 0.1616).

Fig. 4.2(a & b), shows the images obtained after first nine AC coefficients and last 4 DC bitplanes have been scrambled. Averaged over 200 test images, an image is distorted about 78.4 % as estimated by SSIM and 72.2 % as estimated by MS-SSIM, when entire selected data for the perceptual degradation is scrambled using first 9 AC coefficients and last 4 DC bitplanes. The percentage of distorted information in the second case from the remaining metrics is shown in Table 4.3.

Table 4.3: Estimated Ranges of Percentage of Hidden Information after Encrypting All Selected Data

Metric	Range
SSIM	57.3% to 93.7%
MS-SSIM	45.3% to 97.7%
VIF	90.4% to 97.66%
VIFP	87.8 % to 98.6%
UQI	69.3% to 99.2%

It can be seen from the Fig 4.2, that no more visual information is visible from the images. Thus all the visual information can also be encrypted using the proposed scheme and can be called as a complete encryption scheme in a sense that it completely encrypts the visual information.

4.2.2 Development of Design Curve and Selection of Control Factor

The Control / Quality Loss Factor in this proposed perceptual encryption scheme allows degradation in the content in a gradually manner. Although the degradation introduced in the content cannot be perfectly linear, the next level must still be more degraded then the previous one. The calculated percentages corresponding to control factors vary for different types of images. The control factor can be selected from the design curves shown in Fig. 4.3 that is obtained by averaging the results over several test images. The database for the test images consists of 200 images of different size and texture (including natural sceneries, images of objects, facial images and standard test images). The percentage is calculated corresponding to the values of SSIM, MS-SSIM, VIF, VIFP, and UQI. This provides the user to have more control over the

degradation of the multimedia content as any of these IQAs can act as either control or quality loss factor.

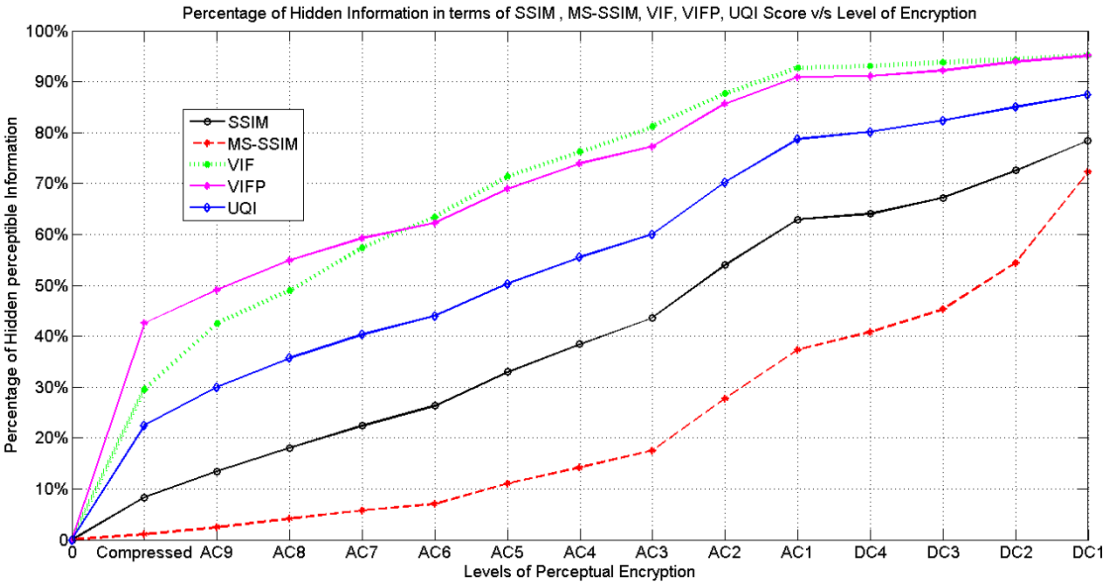


Figure 4.3: The percentage of hidden perceivable information through content and the corresponding number of AC coefficients and DC bitplanes need to be encrypted.

The design curve is produced by plotting the average values of SSIM, MS-SSIM, VIF, VIFP and UQI over all the test images in the database, as these metrics provide more accurate measure of similarity between the images, and also because they represent recent developments in quality measurements. Mathematically the Control Factor can be defined as,

$$CF(k,l) = \sum_{i=9}^{k} AC_i + \sum_{i=1}^{l} DC_i \qquad (4.1)$$

where $1 \le k \le 9$ and $1 \le l \le 4$. The selection of control factor from the above shown design curves is made for following scenarios:

- Degradation required in content is 50 %
- Design Curve employed is UQI

Then from the design curve, it can be seen that AC coefficient from 9 to 5 are required to be encrypted.

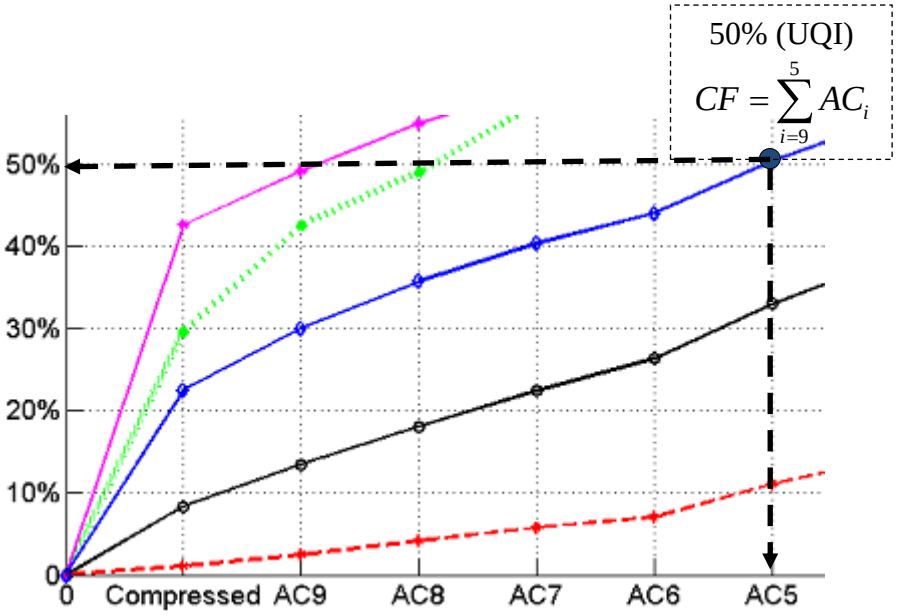


Figure 4.4: Selecting CF for 50% using UQI.

The graphs shown in Fig.4.3 are very near to being linear although in the previously discussed perceptual encryption schemes, the issue of linearity is not discussed and they have not strived for linearity in the degradation of the content. From the point quoted below, the control factor or the quality loss need not necessarily be linear with the degradation.

"……..3) the control factor is generally selected to facilitate the implementation of the encryption scheme, which may not have a linear relationship with the visual quality degradation (but a larger value always means a stronger degradation) …"

Text quoted from [21],
Shujun Li, Guanrong Chen, Cheung, A., Bharat Bhargava, Kwok-Tung Lo, "On the Design of Perceptual MPEG-Video Encryption Algorithms".

However the proposed scheme tends to approximate the linear relationship between the control factor and the degradation introduced in the multimedia content.

4.2.3 Compression Analysis

One of the important aspects of encryption schemes is the impact it has on the compression standard. An ideal encryption scheme does not affect the compression ratios at all. The effect on compression ratio by the proposed perceptual encryption scheme is negligible and does not increase the size of the content. The RUNLENGTH coding in JPEG compression standard is based on 8×8 block and also only the difference of the consecutive DC coefficients is encoded (as described in [46]). The scrambling is performed on the 8×8 DCT blocks and the positions of AC coefficients are changed, which in turn affects the RUNLENGTHs. The compression ratio is also calculated in the above mentioned experiment after encrypting each AC coefficient and DC bitplanes. As can be seen from the graph shown in Fig. 4.5, there is a minor change in the average compression ratios measured after encrypting each AC coefficient and DC bitplane. The change in compression ratio as depicted from the graphs shown in Fig. 4.5 is from 22:1 to 18:1. Thus, no significant change in compression ratio is observed and the proposed scheme can be regarded as compression friendly.

The scrambling of each coefficient is in its own orbit[6]. Mostly the size of the AC coefficients in same orbit but in other DCT blocks is approximately the same. In this scrambling process, if the larger coefficient takes the position of the smaller coefficient or vice versa then that would certainly change the compression ratio. So, there is a possibility that in the scrambling process there may be a case when the AC coefficients are arranged such that it will result in optimized compression ratio. However the probability of this kind of arrangement of the bits is very low.

The compression analysis has not been given due importance in the literature in spite of the fact that it is of considerable importance when dealing with the scenario where the content is compressed as well as encrypted.

[6] It means that 5^{th} AC coefficient can only take the position of other 5^{th} AC coefficient in the some other DCT block.

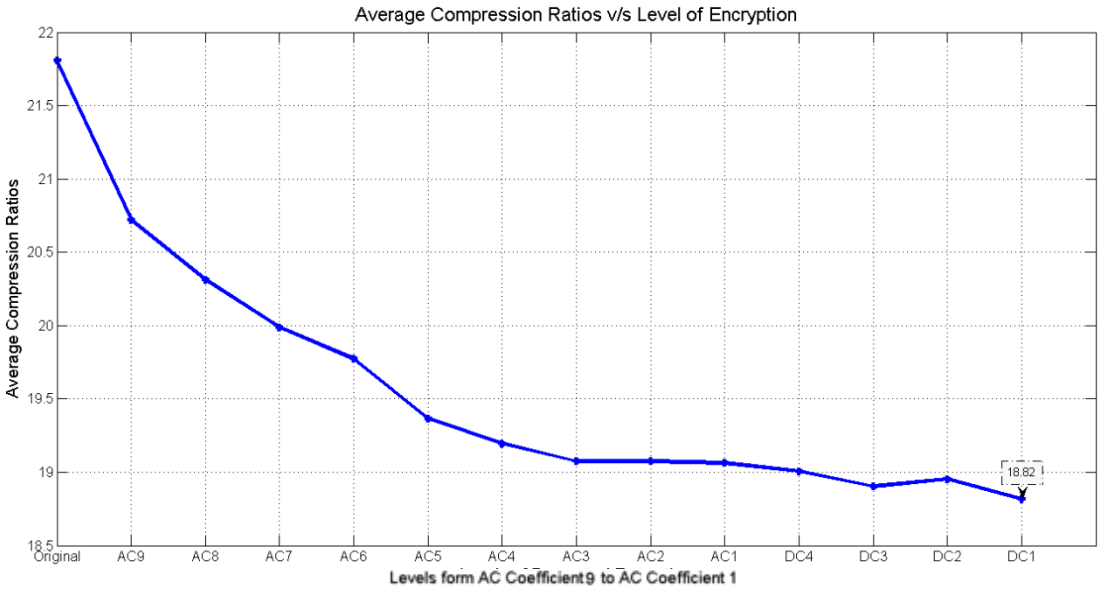


Figure 4.5: Average Compression Ratios against each level of Perceptual Encryption.

4.2.4 Comparison with Reversible Histogram Spreading (RHS) based Perceptual Encryption Scheme [60]

Herein, the proposed perceptual encryption scheme is compared with a perceptual encryption based on Reversible Histogram Spreading Technique [60] that was proposed by *Yang et al*. in 2009. RHS based perceptual encryption scheme is recently proposed scheme which was implemented on images thus, enabling a comparison can be made between the proposed scheme and RHS based technique. The reversible histogram spreading technique was carried out in spatial/pixel domain. The scheme proposed by *Yang et al.* comprised of two steps. In the first step, the image was divided into non-overlapping equal-sized blocks of pixels i.e. $M \times N$. Intra-block pixel shuffling was then performed on each block, using an encryption algorithm based on baker map [61]. In the second step, histogram flattening was carried out. The process of histogram flattening is as follows: From each block, every two neighbouring pixels were grouped together. In other words, if the pixel is represented by P_i where $i = \{1, 2, 3 \ldots M \times N\}$ then the paired neighbouring pixels can be represented as P_{2l-1} and P_{2l},

where $l = \{1, 2, 3 \ldots M \times N/2\}$. Then each pair of pixels was scanned and the following operations were carried out,

$$\begin{Bmatrix} X_l' \\ Y_l' \end{Bmatrix} = \begin{cases} \begin{Bmatrix} Y_l + 1 \\ X_l - 1 \end{Bmatrix} & \text{if} \quad X_l > L_{\min} \quad \text{and} \quad Y_l < L_{\max} \\ \begin{Bmatrix} X_l \\ Y_l \end{Bmatrix} & \text{Otherwise} \end{cases} \tag{4.2}$$

Here X_l and Y_l are the pixel-pair values and L_{min} and L_{max} are the minimum and maximum grey level values in the block. The increase in degradation in the image is dependent on the number of iteration and this can go up to 1000. As compared to this scheme, the proposed scheme is implemented in transform domain and is compliant with popular compression standard. Encryption in transform domain provides more flexibility as compared to pixel domain. In transform domain, the significant data and insignificant data can be easily identified, which is not the case in pixel domain.

4.2.4.1 Computational Load

To determine the number of operations required to degrade the image to a certain level, consider an image of size $M \times N$, where M is the number of rows and N is the number of columns in the image. The image is divided into blocks of size $m \times n$. The total number of DCT blocks in the image will be $L = (M \times N) / (m \times n)$. If the number of arrays, that needs to be permuted, is represented by 'S' and the size of each array is $1 \times L$. Then, size of the scrambling matrix to permute an array 'S' of size $1 \times L$ will be $L \times L$ and the total number of multiplication operations required will be $1 \times L \times L = L^2$ (multiplication operations required to permute one array of elements). The total number of multiplication operations required to permute 'S' arrays will be $S \times L^2$.

For the proposed perceptual encryption scheme: if, $M = 256$, $N = 256$, $m = 8$, $n = 8$, then $L = 64$ and $S = 9$ (for the case when the first 9 AC coefficients are considered for perceptual degradation). In case of proposed perceptual encryption scheme, the total number of multiplication operations when two matrices are being multiplied will be

'L'. Since in the proposed scheme, the scrambling matrix has one '1' in row and column, so the multiplication with zero is not considered. The number of multiplication operation required in this case will be $S \times L = 9 \times (64) = 576$. Now also considering that last four DC bitplanes are scrambled then the value of S and L will be 4 and $(64)^2 = 4096$, respectively. The number of multiplication operation required in this case will be $S \times L = 4 \times (4096) = 16384$. The total maximum operations required in the proposed perceptual encryption scheme will be 576 + 16384 = 16960.

For the case of RHS based perceptual encryption scheme, the scheme consists of two steps. For the first step, similar to the proposed scheme, if $M = 256$, $N = 256$, $m = 8$, $n = 8$, then $L = 64$ and $S = 64$ (as the entire coefficients in the DCT block are considered). The total number of multiplication operations required in this case will be $S \times L^2 = 64 \times (64)^2 = 262144$. For the second step, the said scheme implements the operations of comparison, addition and subtraction. The number of comparison, addition and subtraction required are $L \times (m \times n)$, $L \times (m \times n/2)$ and $L \times (m \times n/2)$, respectively. Suppose, the number of iterations is represented by 'k', thus the total number of comparison, addition and subtraction operations required will be 'k' times $L \times (m \times n)$, $L \times (m \times n/2)$ and $L \times (m \times n/2)$, respectively. For example if $k = 1000$, then the total number of comparison will be 4096000, total number of additions will be 2048000 and total number of subtraction will also be 2048000. The value to 'k' can increase thus increasing number of comparison, addition and subtraction operations. This clearly indicates that the number of computation required to degrade the image are lesser in the proposed scheme as compared to RHS based perceptual encryption scheme and the proposed scheme provides a better selection of control factor using IQA metrics, which is not addressed in RHS scheme.

Table 4.4: Table of comparison between proposed perceptual encryption scheme and RHS based perceptual encryption scheme.

Features /Characteristics	**Proposed Perceptual Encryption Scheme**	**RHS Based Perceptual Encryption scheme [60]**
Domain	DCT domain	Spatial / Pixel
Number of Operation	Maximum 9 AC coefficients and 4 DC bitplanes need to be encrypted e.g. for an image of size 256×256, total number of multiplication operations required are equal to 16960.	The number of multiplication operations required, an image of size 256×256, for the first step is equal to 262144. Number of operations for second step : Comparisons = 4096000 Additions = 2048000 Subtractions = 2048000
Control Factor	Can be chosen from the developed Design Curve	No specific value of degradation, to increase degradation need to increase the number of iterations
Joint encryption and watermarking framework compatible	Yes	No
Effect on Compression Ratios	Minor	Not presented
Perceptual Security	Both Schemes are Perceptually Secure against i) Wiener filtering based image restoration with filter type 'unsharp' and 'gaussian'. ii) Image denoising by the phase preservation method iii) Image Enhancement by the anisotropic diffusion method.	

4.3 Performance Evaluation of the Proposed Watermarking Scheme

The performance of the proposed watermarking scheme can be evaluated in terms of its three main properties, namely, imperceptibility, robustness and security. Imperceptibility is the most important attribute of a watermarking scheme in the discussed joint design. The security of the watermarking scheme is evaluated in terms of the replacement attack. Similarly the robustness of the proposed watermarking scheme is assessed by placing the watermarked image under common image processing techniques. The security and robustness of the watermarking scheme is discussed with the overall security of the proposed Joint Perceptual Encryption and Watermarking Scheme in section 4.4, respectively. Additionally, a comparison of the proposed watermarking scheme is carried out with an existing Quantization Index Modulation based watermarking scheme in [39] and is presented in section 4.3.2. Also a discussion has been made regarding the implementation of the proposed watermarking scheme on medical images in section 4.3.1.1.

4.3.1 Imperceptibility

As an invisible/imperceptible watermarking strategy, the watermarked image should be identical with the original image; therefore, there should be no degradation in the image's perceptual quality after embedding the watermark in it. To study how imperceptible the proposed watermarking is, an experiment is carried out to investigate the suitable quantized DC-component bitplanes to embed the watermark bits in without degrading the quality of the image perceptually. The quantized DC coefficients are collected and arranged into bitplanes. Starting from Least Significant Bitplane, each bitplane is set equal to zero. To measure the similarity between the original image and the resultant image, objective image quality assessment metrics such as Structural Similarity (SSIM) and Multi-Scale Structural Similarity (MS-SSIM) are used and PSNR values are also calculated to enable a comparison between the proposed watermarking technique with the existing schemes.

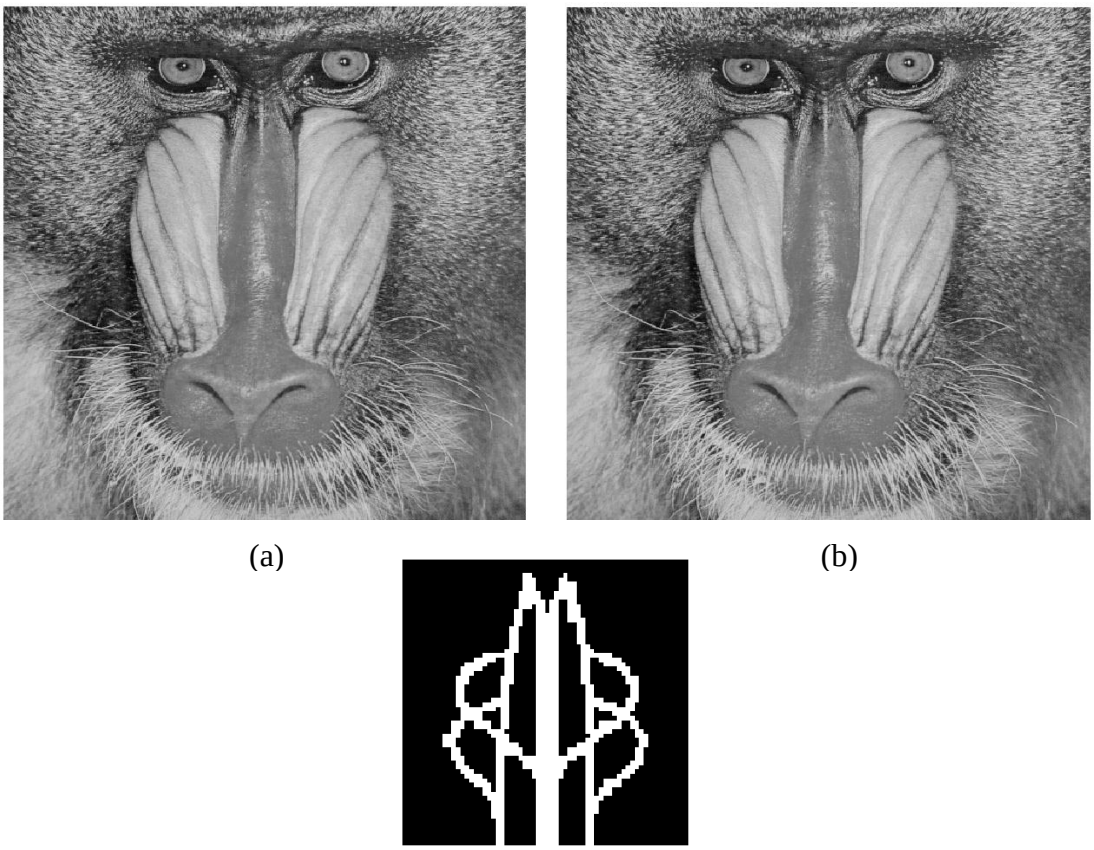
The bitplanes are put equal to zero individually as well as collectively. In other words, first only the 1st Least Significant Bitplane is set to zero, then 1st and 2nd Least Significant Bitplanes are set to zero and so on until all three least significant bitplanes have been set to zero. The corresponding average PSNR, SSIM and MS-SSIM values are shown in Tables 4.5 & 4.6. The values are shown for three least significant bitplanes.

The entries in Table 4.5 and 4.6 are for typical images with neither too strong texture nor too little. From the analysis of the table, it can be concluded that three Least Significant Bitplanes together contain very insignificant fraction of total energy, so they are suitable to embed watermark. However, the proposed scheme can also be further refined, where the selection of the bitplanes can be made adaptive to Human Visual System (HVS) and the texture information in the image but this will result in increased computational cost. This will not be suitable in the case of real-time processing of the content. More number of bitplanes can be used for images having a strong texture which again involves extra processing to determine which image has strong texture as done in few proposed watermarking schemes in [62-63].

Another important characteristic of watermarking scheme is the amount of information it can hold without degrading the content perceptually, it is also known as **payload**. The payload in the proposed scheme is equivalent to two times the number of DC coefficients in the transformed image when two Least Significant Bitplanes are being used.

$$Payload = \#\ of\ Bitplanes \times \#\ of\ DC\ coefficient\ in\ Transformed\ Image$$

It is important to mention that the relationship between the image size and the watermark size is also of significant importance and affects the perceptual quality of the image. To retain good perceptual quality of the image the watermark must be distributed over a number of Least Significant Bitplanes without losing the texture information of the image. As seen from Table 4.5, the proposed watermarking scheme satisfies the property of imperceptibility and does not degrade the image quality perceptually.



(a) (b)

(c)

Figure 4.6: (a) 512×512 Original baboon image.
(b) 512×512 Watermarked baboon image
(SSIM = 0.9956, MS-SSIM = 0.9955)
(c) 64×64 watermark (Universiti Teknologi PETRONAS logo).

Table 4.5: Measured Average Values after Removal of Each Least Significant Bitplane.

DC Bitplanes / Metric Values	PSNR	SSIM	MS-SSIM
Bitplane 1	45.3394	0.9971	0.9982
Bitplane 2	39.3102	0.9891	0.9936
Bitplane 3	33.4471	0.9658	0.9795

Table 4.6: Measured Average Values after the Collective Removal of Least Significant Bitplane.

DC Bitplanes / Metric Values	PSNR	SSIM	MS-SSIM
Bitplane 1 to 2	35.0285	0.9825	0.9911
Bitplane 1 to 3	29.1229	0.9438	0.9717

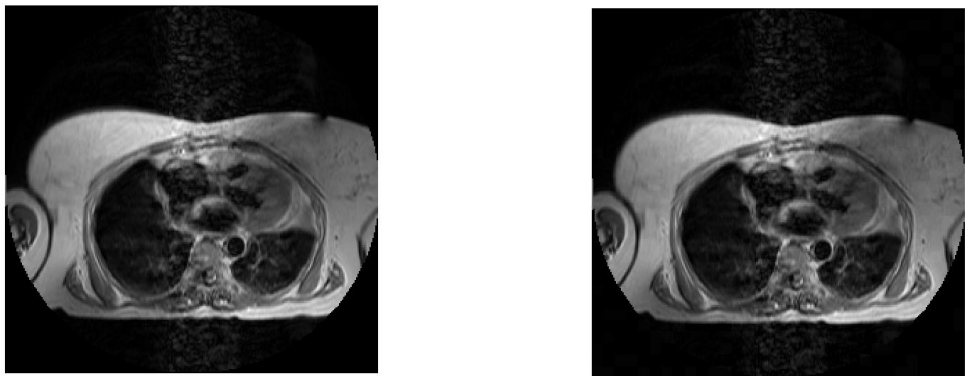
Fig 4.6 (a) and Fig (b) shows an original test image named ‘baboon’ and watermarked image, respectively. The watermark is shown in Fig. 4.6 (c), which is a binary image of generated by Universiti Teknologi PETRONAS (UTP) logo (more information regarding UTP logo can be found on [55]). The values of SSIM (0.9956) and MS-SSIM (0.9955), affirms that after the embedding of the watermark, the image has retained its original quality thus making the proposed scheme imperceptible.

4.3.1.1 Application in Medical Images

Medical images are more critical in nature and medical practitioners do not want any degradation at all, since even minor degradation can lead to defective clinical outcomes. Thus, a high level of imperceptibility is required in this case. Secondly, Electronic Patient Report (EPR) that is embedded in the image itself, during transmission requires confidentiality. The significance of embedding of EPR into the medical image is to save the storage space required to store EPR separately, and also to save the time required to transmit the EPR separately from the image. Due to the availability of image manipulation tools the authenticity of the image also needs to be verified. Even though a lot of work has been done in this area [64-66], it is still considered an open field of research as not all of the issues have been addressed.

The proposed watermarking scheme satisfies the important property of imperceptibility which is one of the essential characteristics when dealing with medical images. Additionally, the proposed scheme can be modified to be used for authentication of medical images. However, the main focus here is to show that EPR can also be embedded into medical images using the proposed scheme without degrading the image quality noticeably as can be seen from Fig. 4.7. The Fig. 4.7 (a) shows a 256×256 MRI image is watermarked with using the image in Fig. 4.6 (c) to obtain a watermarked image in Fig. 4.7(b). The measured values of SSIM i.e. 0.9617

and MS-SSIM i.e. 0.9951 verifies imperceptibility of the watermarking scheme in case of medical images.



(a) (b)

Figure 4.7: 256×256 MRI Image [67] (b) Watermarked MRI Image (SSIM = 0.9617, MS-SSIM = 0.9951).

4.3.2 Comparison with QIM based technique in [39]

The proposed watermarking scheme is compared with an existing QIM based watermarking technique [39] in order to thoroughly evaluate the performance of the proposed scheme. The comparison between the proposed DC component Bitplanes watermarking scheme (proposed scheme) and the QIM based watermarking scheme in [39] is shown in Table 4.7.

Although the PSNR values of the extracted watermark by the proposed scheme after attacks is smaller than those by the QIM based watermarking technique, but the extracted watermark is in a quality where it is understandable. However, the proposed scheme is simpler to implement with less overhead as compared to the QIM watermarking technique in [39] that requires a generation of quantization vectors.

Table 4.7: Comparison between the Proposed Scheme and the QIM Based Watermarking Scheme.

Attacks / PSNR Values	**Proposed Watermarking Scheme**	**QIM Based Scheme [39]**
Salt & Pepper Noise	41.1550	44.0453
Gaussian Noise	7.95	35.2055
Median Filtering	4.492	38.6074

Secondly, the QIM based technique in [39] is robust under the given attacks as compared to the proposed scheme which is sensitive to these attacks along with maintaining the watermark. Thus the proposed scheme can be implemented to serve two purposes, i.e. to store a copyright logo as well as for authentication or tamper detection, as compared to QIM based technique. Any little modification made in the watermarked image is detectable and also the watermark in not completely destroyed under attacks. Also the watermarking scheme is compatible with JPEG compression standard, in other words the watermark survives the JPEG compression.

There are several dimensions for a watermarking technique depending upon the application it is used for, thus modifications can be made according to the required application scenario.

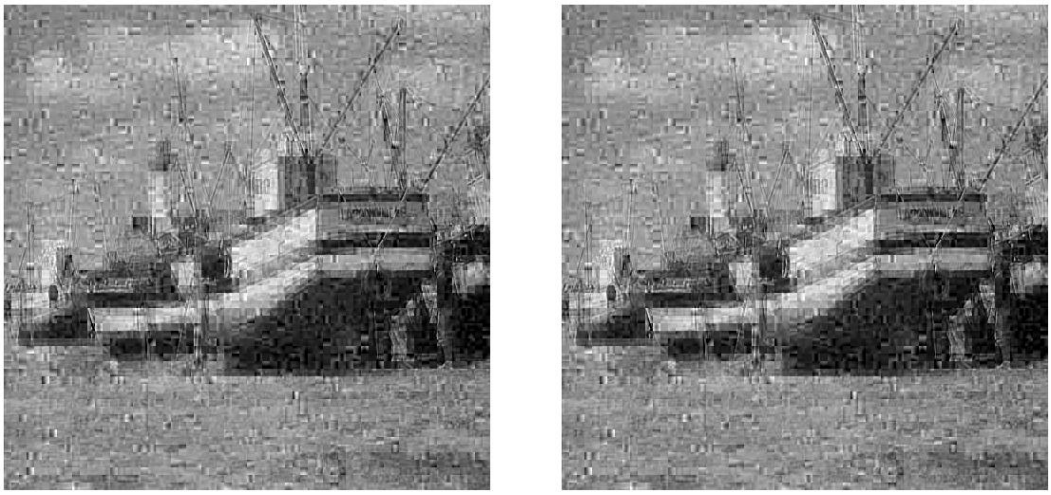
4.4 Security Analysis

The security of any multimedia for transmitted sensitive information is of great importance and critical. The multimedia content encryption is different from the encryption of raw data / text. As multimedia content is generally of huge size, encrypting the whole multimedia content in real time is not possible. Doing so will increase computational cost and also delay the delivery of the content, thus only few a-priori chosen parts of the content are encrypted. Sometimes partial viewing of the content is allowed in such a manner that it can be understood by the user. For multimedia encryption algorithms, the security is evaluated more carefully and from aspects different from those of data.

The overall security of the proposed Joint Perceptual Encryption and Watermarking Scheme can be assessed in gradual steps. First, the security is assessed by assuming that the encrypted data is the image corrupted by noise, so, filtering based approaches are used to recover the image. Alternatively, the AC coefficients and DC bitplanes that are used for encryption are set to zero. The image so recovered is an approximation of original image. If the image is good enough, the level of

encryption is considered poor and unacceptable. Both these techniques fall under cipher-text only attacks. The susceptibly of the scheme is studied against these attack and is presented in later sections. Then discussion is carried out on the scenario if the attacker wants to replace the copyright information. After that the robustness of the watermarking scheme is evaluated by placing the watermarked image under common image processing modifications. In last Rearrangement attack, key size and management is discussed.

(a) (b)



(c) (d)

Figure 4.8: (a) 512×512 Original image. (b) 512×512 Watermarked image (SSIM = 0.9918, MS-SSIM = 0.9944, PSNR = 41.3) (c) 512×512 Partially encrypted image (SSIM = 0.4157, MS-SSIM = 0.6350, PSNR = 20.54) (d) 512×512 Partially encrypted and watermarked image (SSIM = 0.4186, MS-SSIM = 0.6381, PSNR = 20.54)

4.4.1 Image Restoration - Perceptual Security

The perceptual security focuses on the perceptibility of the content by human beings, i.e., it measures how much of the multimedia content is understandable or meaningful. The basic idea of perceptual security is to make the content unintelligible, so that no information can be perceived through that content whether it is an audio, video or image.

The perceptual security of the encrypted content can be measured using two types of metrics - subjective and objective metrics. Subjective metrics are based on scores and comments given by some of the participants who assess the level of quality of the encrypted content. There are some standards to use subjective quality assessment techniques recommended by ITU, some of which are ITU-T P.911 [68], ITU-R BT.500-12 [69], etc. The basic procedure of evaluation is that the encrypted content is shown to a number of participants for a specific interval of time. Those scorers then assign each shown picture a predefined level of score.

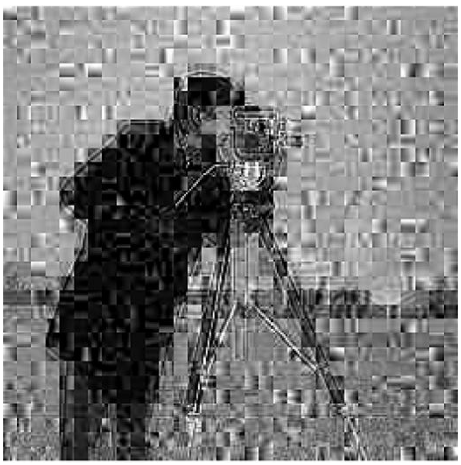
The other means to measure the perceptual security is the use of objective metrics. In the past, there were not many objective metrics available. Usually PSNR (Peak-Signal-to-Noise-Ratio), MSE (Mean Square Error) [70] and SNR (Signal-to-Noise-Ratio, mostly employed to measure the errors introduced in audio signal) [71] were used, but logically the metric which measures the level of perceptual security of the multimedia content should be based on the understanding of the image/video. In other words, it should calculate the amount of the information being perceived from the image or video. PSNR, MSE and SNR are used to calculate error introduced in the content. These metrics are not suitable for measuring the amount of information visible through the image/video [49]. For the proposed scheme along with PSNR and SNR, metrics like SSIM, MS-SSIM, VSNR, VIF, VIFP, UQI, IFC and WSNR are used to measure the level of perceptual security. As some of these metrics are newly designed, thus they were not been widely used in the previously presented literature. For this case of perceptual encryption, perceptual security can be referred as the degradation of quality of the image. The measured values of the above discussed objective metrics have been presented earlier in Table 4.2. The equivalent percentage

corresponding to those values will be the mathematically visible information through the image.

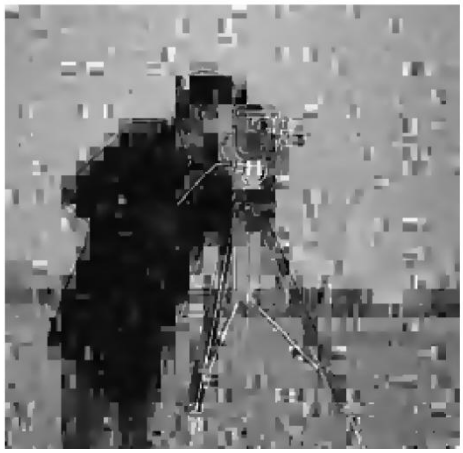
4.4.1.1 Filtering Based Attacks

To evaluate the perceptual security of the scheme, a number of experiments have been conducted using common image processing filtering techniques i.e. wiener filtering, to determine whether a more clearer image is obtained after going through these filtering function or not. These filtering techniques can be regarded as a case of Ciphertext-Only Attacks. It can be seen from Fig. 4.9, that shows the output image after the following filtering function i.e. wiener filtering as filter type ‘unsharp’ and ‘gaussian’, denosing using phase preservation method and enhancement using anisotropic diffusion method, does not show any significant improvement in the encrypted image. The output image after the wiener filtering as a filter type ‘unsharp’ in Fig. 4.9(a), show a little improvement in the values of PSNR, SSIM and MS-SIM the rest of the image does not show improvement in the quality of the image. Although in Fig.4.9(c) the quality of the image has been worsen perceptually as compared to the encrypted image.

(a)



(b)



(c) (d)

Figure 4.9: (a) Image restored after Weiner filtering as filter type ‘unsharp’. (PSNR = 19.2399, SSIM = 0.4127, MS-SSIM = 0.6279). (b) Image restored after Weiner filtering as filter type ‘Gaussian’. (PSNR = 16.7864, SSIM = 0.2739, MS-SSIM = 0.5375). (c) Image restored after Denoising. (PSNR = 7.4762, SSIM = 0.1039, MS-SSIM = 0.4126). (d) Image Enhancement using Anisotropic Diffusion method. (PSNR = 18.704, 5SSIM = 0.4925, MS-SSIM = 0.6637).

These Weiner filtering with the filter type ‘unsharp’ and ‘gaussian’ is carried out by using MATLAB function ‘deconvwnr’. The denoising is done, as shown in Fig. 4.9(b), using a phase preservation method and the enhancement is done, as shown in Fig. 4.9(d), using anisotropic diffusion method, both can be found at [78].

4.4.1.2 Attack-Zero

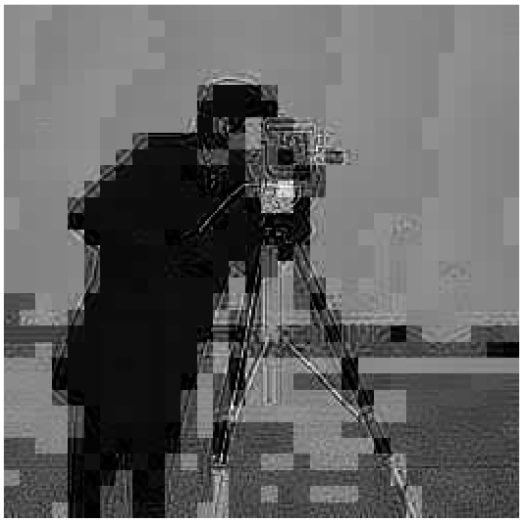
One of the possible attacks on the perceptually encrypted image is Attack-Zero that falls under Ciphertext-Only Attack. In this attack it is assumed that the attacker knows the working of the scheme and somehow the attacker has gained knowledge about the number of coefficients and DC bitplanes that has been encrypted and then the attacker set that scrambled data equal to zero.

(a)

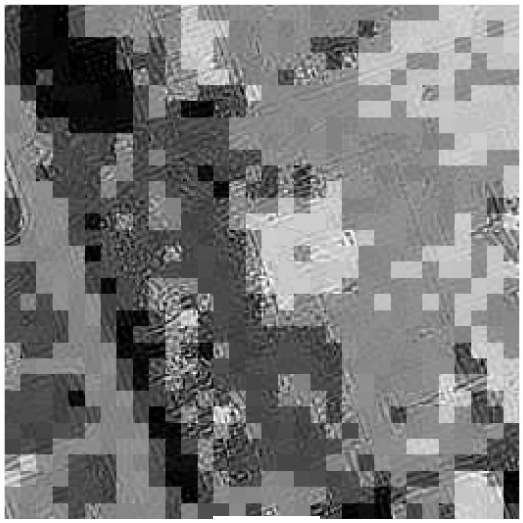
(b)

(c)

(d)



(e)



(f)

Figure 4.10: (a) Cameraman Image restored by setting AC 9 to AC 5 equal to zero. (PSNR = 22.30, SSIM = 0.7988, MS-SSIM = 0.9079). (b) Airfield Image restored after setting AC 9 to AC 5 equal to zero. (PSNR = 22.14, SSIM = 0.6993, MS-SSIM = 0.8447). (c) Cameraman Image restored by setting first 9 AC coefficients equal to zero. (PSNR = 20.24, SSIM = 0.6792, MS-SSIM = 0.8272). (d) Airfield Image restored after setting first 9 AC coefficients to zero. (PSNR = 18.92, SSIM = 0.5402, MS-SSIM = 0.7273). (e) Cameraman Image restored by setting first 9 AC coefficients and 4^{th} DC bitplane equal to zero. (PSNR = 15.73, SSIM = 0.6028, MS-SSIM = 0.6984). (b) Airfield Image restored after setting first 9 AC coefficients and 4^{th} DC bitplane to zero. (PSNR = 15.02, SSIM = 0.4162, MS-SSIM = 0.6133).

Only from this attack, the attacker can get best possible approximation of the image on if the control factor is lesser then 5 as can be seen from Fig. 4.10 (a & b). If the control factor is increased then as can be seen from Fig. 4.10 (c, d, e & f), that the image is no longer in perceptually good quality. Thus, it is suggested to encrypt minimum of least 5 AC coefficients to get the visually degraded image.

4.4.2 Rearrangement Attack

Usually, it is assumed that the cryptanalyst (the one who practises the art of breaking the encryption algorithms) knows the working of the encryption algorithm. This analysis of an encryption algorithm can be done by carrying out several numbers of attacks. The resistance shown by the encryption algorithm heightens the level of

security of that encryption algorithm. Let us see the case of Rearrangement Attack, in which the cryptanalyst tries to rearrange the scrambled data. For the scenario, in which only 9^{th} AC coefficient is being scrambled, consider the image of size 256×256. As in JPEG compression standard, for processing, it will be divided into 1024 blocks of size 8×8. So the total possible combinations required to check for one coefficient will be 1024! If all the 9 AC are scrambled together, then there are 9216! possible combinations. Exhaustive searches of combination are needed to be carried out. Similarly, in the case of 5 AC coefficients, 5120! searches need to be carried out to find the possible combination of the arrangement of the coefficients. Besides computational cost, human observers are also required to see if the combination of the coefficients results in a meaningful information.

The multimedia encryption scheme is considered to be secure if the cost of breaking is higher than the cost of buying that content, and the time required to break the encryption algorithm is more than the time in which that content is considered to be useful [72]. Like in the case of breaking news or a live football match, it is only worthy when being telecast live. After some time it will not be as worthy as when it was broadcasted live, and also the cost of breaking the multimedia encryption should be less than the cost to buy that particular content.

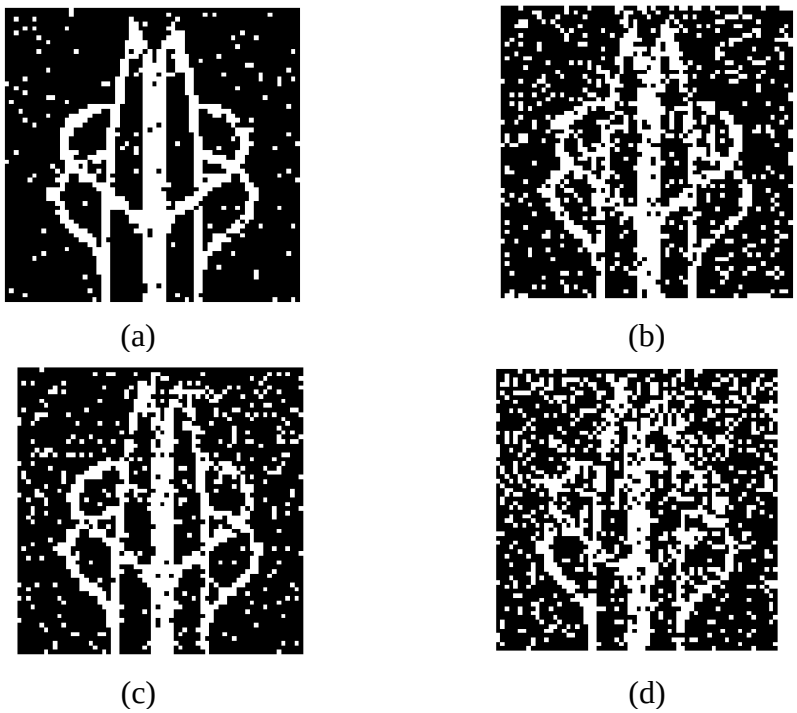
4.4.3 Watermark Replacement Attack

This is the scenario where the attacker has the watermarked image and then tries to replace the existing watermark, copyright information, by its own. This replacement of the watermark can be carried out only if the attacker knows the positions or the locations where the watermark bits have been substituted in the DC bitplanes, which is not possible without the knowledge of correct key. Another possible case is in which the attacker has the knowledge of the bitplanes in which the watermark bits has been embedded and the attacker tries to remove these biplanes by setting them equal to zero. However, this removal can be easily identified by checking anomalies in the corresponding bitplane where the watermark was embedded.

4.4.4 Robustness

In order to assess the robustness of the watermarking scheme, it can be subjected to several attacks. Some of the most common attacks like salt & pepper noise, Gaussian Noise and Median filtering are commonly used for the purpose. These were also carried out to study the robustness of the proposed watermarking scheme. For the experiment, several images of different texture and sizes were taken and watermarked, and also watermarks of different sizes were used.

An example of 512×512 baboon image (standard test image) was taken and watermarked with the image (symbol / logo of Universiti Teknologi PETRONAS) in Fig. 4.6(c). Then the watermarked image was placed under few attacks. The corresponding recovered watermarks and the measured SSIM values are shown in Fig. 4.11.



(a) (b)

(c) (d)

(e)

Figure 4.11: 64×64 watermark recovered from images placed under attacks (a) Salt & Pepper Noise with noise density 0.001 (SSIM = 0.6505, PSNR = 41.3). (b) Salt & Pepper Noise with noise density 0.005 (SSIM = 0.4071, PSNR = 8.95). (c) Gaussian Noise with '0' mean and 0.0001 variance (SSIM = 0.4996, PSNR = 10.03). (d) Gaussian Noise with '0' mean and 0.0005 variance (SSIM = 0.3274, PSNR = 6.6). (e) 3×3 median filtering (SSIM = 0.2826, PSNR = 6.5).

Fig 4.11 (a) to (e) show the results of salt & pepper noise with noise density 0.001 and 0.005, Gaussian Noise with 0 mean, and 0.005 and 0.001 variance, and Median filtering of size 3×3. The scheme is considered robust if the extracted watermarking is meaningful. The results shown in Fig. 4.11 indicate that the extracted watermark is meaningful except for the watermark extracted after median filtering (Fig. 4.11(e)). Thus, the proposed watermarking scheme can also be regarded as robust.

4.4.5 Key Size (Brute-Force Attack)

The key size or the length of the key plays an important role in achieving a cryptographically secure algorithm. Intuitively, the greater the key size, more effort is required to recover the key. The adopted scrambler uses 128-bit key. As an example, consider permutation with repetition, then there will be $2^{128} = 3.40282367 \times 10^{38}$ possible keys in the case of brute-force attack. Assuming that the attacker has the capability of trying 1 billion keys per second then it will take $1.07902831 \times 10^{22}$ years to conclude the exhaustive key search. Additionally to perform these kinds of exhaustive key searches, special purpose hardware is required which is also costly. This is in contrast with the principles of security for multimedia

encryption algorithm i.e. the multimedia content is secure if the time require to break the multimedia encryption algorithm is more than the time in which that content is considered valuable. Besides, if the cost of breaking the multimedia algorithm is more than the cost of the multimedia content itself [72], the exercise is considered futile.

4.4.5.1 Key Management

The adopted scrambler is a symmetric key algorithm which employs that same key for encryption and decryption. Key management deals with the issues which arise because of sharing of the key among the receiver and the sender. The exchange of this key must be made secure. Compromising the key will lead to the loss of encrypted information / data. Besides maintaining the confidentiality, the authenticity must also be verified. In other words, the receiver of the key should be sure of the true identity of the sender of the key. The adopted scrambler uses **IEEE 802.11*i*** key management protocol. There exist several other key management protocols that can also serve the purpose in the proposed scheme.

4.5 Summary

In this chapter results of the proposed Joint Perceptual Encryption and Watermarking Scheme are presented along with their detailed analysis. Firstly, the results for the proposed perceptual encryption scheme are presented and its effect on the compression ratio and selection of control factor is then discussed. The levels of perceptual encryption are measured using recently designed IQA's. Additionally, a comparison between a recently proposed RHS based perceptual encryption scheme and the proposed perceptual encryption scheme, is done. It is noticed that the proposed perceptual encryption scheme outperforms the RHS based perceptual encryption scheme in terms of number of operations. Results of DC component bitplanes based watermarking scheme are also presented and its imperceptibility was discussed. The proposed scheme enables one to select the appropriate number of bitplanes to distribute the watermark. Moreover, suitability of the proposed

watermarking scheme for application to medical images has been demonstrated and discussed. This design of watermarking scheme allows one to have more control. The proposed scheme has also been compared with the QIM based watermarking scheme. The overall security of the joint scheme has been presented in detail and different aspects of the multimedia security have been discussed. Based on the results and performance evaluation, the whole scheme can be regarded as secure.

This page is intentionally left blank Chapter 5 starts from next page.

CHAPTER 5

THE PROPOSED ROI BASED PERCEPTUAL ENCRYPTION SCHEME

5.1 Introduction

In the previous two chapters, the design of the proposed Joint Perceptual Encryption and Watermarking scheme was presented together with its performance evaluation. In this chapter, a perceptual encryption scheme will be presented. The perceptual encryption scheme is based on Region Of Interest (ROI) and is in the framework of JPEG. The performances of the proposed perceptual encryption schemes will be evaluated in the next chapter. The reason for designing and implementing independent perceptual encryption scheme is that it allows more data to be manipulated to serve the purpose perceptual degradation. In other words, there exist no limitations on the selection of data as these limitations were in previously proposed design of JPEW. The availability of more data allows more control over levels of degradation and also improves security. Thus, if more levels of perceptual degradation is desired than independent designs can be employed.

5.2 Background

Even though there is always a need for the design of perceptual encryption scheme that is simple in implementation with low overhead of computational cost, there are not many perceptual encryption schemes presented in the literature. Also, it will be of great advantage if the perceptual encryption scheme can achieve linear

degradation in the content. The linear degradation of the multimedia content has not been given much importance due to the unavailability of standard metrics to measure the degradation in the audio/video/image quality. The proposed scheme makes use of several IQAs to achieve linear degradation.

The number of levels of perceptual encryption must also be taken into consideration as it will provide more control to the user. Due to huge amount of visual data being transmitted via the internet, to save the bandwidth this visual data must be transmitted in compressed form. Thus, the perceptual encryption scheme should be integrable with the compression standard. The proposed perceptual encryption schemes so designed that they can be integrated with JPEG compression standard. However, dedicated perceptual encryption scheme need to be designed and implemented for each compression standard. Popular compression standards like MPEG 2, which is the most commonly used standard for videos, can easily adapt this designed perceptual encryption schemes. It is so because the proposed techniques make use of JPEG standard and, as mentioned earlier, JPEG compression standard mimics the intra-frame coding in the MPEG compression standards. This will allow these proposed perceptual encryption schemes to be extended to the MPEG compressed videos without any major modifications.

A general block diagram of the proposed perceptual encryption schemes is shown below in Fig. 5.1. Scrambling is carried out after the quantization process, similar to the JPEW framework.

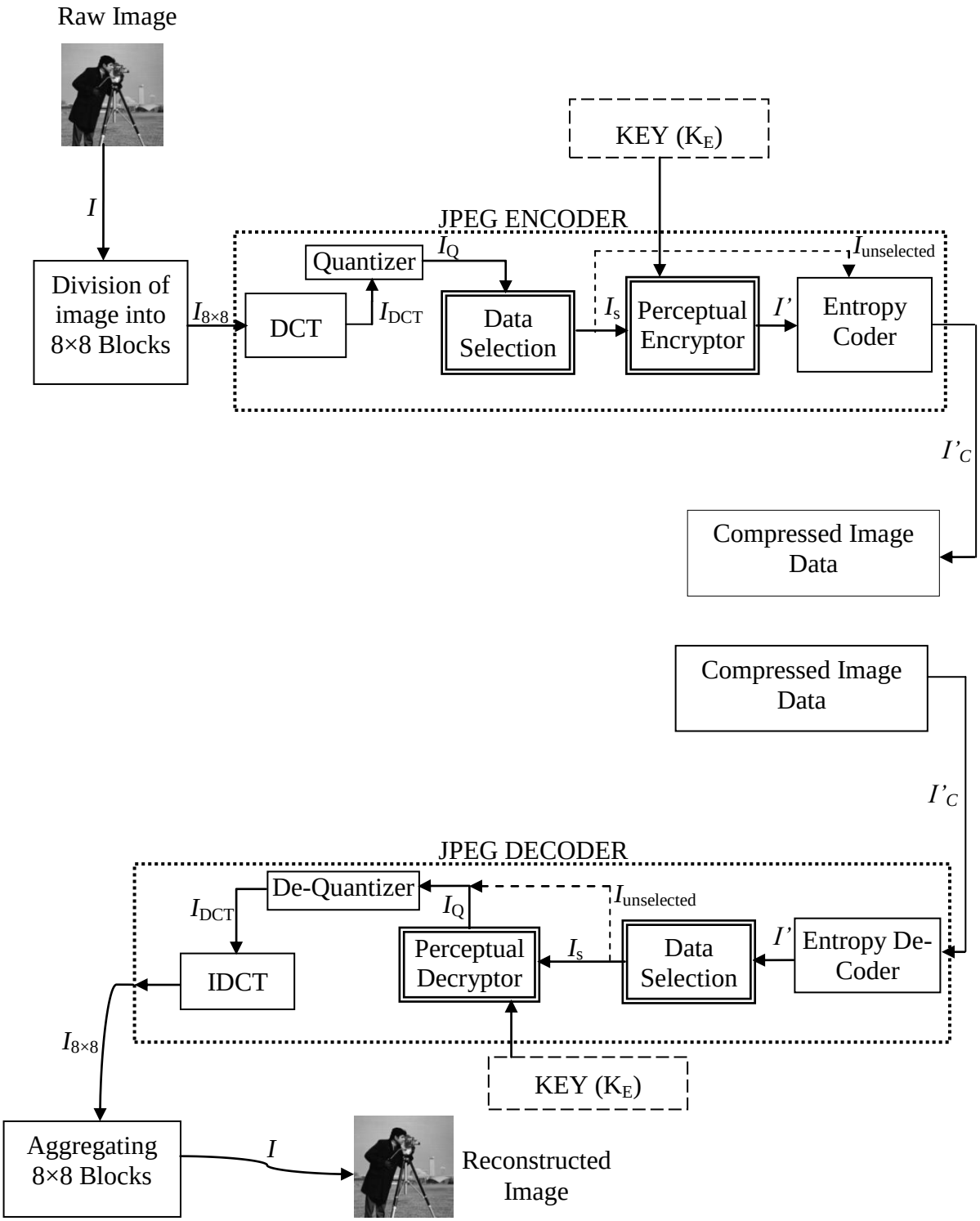


Figure 5.1: JPEG Coder and Encoder with Scrambler and Descrambler embedded in it respectively for the purpose of perceptual degradation.

5.3 ROI Based Perceptual Encryption Schemes

Inspired by the idea in [13] and [20], this proposed perceptual encryption scheme and its variants are based on 2 levels of scrambling – first the 8×8 blocks in the Region Of Interest (ROI) and second, the number of AC coefficients of DCT as stipulated in JPEG compression standard. To scramble the selected DCT blocks and AC coefficients, the same chaotic scrambler that is used in the proposed design of JPEW is used here and it is described in Appendix A. For the purpose of measuring the level of degradation introduced in the image, along with PSNR, objective image quality metrics (SSIM, MS-SSIM, VIF, VIFP, UQI, VSNR and IFC) are again used.

The proposed scheme provides two degree of freedom, as it consists of two levels; first the ROI, which needs to be encrypted in the image/video, is identified and encrypted. Secondly, some selected numbers of AC coefficients are scrambled in order to degrade the perceptual quality of the entire image/video. The main idea here is to identify the area which needs to be encrypted. We take advantage of the fact that usually important information is focused in the centre of the image or video. Therefore one can degrade the content from the centre. Several other variants of DCT block scrambling along with AC coefficients to degrade the perceptual quality of the image are considered. These DCT blocks are selected in such a manner that they form a square in the centre. The number of selected blocks from the centre is increased to show progressive perceptual encryption.

Besides DCT block scrambling, selected number of AC coefficients is scrambled to degrade the perceptual quality of the entire image. Another possible variant that is presented is where some DCT blocks from the image are randomly selected and then scrambled. Also, some additional AC coefficients are selected and scrambled with it. For the purpose of scrambling, the scrambler is incorporated after the quantization block in the JPEG compression standard as shown in Fig. 5.1. Also it is worth mentioning that, the indices of the quantized DCT blocks and AC coefficients are read

in the conventional zigzag manner. If the region of interest is other than a square area, then raster scan can also be used to read their indices. This presented perceptual encryption scheme mainly focuses on the security against the casual listeners/observers, so it tries to provide sufficient security against casual listeners as discussed in section 6.2.7.

5.4 Control Factor / Quality Loss Factor

The control factor in ROI based scheme is based on the number of DCT blocks and in the extended scheme the control factor is the extension from JPEW by increasing the levels of perceptual encryption as now the DC component's bitplanes are being scrambled. The selection of control factor for both the proposed perceptual encryption schemes are based on the design curve. The development of design curve is similar to the one done in the design of JPEW and has been discussed in section.4.2.2.

5.5 Methodology of performance evaluation

The performance of the proposed ROI based perceptual encryption scheme is evaluated on the same style as done for the perceptual encryption scheme in JPEW proposed in previous chapters. The important attributes of the perceptual encryption scheme includes security and compression efficiency. Both of these attributes are discussed in next chapter. The compression analysis is performed in section 6.2.6, and is carried out on the same principles as was done in section. 4.2.3, for JPEW. Form the perspective of security, as same chaotic scrambler as in JPEW, has been adopted in the proposed ROI based scheme. Thus the key size and management will be the same as discussed section 4.4.5 and section 4.4.5.1. However the attacks related to image restoration will be different for the proposed scheme. The Image restoration attacks include the interpolation and extrapolation attacks carried out with the help of

data available in the surrounding of ROI interpolate or extrapolate the values in place of encrypted data and are presented in section 6.2.7.1. Similar to the previous perceptual encryption scheme in JPEW, a rearrangement attack on the perceptually encrypted image can be carried out and is discussed in section 6.2.7.2.

5.6 Summary

In this chapter a perceptual encryption schemes is proposed. The scheme is based on Region Of Interest (ROI), where degradation is introduced in the content by scrambling the DCT blocks in the ROI. Furthermore, some variant of ROI based schemes are also discussed. In last, the methodology for the performance evaluation of the scheme is discussed.

CHAPTER 6

RESULTS AND ANALYSIS OF PROPOSED ROI BASED PERCEPTUAL ENCRYPTION SCHEME

6.1 Introduction

In the previous chapter, a ROI based perceptual encryption schemes within the frame work of JPEG compression has been proposed. In this chapter, the results of its performance are presented and analyzed in terms of their dependence on compression and resulting security. There are several variant of the proposed ROI based scheme, each of the variant have also been discussed in this chapter followed by the discussion on the development of its design curve.

6.2 Results of ROI Based Perceptual Encryption scheme

The performance of the abovementioned scheme and its variants are evaluated by keeping several aspects in consideration. The quality or the level of distortion introduced in the image by the encryption is measured by objective image quality assessment metrics such as SSIM, MS-SSIM, VIF, VIFP, VSNR, IFC and UQI for each variant separately. Another aspect, that is the compression efficiency as affected by encryption is also analysed. The effect of the encryption scheme on compression ratio and the security of the scheme are discussed in section 6.2.6 and 6.2.7, respectively.

6.2.1 Scrambling of DCT-Blocks selected from Center of the Image

In majority of the images and videos, the main object of interest mostly appears in the center. So, it will be a good practice if the image or video is only degraded from the center as it will save the time required for encryption process and can result in reduction of cost. Thus, center of the image will act as the ROI. In this case, quantized DCT blocks (size of 8×8 pixels) from center are selected and scrambled. The experiment is initiated by taking 4 (2×2) DCT blocks in the center and then they are scrambled. At this stage, the amount of degradation introduced is measured. If the degradation is considered insufficient, more blocks of DCT are included around the 4 blocks already chosen and scrambled. The number of the DCT blocks selected from the center of image is systematically increased to 16 (4×4). In a similar manner, the number of DCT blocks selected from the center is increased to (6×6), (8×8) and so on until the whole image is scrambled. The corresponding values of the SSIM, MS-SSIM, VIF, VIFP, UQI, IFC and PSNR are measured after every step. Table 6.1 shows this these values averaged over about 50 test images. As one can observe from the table, an increase in the number of DCT blocks from the center will increase the percentage of degradation in the image. On an average, it can be seen that about 13.75% (estimated by SSIM) and 22.5% (estimated by MS-SSIM) of the information visible through the image is distorted if ROI consist of 144 DCT blocks from the center. This percentage is increased to 58.4% (estimated by SSIM) and 73.96% (estimated by MS-SSIM) when the ROI is 26×26 (676) DCT blocks from the center. The selection of the blocks depends upon the application and the content. One can increase the number of selected DCT blocks according to its need. The corresponding design curve for the selection of control factor is shown in Fig.6.2.

In the Fig. 6.1(b) it is shown that 144 (12×12) DCT blocks are selected and scrambled using the chaotic scrambler. The values of degradation measured using various metrics are mentioned in the caption of the Fig 6.1. The average values are shown in Table 6.1.

(a) (b)

Figure 6.1: 256×256 Lena image. (SSIM = 1, MS-SSIM = 1, VIF = 1, VIFP = 1, UQI = 1), (b) 256×256 center selected Lena Image (PSNR = 18.83, SSIM = 0.8478, MS-SSIM = 0.7022, VIF = 0.6835, VIFP = 0.7654, VSNR = 8.59, UQI = 0.8429).

Note: Metric values are measured by ROI from 2×2 (four blocks) up to 32×32 (1024 blocks) for the individual image in the database. These calculated values are not shown here due to limited space.

Table 6.1: The Corresponding Measured Metric Values of Scrambled DCT-Blocks from center of Image.

Metrics / Block Size	Measured Average value for Center Selected Scrambling									
	6×6	**8×8**	**10×10**	**12×12**	**14×14**	**16×16**	**18×18**	**20×20**	**22×22**	**24×24**	**26×26**
PSNR	28.27	25.51	23.31	18.22	18.03	18.98	17.53	16.65	15.80	15.01	14.39
SSIM	0.9675	0.9413	0.9078	0.8625	0.7980	0.7687	0.7061	0.6454	0.5769	0.4963	0.4159
MS-SSIM	0.9502	0.9068	0.8543	0.7747	0.6514	0.6377	0.5319	0.4663	0.3868	0.3118	0.2604
VSNR	19.147	15.926	13.325	11.337	7.665	8.642	7.141	6.233	5.348	4.555	3.933
VIF	0.8941	0.8350	0.7660	0.6847	0.6017	0.5269	0.4323	0.3431	0.2540	0.1654	0.0943
VIFP	0.9195	0.8699	0.8088	0.7351	0.6986	0.5873	0.4977	0.4093	0.3187	0.2244	0.1317
UQI	0.9623	0.9330	0.8956	0.8455	0.7903	0.7349	0.6628	0.5877	0.5058	0.4062	0.3044
IFC	61.735	58.034	53.674	48.975	45.913	37.512	31.108	23.964	16.610	9.677	4.509

The control factor for the above discussed variants of block based perceptual encryption scheme can be selected from the corresponding graphs shown in Fig. 6.2. A number of choices have been given to select the control factor using several IQAs. The selection of control factor can be carried out using the same procedure as described in section 4.2.2, where the Control Factor / Quality Loss Factor was selected for JPEW. But in this case, instead of AC coefficients and DC bitplanes, the number of DCT blocks is acting as a control factor.

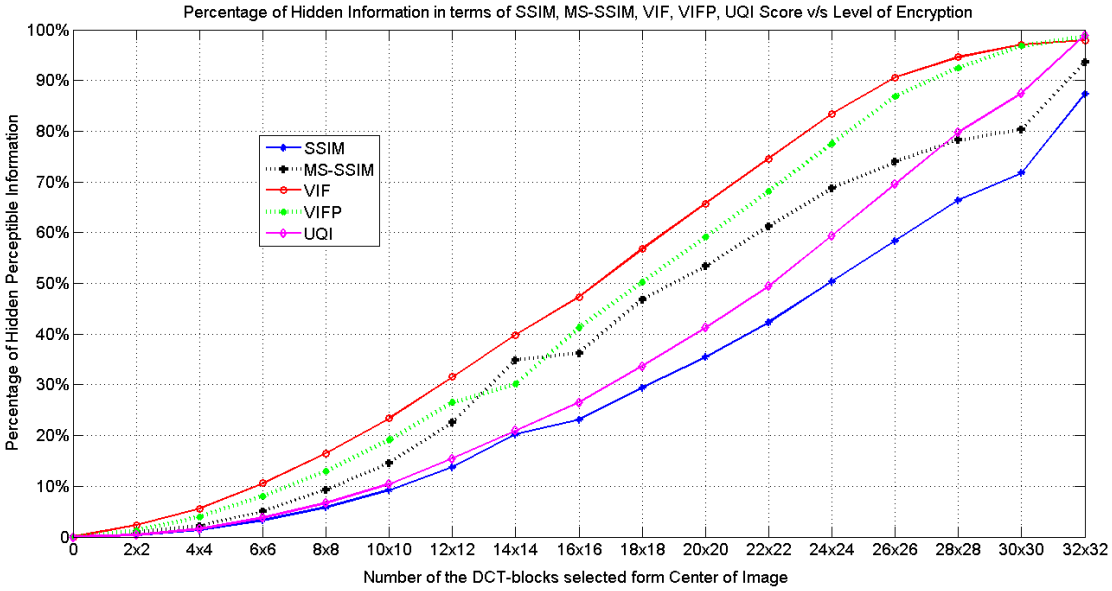


Figure 6.2: Graph showing the selected DCT-blocks from the center of the image vs. the percentage of hidden information measured in terms of SSIM, MS-SSIM, VIF, VIFP, and UQI.

In case when image size other than 256×256 is required to be degraded then the following equation can be used for the selection of control factor,

$$CF_o = Round_{nearest\_even}\left(\frac{image\ size}{256\times 256}\times CF_d\right) \qquad (6.1)$$

Where CF_d is the control factor corresponding to the desired level of perceptual degradation selected from the design curve, $Round_{nearest\_even}$ is the function which round the obtained value to the nearest even number. CF_o is the optimized control factor according to the size of the image.

6.2.2 Scrambling of DCT-Blocks selected from center along with 5th AC Coefficient

As in the abovementioned case, only the DCT-blocks in the center are only scrambled and the information around the ROI (center of the image being scrambled) is clearly visible, and allows the availability of plaintext. To encounter this issue, one can use the AC coefficients to degrade the whole image to a certain level of quality. First few AC coefficients contain large values and are sufficient to perceptually degrade the quality of content [47]. So for the given cases an investigation will be carried out to see the level of perceptual encryption one will get by encrypting first 5 AC coefficients along with the scrambled DCT-blocks from the center. In this case the same abovementioned experiment is repeated with scrambling of 5th AC coefficient. The AC coefficients are read in zigzag order from DCT block. Table 6.2 shows the measured values after every step. For 144 DCT blocks selected from the center along with 5th AC coefficient, on average 32.78% measured by SSIM and 32.46% measured by MS-SSIM of visible information is distorted. The scrambling of the AC coefficients is performed in such a manner that they remain in their own orbit or plane. The corresponding design curve for the selection of control factor is shown in Fig.6.4.

Figure 6.3: 256×256 center selected Lena Image along with 5th AC coefficient scrambled (PSNR = 18.27, SSIM = 0.6291, MS-SSIM = 0.6486, VIF = 0.2639, VIFP = 0.2921, VSNR = 8.41, UQI = 0.5360).

Table 6.2: The Corresponding Measured Metric Values of Scrambled DCT-Blocks from Center of Image Along With 5th AC Coefficient.

Metrics / Block Size	Measured Average value for Center Selected Scrambling										
	6×6	**8×8**	**10×10**	**12×12**	**14×14**	**16×16**	**18×18**	**20×20**	**22×22**	**24×24**	**26×26**
PSNR	25.46	23.78	22.26	20.83	19.73	18.66	17.34	16.52	15.71	14.95	14.36
SSIM	0.7893	0.7684	0.7416	0.7050	0.6722	0.6318	0.5818	0.5349	0.4812	0.4189	0.3563
MS-SSIM	0.8935	0.8528	0.8039	0.7291	0.6754	0.6016	0.5032	0.4422	0.3680	0.2985	0.2508
VSNR	17.055	14.883	12.836	11.072	9.799	8.547	7.109	6.212	5.342	4.540	3.920
VIF	0.4231	0.3955	0.3621	0.3217	0.2869	0.2476	0.2038	0.1632	0.1233	0.0857	0.0549
VIFP	0.3843	0.3640	0.3383	0.3053	0.2764	0.2442	0.2062	0.1691	0.1337	0.0966	0.0631
UQI	0.5846	0.5632	0.5366	0.4996	0.4679	0.4286	0.3826	0.3360	0.2875	0.2282	0.1712
IFC	2.645	2.483	2.289	2.057	1.851	1.607	1.332	1.069	0.780	0.548	0.335

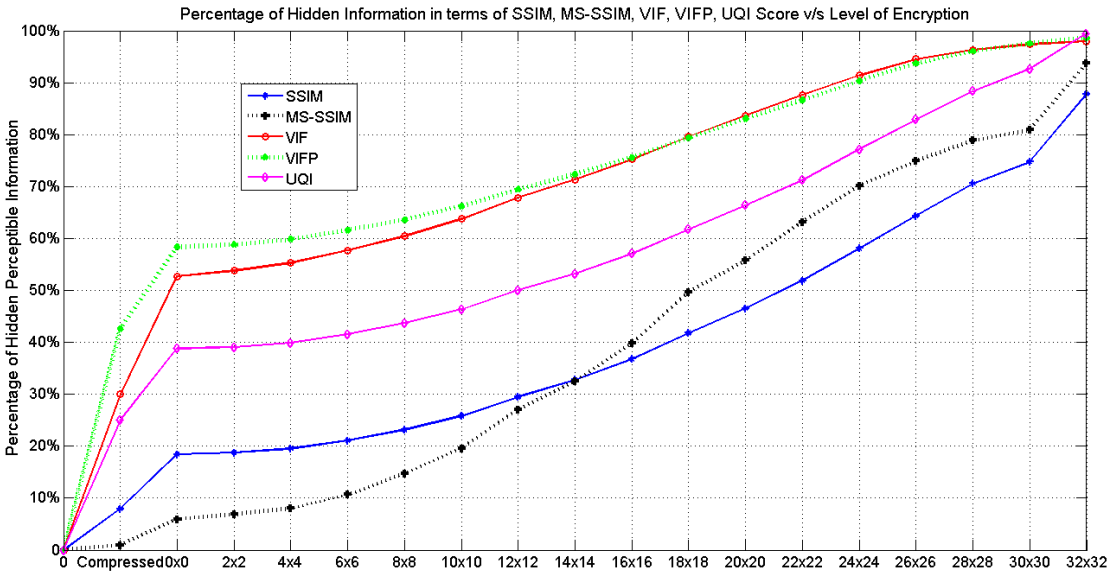


Figure 6.4: Graph showing the selected DCT-blocks from the center of the image with 5th AC Coefficient Scrambled vs. the percentage of hidden information measured in terms of SSIM, MS-SSIM, VIF, VIFP, and UQI.

6.2.3 Scrambling of DCT-Blocks selected from center along with 5th, 4th and 3rd AC Coefficient

A similar experiment was repeated as in section 6.2.2 now scrambling 5th, 4th and 3rd AC coefficients. The results are shown in Table 6.3. It is noticed that again for 144 DCT blocks selected from the center along with 5th, 4th and 3rd AC coefficient, on average 42.60% measured by SSIM and 32.67% measured by MS-SSIM of visible information is hidden. The corresponding design curve for the selection of control factor is shown in Fig.6.6.

Figure 6.5: 256×256 center selected Lena Image 5th, 4th and 3rd AC coefficient scrambled (PSNR = 17.88, SSIM = 0.5167, MS-SSIM = 0.6089, VIF = 0.1472, VIFP = 0.2097, VSNR = 8.19, UQI = 0.4298).

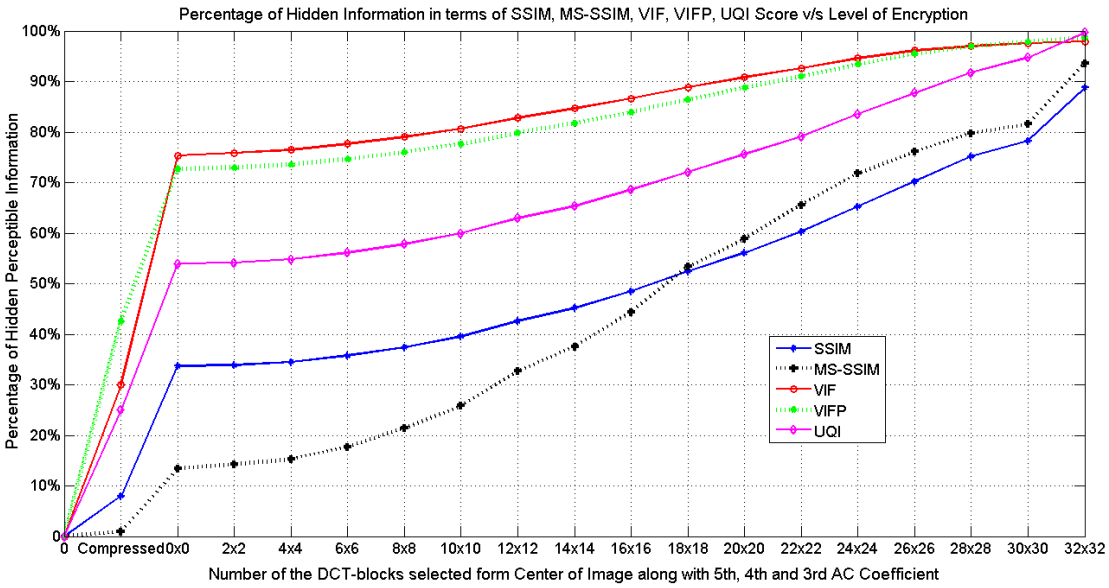


Figure 6.6: Graph showing the selected DCT-blocks from the center of the image with 5th, 4th and 3rd AC Coefficient Scrambled vs. the percentage of hidden information measured in terms of SSIM, MS-SSIM, VIF, VIFP, and UQI.

Table 6.3: The Corresponding Measured Metric Values of Scrambled DCT-Blocks from Center of Image Along With 5^{th}, 4^{th} and 3^{rd} AC Coefficient.

Metrics / Block Size	**Measured Average value for Center Selected Scrambling**										
	6×6	**8×8**	**10×10**	**12×12**	**14×14**	**16×16**	**18×18**	**20×20**	**22×22**	**24×24**	**26×26**
PSNR	23.63	22.44	21.33	20.19	19.25	18.31	17.10	16.35	15.59	14.87	14.30
SSIM	0.6426	0.6257	0.6043	0.5740	0.5481	0.5146	0.4755	0.4390	0.3971	0.3470	0.2976
MS-SSIM	0.8231	0.7860	0.7417	0.6733	0.6242	0.5564	0.4662	0.4114	0.3444	0.2815	0.2392
VSNR	14.482	13.087	11.705	10.313	9.240	8.178	6.862	6.053	5.237	4.468	3.875
VIF	0.2233	0.2094	0.1937	0.1719	0.1538	0.1339	0.1118	0.0921	0.0735	0.0545	0.0391
VIFP	0.2530	0.2398	0.2237	0.2016	0.1829	0.1611	0.1361	0.1125	0.0902	0.0661	0.0453
UQI	0.4386	0.4216	0.4005	0.3701	0.3464	0.3141	0.2790	0.2442	0.2091	0.1646	0.1228
IFC	1.24	1.168	1.082	0.971	0.874	0.764	0.642	0.530	0.421	0.308	0.215

6.2.4 Scrambling of DCT-Blocks selected from center along with first 5 AC Coefficients

The same experiment as in section 6.2.2 & section 6.2.3 was repeated, but now with all fist five AC coefficients selected for scrambling. Now, one can see that for the case of 144 DCT blocks on average 61.65% calculated by SSIM and 47.85% calculated by MS-SSIM is distorted. The results are show in Table 6.4 and the corresponding design curve for the selection of control factor is shown in Fig.6.8.

Figure 6.7: 256×256 center selected Lena image along with first 5 AC coefficients scrambled (PSNR = 16.02, SSIM = 0.3035, MS-SSIM = 0.4616, VIF = 0.0576, VIFP = 0.0788, VSNR = 6.03, UQI = 0.2184).

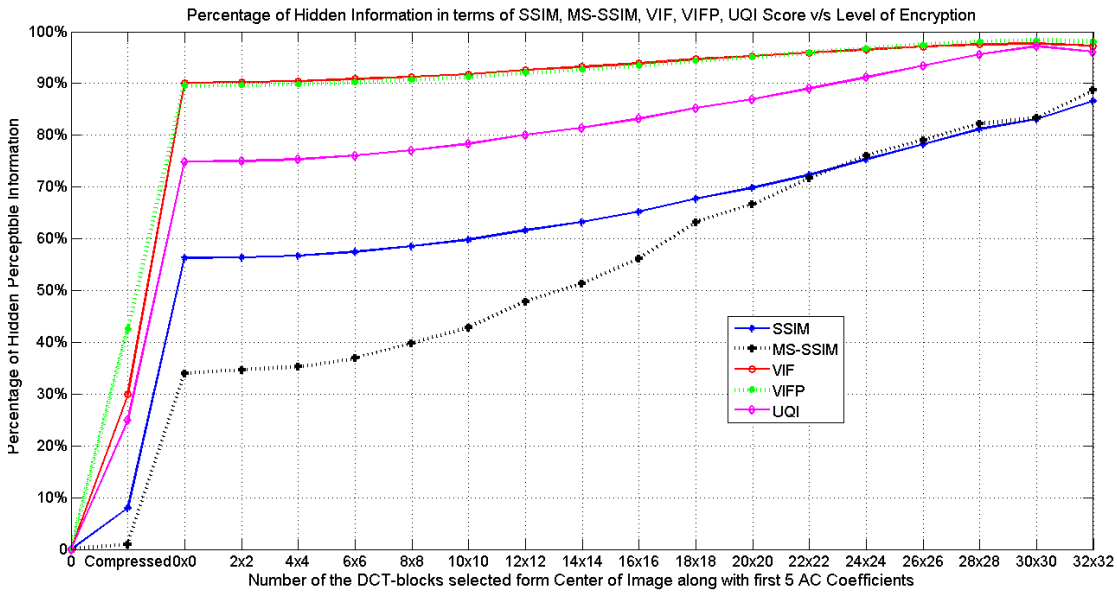


Figure 6.8: Graph showing the selected DCT-blocks from the center of the image with first 5 AC Coefficient Scrambled vs. the percentage of hidden information measured in terms of SSIM, MS-SSIM, VIF, VIFP, and UQI.

Table 6.4: The Corresponding Measured Metric Values of Scrambled DCT-Blocks from Center of Image Along With first 5 AC Coefficients.

Metrics / Block Size	Measured Average value for Center Selected Scrambling									
	6×6	**8×8**	**10×10**	**12×12**	**14×14**	**16×16**	**18×18**	**20×20**	**22×22**	**24×24**	**26×26**
PSNR	19.89	19.40	18.89	18.29	17.75	17.15	16.28	15.76	15.13	14.56	14.06
SSIM	0.4256	0.4145	0.4018	0.3835	0.3679	0.3480	0.3228	0.3015	0.2766	0.2466	0.2174
MS-SSIM	0.6304	0.6025	0.5715	0.5215	0.4862	0.4382	0.3688	0.3339	0.2828	0.2394	0.2090
VSNR	9.800	9.278	8.696	8.033	7.421	6.797	5.893	5.373	4.712	4.115	3.628
VIF	0.0914	0.0869	0.0820	0.0743	0.0680	0.0611	0.0532	0.0476	0.0408	0.0346	0.0287
VIFP	0.0972	0.0925	0.0872	0.0792	0.0729	0.0657	0.0564	0.0488	0.0405	0.0326	0.0252
UQI	0.2389	0.2290	0.2169	0.1995	0.1853	0.1681	0.1476	0.1304	0.1100	0.0880	0.0657
IFC	0.497	0.473	0.447	0.408	0.374	0.336	0.293	0.261	0.221	0.184	0.149

6.2.5 Randomly Selecting and Scrambling DCT-Blocks

One of the possible variants is random selection of the DCT blocks. Along with the random selection, the quality of the whole image can also be distorted by encrypting some selected number of AC coefficients as has been done in the abovementioned cases. The number of DCT blocks can vary according to the required degradation. In the proposed scheme, for experiment, three ranges of DCT blocks are randomly selected and scrambled. The experiment is also performed by encrypting first 5 AC coefficients gradually as shown in Figs. 6.9 (a, b, c, d) and the corresponding values of SSIM, MS-SSIM, VIF, VIFP, and UQI were calculated after every step, which are shown in Table 6.5.

(a)

(b)

(c)

(d)

Figure 6.9: (a) 256×256 Lena image randomly scrambled DCT block Lena image (PSNR = 16.78, SSIM = 0.7151, MS-SSIM = 0.6875, VIF = 0.5179, VIFP = 0.5974, VSNR = 6.5998, UQI = 0.6806).
(b) 256×256 Lena image randomly scrambled DCT block along with 5th AC coefficient scrambled (PSNR = 16.43, SSIM = 0.5441, MS-SSIM = 0.6451, VIF = 0.2152, VIFP = 0.2418, VSNR = 6.63, UQI = 0.4633).
(c) 256×256 Lena image randomly scrambled DCT block along with 5th, 4th, and 3rd AC coefficient scrambled. (PSNR = 16.19, SSIM = 0.4528, MS-SSIM = 0.6056, VIF = 0.1272, VIFP = 0.1764, VSNR = 6.41, UQI = 0.3794).
(d) 256×256 Lena image randomly scrambled DCT block along with 5th, 4th, 3rd, 2nd and 1st AC coefficient scrambled. (PSNR = 14.99, SSIM = 0.2750, MS-SSIM = 0.4652, VIF = 0.0542, VIFP = 0.0699, VSNR = 4.92, UQI = 0.2026).

Table 6.5: The Corresponding Measured Metric Values for Randomly Selected and Scrambled DCT-Blocks.

Metrics /Block Size	**Measured Average value for Randomly Selected DCT Blocks Scrambling**			
	Without any AC Coefficient Scrambled	With 5th AC Coefficient Scrambled	With 5th ,4th and 3rd AC Coefficient Scrambled	With 5th , 4th, 3rd, 2nd and 1st AC Coefficient Scrambled
PSNR	18.2316	17.9595	17.6555	16.6183
SSIM	0.7533	0.6234	0.5140	0.3483
MS-SSIM	0.7073	0.6701	0.6232	0.4891
VSNR	7.7933	7.7002	7.4011	6.2094
VIF	0.5277	0.2593	0.1467	0.0673
VIFP	0.5975	0.2634	0.1787	0.07243
UQI	0.6877	0.4275	0.3241	0.1775

6.2.6 Compression Analysis

An analysis has also been done to investigate the effect of encryption on compression. The corresponding graphs are shown in Fig. 6.10. A minor effect of scrambling on compression efficiency can be noticed in the graph. It can be explained from the fact that when the DCT blocks are scrambled, the positions of the DC coefficients are also changed which will result in the change in difference between the two DC coefficients in the consecutive blocks. Since, in JPEG compression standard the difference is encoded for DC coefficients, the compression is slightly affected. Also, due to the scrambling of the AC coefficients, the positions of the coefficients are changed resulting in different RUNLENGTHS. However, the change in compression ratio is from 22:1 to 18:1 which is not very significant in the case of multimedia encryption.

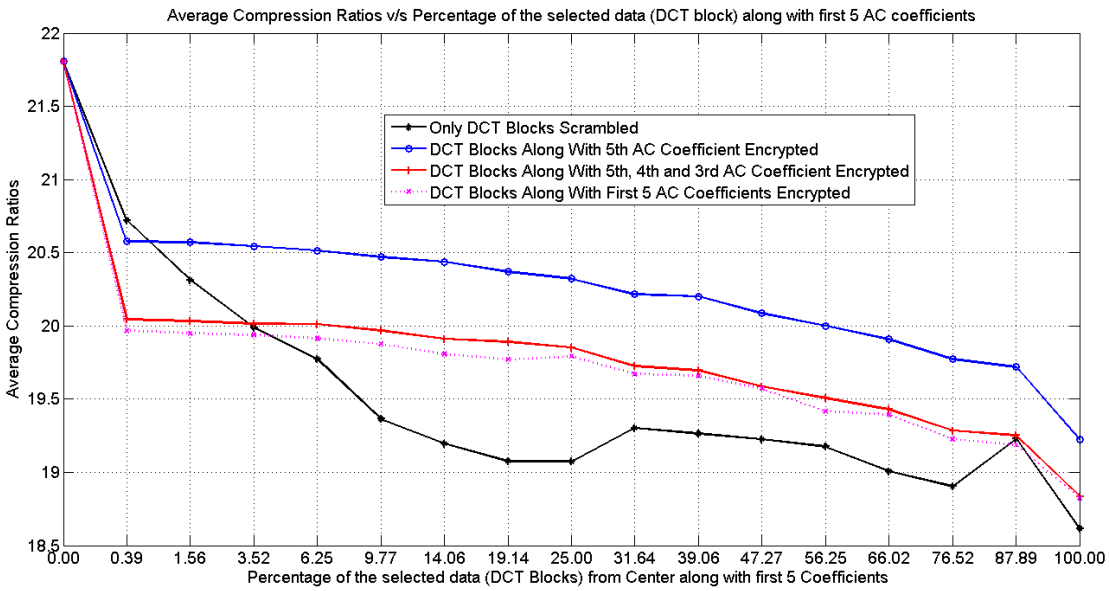


Figure 6.10: Average Compression Ratios vs. Number of Selected DCT Block from Center along with first 5 AC Coefficient.

The analysis shows that the change in the compression ratios varies for image to image. Scrambling can give rise to different RUNLENGRHS which may result in different compression ratios. However, there is no way of knowing whether scrambling will increase or decrease the compression ratio.

6.2.7 Security Analysis

Similar to the security analysis of the perceptual encryption scheme in JPEW, the security of the proposed scheme can be assessed. However, in this designed scheme there is no limitation on the selection of data which was in the design of JPEW, thus it allows the freedom to manipulate more data in order to strengthen perceptual security and the increased level of degradation.

6.2.7.1 Image Restoration Techniques

The discussion on perceptual security will also be the same as discussed in section 4.4.1, for the perceptual encryption scheme in JPEW, and is measured by IQAs as shown in the tables presented after each case / variant. However, In this case the techniques to restore encrypted image is different as compared to the earlier perceptual encryption scheme. It has been concluded from section 4.4.1 that the restoration using filtering techniques i.e. wiener filter with filter type 'unsharp' and 'gausian', denoising and enhancement techniques etc. are unable to restore the original image. These filtering techniques are based on the assumption that the encrypted image is original image plus noise. Similarly, the Attack-Zero also does not provide any good approximation of the ROI encrypted image as, setting the ROI of the image will further worsen the quality of image.

Another potential attack on ROI based scheme is to extrapolated the pixel values from the available unencrypted data in the surrounding or ROI. Some readily available interpolation techniques and extrapolation techniques are used i.e. Difference Table Method [73], Liner Extrapolation [74], Cubic spline interpolation [75] and Piecewise cubic Hermite interpolation [76]. Fig 6.11 shows the image recovered by using the Piecewise cubic Hermite interpolation technique. This was implemented in MATLAB with the help of MATLAB function 'interp1' with the method argument as 'pchip'. As can be seen from the figure the ROI after the recovery is still no meaningful. Thus, it is concluded that it is not possible to interpolate / extrapolate the encrypted pixel values by using these techniques. Thus the encrypted data cannot be recoverable using those techniques.

Figure 6.11: Encrypted ROI of Cameraman image recovered by using Piecewise cubic Hermite interpolation technique [76].
(PSNR = 14.8, SSIM = 0.7097, MS-SSIM = 0.5203)

6.2.7.2 Rearrangement Attack

Consider a case when all the 8×8 DCT blocks of image of size 256×256 is being scrambled along with the first 5 AC coefficients. This scrambling of a coefficients and DCT blocks are independent of each other. So an exhaustive search of possible combinations of DCT blocks and AC coefficients is required to recover the image. As mentioned in [77], security is required against two types of attackers (i.e. casual listeners / observers and professional unauthorized recipients). For casual listeners / observers security is required only for few hours but for professional unauthorized recipients (cryptanalysts) security is required for years. The variants of DCT block scrambling discussed are suitable for casual listeners/observers and may not be effective in case of professional cryptanalyst.

6.3 Summary

In this chapter the results of the proposed perceptual encryption schemes are presented and their performances are evaluated in detail. First, the results of ROI based scheme and its variants are presented. Then the results of second extended

perceptual encryption scheme are presented and its performance is analysed. It is also found to be secure and its effect on the compression ratios is negligibly.

CHAPTER 7

CONCLUSIONS AND FUTURE WORK

7.1 Introduction

In the last five chapters, a detailed literature review, the proposed Joint Perceptual Encryption and Watermarking scheme (JPEW) and a ROI block based scrambling for perceptual encryption have been presented. Moreover, the performance of each presented scheme has been evaluated thoroughly as well. In this chapter, some conclusions will be drawn from the entire work that has been presented including some recommendations for future work.

7.2 Conclusions

In this thesis, a novel joint perceptual encryption and watermarking scheme within JPEG framework is designed and evaluated. The design was arrived at by a detailed and exhaustive literature survey of different types of multimedia content encryption available in the literature. To the best of our knowledge, the literature covered is up to date and includes all the Joint Encryption and Watermarking techniques (Commutative Encryption and Watermarking Techniques), Perceptual Encryption schemes for images / videos and DC component based Watermarking schemes. The detailed survey on the above mentioned areas has led us to identify the space for research which are listed as hereunder:

- The idea of Joint or Commutative Encryption and Watermarking is relatively new, thus, not much work has been done in this area. Only six schemes have

been proposed in the literature. None of these schemes are within JPEG framework. A detailed survey in this area is required to identify the potential problems and to generate ideas to solve those problems.

- Along with the growth in internet technologies and multimedia commerce, the usage of those applications that involve perceptual encryption has also significantly increased, but up until now, not much work has been reported in this respect. One of the reasons is due to the unavailability of objective quality assessment metrics to assess the image quality. Subjective quality assessment metric involves human labour which is not suitable in real time applications. Also, not a detailed design of any perceptual encryption scheme has been presented in the literature.

- There is always a need for an efficient design of any encryption scheme. Additionally, efficiency of the scheme can be increased if the encryption scheme is compliant with some compression standards as most of the multimedia data are transmitted in compressed form. Thus, an encryption scheme that is compliant with a compression standard also reduces computational cost.

- In respect of watermarking, not many of the schemes which are based on DC component have been presented in the literature. Thus, it is also desirable to explore new, efficient and secure ways to watermark the DC component.

By keeping the above points in consideration and based on the knowledge acquired from the literature survey, in this thesis different aspects of the proposed schemes have been explored. This was done with the help of experimental results as well as analytical study.

In this thesis, an idea of Joint Perceptual Encryption and Watermarking (JPEW) has been presented. Some work on Joint Encryption and Watermarking can be found in the literature, but the design and framework of Joint Perceptual Encryption and Watermarking that is compliant with JPEG compression standard is novel in its

nature. The main objective for the design of JPEW is to achieve maximum efficiency and to reduce the computational cost by performing the operations (compression, perceptual encryption and watermarking), independent of each other. This is very critical in real time applications. For example, in the case of broadcasting live football match, the football match is only valuable when it is being broadcast live without any delay. Decreasing these delays would surely increase the efficiency of the whole system. The main reason behind the delay is the inability of the system to perform the mentioned operations simultaneously on the same multimedia content.

Thus, a design of a joint perceptual encryption and watermarking (JPEW) scheme that is integrable within JPEG framework is proposed in this research work. The design of JPEW can be split into three phases (i) Intelligent splitting of data, (ii) Design of a perceptual encryption scheme and (iii) Design of a watermarking scheme. The intelligent splitting of data in the proposed work is based on statistical analysis of the continuous-tone greyscale still images. Derived from this analysis it was decided to use first 9 AC coefficients and last four significant bitplanes to achieve perceptual degradation in the content and DC components least significant bitplanes to embed the watermark. Next, a perceptual encryption scheme based on scrambling of the AC coefficients and DC bitplanes in transformed (frequency) domain was presented. The scrambling was carried out after quantization in JPEG. One of the most worth mentioning contribution of the presented work is the usage of newly designed Objective Image Quality Assessment metrics, i.e. SSIM, MS-SSIM, VIF, VIFP, instead of using classical metrics like PSNR and MSE, which are not suitable for assessing the quality of images as PSNR and MSE only measure the errors introduced in the content. In contrast, IQAs are specially designed to measure the similarity between the images. In the proposed perceptual encryption scheme, the control factor can be selected from the design curve that is produced by measuring the progressive degradation in the image by IQAs. One can select the number of AC coefficients (the number would act as a control factor or quality loss factor) to be scrambled corresponding to the desired percentage of degradation in the image. Then, a blind watermarking scheme that is based on DC component was presented. The proposed

watermarking scheme is designed by exploiting the fact that DC component has most of the energy in DCT block. Most of the watermarking schemes in the literature in Discrete Cosine Transformed domain are based on AC component. The basis for not using the DC component for the watermarking purpose is because of its high energy, and any modification in DC component will affect the quality of the image. However, the division of DC component into bitplanes and only using the least significant bitplanes to substitute the watermark bits resolves this issue as shown by the presented experimental results. The selection of bitplanes can be made generic by using the texture information, but logically it will not be the best practice for real time applications. Also, a bitplane analysis was done to study the relationship between the payload and the number of bitplanes to embed the watermark. The proposed watermarking scheme enables one to select the appropriate number of bitplanes to distribute the watermark, and provides more choices for inserting watermark in images by optimizing the trade-off between image quality and payload. Thus, allowing one to have more control over watermarking images.

The performance evaluation of the JPEW was also carried out individually in terms of performance evaluation of perceptual encryption scheme and performance evaluation of watermarking scheme. In addition, for the evaluation of the perceptual encryption scheme a compression analysis was also done. From the compression analysis, it is found that the perceptual encryption scheme has negligible effect on the compression ratios. The compression analysis was not given much importance in the previously proposed multimedia encryption schemes despite the fact that the encryption algorithm can influence the compression ratio which could result in compromising the efficiency of the overall system. Moreover, a comparison of the proposed perceptual encryption scheme was also carried out with a recently proposed RHS based perceptual encryption scheme. The proposed perceptual encryption scheme out performs the RHS based scheme in terms of lesser computational load. Moving forward to the performance evaluation of the watermarking scheme, an analysis for the imperceptibility was carried out and the watermarking was also compared with the commonly used QIM based watermarking scheme. The proposed

watermarking scheme is found to be imperceptible. It was observed that the watermarked image and the original image were identical to each other. In other words there were no perceptual degradation in the quality of the image after being watermarked, thus also satisfying the property of imperceptibility. Additionally, application of the proposed watermarking scheme in medical images was discussed because of its imperceptibility. The results have shown that the proposed scheme is more can serve for storing copyright information as well as used for authentication and tamper detection. Moreover, the scheme is simpler in implementation with low overhead cost. The proposed watermarking scheme can also be used independently from joint scenario.

The security analysis of the JPEW has also been carried out by conducting attacks. These attacks include image restoration attacks by using filtering techniques to evaluate perceptual security. In this attack the degradation in the image is treated as noise thus common filtering techniques i.e. wiener filtering, denoising etc. were applied to remove the noise and restore original image. However it was shown that by using these techniques it is not possible to restore original image. Another study was done to assess the affect of attack named as attack-zero. In this attack it is assumed that the attacker has the knowledge of the encrypted data so the attacker sets the encrypted data equal to zero. It was concluded and suggested that by choosing 5 as minimum value of control factor will also make this attack useless. Also a rearrangement attack is discussed which is also found to be ineffective in this case. Thus proposed scheme can be regarded as perceptually secure. Furthermore, the robustness of the watermarking was evaluated in which the watermarked image was placed under common signal processing modifications and the scheme was found to be robust. In last a discussion has also been made on a watermark replacement attack, in which it is concluded that without the knowledge of the key, the replacement of the watermark is not possible. Key size and key management have also been discussed.

Moreover, a stand-alone perceptual encryption schemes was presented besides JPEW. The presented perceptual encryption scheme was ROI based, where degradation was achieved by scrambling of DCT blocks. Also several variant of

scrambling of DCT blocks, along with selected AC coefficients, were presented in a similar manner as the perceptual scheme presented in JPEW design. The design of this scheme is focused on providing the security against casual attacker. Hence providing more levels of perceptual encryption or in other words, providing more choices for selecting the control factor (quality loss factor). Finally, the performance of the presented perceptual encryption scheme was evaluated in terms of compression and security analysis. Minor change in the compression ratios was noticed for the proposed scheme. For the security analysis, previously conducted attacks on JPEW were ineffective on the ROI based scheme. However, in the ROI based scheme the availability of the unencrypted data on the surroundings of ROI enable extrapolation/interpolation attack, which was carried out on the ROI encrypted image. It was concluded that using interpolation/extrapolation techniques the recovery of unencrypted image also not possible, thus making the ROI scheme secure.

7.3 Thesis Contribution

The contribution of the work presented in this thesis includes the following,

- A novel design of Joint Perceptual Encryption and Watermarking Scheme (JPEW), which according to the best of our knowledge is the first design being reported in this area, has been presented in this thesis. The designed scheme is within JPEG compression standard and is composed of the following two parts:

    - ✓ A perceptual encryption scheme designed based on statistical analysis of continuous-tone still images and involves the usage of newly developed Objective Image Quality Assessment Metrics for the development of design curves which enables selection of control factor.

- ✓ A DCT based blind watermarking scheme based on DC component bitplanes. Achieving high level of imperceptibility, this watermarking scheme can be used independently especially in applications involving sensitive images (i.e. medical images).

- A stand-alone perceptual encryption schemes for the application of multimedia content preview. This scheme is simple to implement and is easily integrated in JPEG because of the fact that most of the visual data are transmitted in compressed form. Again the newly developed Objective Image Quality Assessment metrics were used to measure the perceptual quality of the images instead of PSNR and MSE which are commonly used but are not suitable to measure similarity between two images.

- The performances of all the proposed schemes have also been analysed for overall security and computational cost.

7.4 Future Work

- The proposed schemes can be further implemented on other DCT based codecs i.e. MPEG 2, H.264/MPEG4 and their performance over these codecs can be evaluated.

- Besides using objective quality assessment metrics, subjective quality measurements can also be used to improve the experimental results and analyses.

- The proposed watermarking scheme can also be further refined to adaptive selection of quantized DC component bitplanes depending upon the texture information in the image.

- Issues related to Joint Encryption and Watermarking also need to be addressed and the development of more secure and efficient schemes need to be devised,

in which the encryption and watermarking can be done on the same data without using partial encryption.

- A standard image quality assessment metrics need to be developed, one which will enable benchmarking of the experimental results.
- The scheme can be implemented within JPEG codecs and MPEG codecs either in hardware or software and evaluated.
- The work could be extended to distributed source coding framework.

References

[1] B.M. Macq and J.-J. Quisquater. (2002, Jun.). Cryptology for Digital TV Broadcasting. *Proc.of IEEE*. *83(6)*, pp. 944 – 957.

[2] I. Cox, M. Miller, J. Bloom, J. Fridrich and T. Kalker, *Digital Watermarking and Steganography.* 2nd Ed. San Francisco, CA: Morgan Kaufmann, 2007.

[3] S. Lian, Z. Liu, R. Zhen, and H. Wang, "Commutative watermarking and encryption for media data," *Optical Engineering*, 2006, vol. 45, no. 8, pp. 080 510.1 – 080 510.3.

[4] *ADVANCED ENCRYPTION STANDARD (AES)*, Federal Information Processing Standards Publication 197, November 26, 2001.

[5] *DATA ENCRYPTION STANDARD (DES)*, Federal Information Processing Standards Publication 46-2, December 30, 1993.

[6] X. Lai and J. L. Massey, "A proposal for a new block encryption standard," In *Proc. of the workshop on the theory and application of cryptographic techniques on Advances in cryptology (EUROCRYPT)*, 1991, vol. 473 of LNCS, pp. 389 – 404.

[7] Y. Matias and A. Shamir, "A Video Scrambling Technique Based On Space Filling Curves," *in Advances in Cryptology - CRYPTO'87, 1987,* vol. 293 of LNCS, pp. 398 – 417.

[8] L. Qiao and K. Nahrstedt, "A New Algorithm for MPEG Video Encryption," In *Proc. 1st Int. Conf. on Imaging Science, Systems, and Technology (CISST'97)*, Las Vegas, NV, 1997, pp.21 – 29.

[9] P.P. Dang and P.M. Chau, "Image encryption for secure Internet multimedia applications," In *Proc. of Int. Conf. on Consumer Electronics (ICCE)*, 2000, vol.46, no.3, pp.6 – 7.

[10] X. Yi, C. H. Tan, C. K. Slew, and M. R. Syed. (2001, Feb.). Fast encryption for multimedia. *IEEE Trans. on Consumer Electronics*. *47(1)*, pp.101 – 107.

[11] Q. Hou and Y. Wang, “Security traffic image transmission based on EZW and AES,” In *Proc. IEEE Int. Conf. on Intelligent Transportation Systems*, 2003, vol.1, pp. 86 – 89.

[12] M. V. Droogenbroeck, “Partial Encryption Of Images For Real-Time Applications,” In *Proc. 4th IEEE Signal Processing Symposium*, Hilvarenbeek 2004, pp. 12 – 15.

[13] W. Zeng and S. Lei. (2003, Mar.). Efficient frequency domain selective scrambling of digital video. *IEEE Trans. on Multimedia*. *5(1)*, pp. 118 – 129.

[14] M. Podesser, H-P. Schmidt, and Andreas Uhl, “Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environments,” In *Proc. 5th Nordic Signal Processing Symposium*, on board Hurtigruten, 2002, pp. 1037.

[15] A. Said and W.A. Pearlman. (1996, Jun.). A new, fast, and efficient image codec based on set partitioning in hierarchical trees. *IEEE Trans. on Circuits and Systems for Video Technology*. 6(3), pp.243 – 250.

[16] M. V. Droogenbroeck and R. Benedett, “Techniques for a selective encryption of uncompressed and compressed images,” In *Proc. of Advanced Concepts for Intelligent Vision Systems (ACIVS)*,2002, pp.90 – 97.

[17] J.M Rodrigues, W. Puech, and A. G Bors, “Selective Encryption of Human Skin in JPEG Images," In *Proc. IEEE Int. Conf. on Image Processing*, 2006, pp.1981 – 1984.

[18] L. Weng and B. Preneel, “On Encryption and Authentication of the DC DCT Coefficient,” In *Proc. 2nd Int. Conf. on Signal Processing and Multimedia Applications (SIGMAP)*, 2007, pp. 375 – 379.

[19] C. N. Raju, K. Srinathan, and C.V Jawahar, “A Real-Time Video Encryption Exploiting the Distribution of the DCT coefficients,” *IEEE Region 10 Conf. TENCON*, 2008, pp. 1 – 6.

[20] A. Torrubia, and F. Mora, “Perceptual cryptography of JPEG compressed images on the JFIF bit-stream domain,” *IEEE Int. Conf. Consumer Electronics (ICCE)*, 2003, pp. 58 – 59.

[21] S. Li, G. Chen, A. Cheung, B. Bhargava, and K.-T. Lo. (2007, Feb.). On the Design of Perceptual MPEG-Video Encryption Algorithms. *IEEE Trans. On Circuits And Systems For Video Technology. 17(2),* pp. 214 – 223.

[22] S. Lian, J. Sun and Z. Wang, "Perceptual cryptography on SPIHT compressed images or videos," In *Proc. IEEE Int. Conf. on Multimedia and Expo (ICME),* 2004, vol.3, pp. 2195 – 2198.

[23] S. Lian, J. Sun and Z. Wang, "Perceptual cryptography on JPEG2000 compressed images or videos," In Proc. *The 4th Int. Conf. on Computer and Information Technology (CIT),* 2004, pp. 78 – 83.

[24] S. Lian, J. Sun and Z. Wang, "Perceptual cryptography on MPEG compressed videos," In *Proc. Int. Conf. on Signal Processing (ICSP),* 2004, vol.3, pp. 2371 – 2374.

[25] S. Lian, D. Ye, J. Sun, and Z. Wang, "Perceptual MPEG-4 video encryption and its usage in video-on demand systems," *IEEE Int. Symposium on Consumer Electronics,* 2004, pp. 83 – 86.

[26] B. Bhargava, C. Shi, and S.-Y. Wang. (2004, Sept.). MPEG video encryption algorithms. *J. Multimedia Tools and Applications. 24(1),* pp. 57 – 79.

[27] A. Torrubia, and F. Mora, "Perceptual cryptography on MPEG-1 layer III bit-streams," In *Proc. Int. Conf. on Consumer Electronics (ICCE),* 2002, pp. 324 – 325.

[28] A.S Tosun and W.-C. Feng, "Efficient multi-layer coding and encryption of MPEG video streams," In *Proc. IEEE Int. Conf. on Multimedia and Expo (ICME),* 2000, vol.1, pp.119 – 122.

[29] B. B Zhu, C. Yuan, Y. Wang, and S. Li. (2005, Apr.). Scalable protection for MPEG-4 fine granularity scalability. *IEEE Transactions on Multimedia. 7(2),* pp. 222 – 233.

[30] S. Wee, and J. Apostolopoulos, "Secure scalable streaming and secure transcoding with JPEG-2000," In *Proc. Int. Conf. on Image Processing (ICIP),* 2003, vol.1, pp. I- 205 – 8.

[31] W. Tang and Y. Aoki, "A DCT-based coding of images in watermarking," Information, In *Proc. Int. Conf. on Communications and Signal Processing (ICICS)*, 1997, vol.1, pp.510 – 512.

[32] M. Al Baloshi and M.E. Al-Mualla, "A DCT-Based Watermarking Technique for Image Authentication," In *Proc. IEEE/ACS Int. Conf. on Computer Systems and Applications, (AICCSA '07)*, 2007, pp.754 – 760.

[33] C.-C. Wang and Y.-C. Hsu, "Fragile Watermarking Algorithm for DCT-Domain Image Authentication and Recompression," In *Proc. 24th Workshop on Combinatorial Mathematics and Computation Theory (CMCT'07)*, 2007, pp. 158 – 161.

[34] N. Hubballi and Kanyakumari D P. (2009, May). Novel DCT based watermarking scheme for digital. Int. J. of Recent Trends in Engineering. 1(1), pp.430 – 433.

[35] J. Huang, Y. Q. Shi, and Y. Shi. (2000 Sept.). Embedding image watermarks in dc components. IEEE Trans. on Circuits and Systems for Video Technology. 10(6), pp.974-979.

[36] H. Lu, X. Shi, Y.Q. Shi, A.C. Kot, and L. Chen, "Watermark embedding in DC components of DCT for binary images," *IEEE Workshop on Multimedia Signal Processing*, 2002, pp. 300 – 303.

[37] F. Deng and B. Wang, "A novel technique for robust image watermarking in the DCT domain," In *Proc. Int. Conf. on Neural Networks and Signal Processing*, 2003, vol.2, pp. 1525 – 1528.

[38] M.-H. Lee, M.-F. Horng and B.-C. Chang, "A DC-based Approach to Robust Watermarking with Hamming-Code," In *Proc. 3rd Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, 2007, vol.2, pp.369 – 372.

[39] G. Zeng and Z. Qiu, "Image Watermarking Based on DC Component in DCT," In Proc. *Int. Symposium on Intelligent Information Technology Application Workshops (IITAW '08)*, 2008, pp.573 – 576.

[40] S. Lian, "Commutative Watermarking and Encryption," in *Multimedia Content Encryption: Techniques and Applications*. CRC press, 2008, ch.9, pp. 132.

[41] S. Lian, Z. Liu, Z. Ren and H. Wang. (2007, Jun). Commutative Encryption and Watermarking in Video Compression. *IEEE Trans. on Circuits and Systems for Video Technology. 17(6),* pp.774-778.

[42] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. De Natale, and A. Neri, "A joint digital watermarking and encryption method," In *Proc. SPIE*, 2008, vol. 6819, pp. 68191C – 68191C-10.

[43] F. Battisti, M. Cancellaro, M. Carli, G. Boato, and A. Neri, "Watermarking and encryption of color images in the Fibonacci domain", In *Proc. SPIE*, 2008, vol. 6812, pp. 68121C – 68121C-9.

[44] F. Battisti, M. Cancellaro, G. Boato, M. Carli, and A. Neri. (2009, Jan.). Joint watermarking and encryption of color images in the Fibonacci-Haar domain. *EURASIP J. on Advances in Signal Processing. 2009*.

[45] S. Lian. (2009, May). Quasi-commutative watermarking and encryption for secure media content distribution. *J. of Multimedia Tools Applications. 43(1)*, pp. 91 – 107.

[46] G. K. Wallace. (1992, Feb.). The JPEG still picture compression standard. IEEE Transactions on Consumer Electronics. 38(1), pp. xviii – xxxiv.

[47] J. Meyer and F. Gadegast. (1995, May). Security Mechanisms for Multimedia Data with the Example MPEG-1 Video - Project Description of SECMPEG. Technical University of Berlin, Germany, Available: http://www.gadegast.de/frank/doc/secmeng.pdf

[48] Peak Signal-to-Noise Ratio (PSNR), http://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio

[49] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli. (2004, Apr.). Image quality assessment: from error visibility to structural similarity. *IEEE Trans. on Image Processing. 13(4)*, pp.600- 612.

[50] Z. Wang, E. P. Simoncelli, and A. C. Bovik, "Multi-scale structural similarity for image quality assessment," In *Proc. IEEE Asilomar Conf. Signals, Systems and Computers*, 2003, pp. 1398 – 1402.

[51] H.R. Sheikh and A.C. Bovik. (2006, Feb.) Image information and visual quality. *IEEE Trans. on Image Processing. 15(2)*, pp. 430- 444.

[52] D. M. Chandler and S. S. Hemami. (2007, Sept.). VSNR: A Wavelet-Based Visual Signal-to-Noise Ratio for Natural Images. *IEEE Trans. on Image Processing. 16(9)*, pp. 2284 – 2298.

[53] Z. Wang and A. C. Bovik. (2002, Mar.). A universal image quality index. *IEEE Signal Processing Letters, 9(3)*, pp. 81-84.

[54] H.R. Sheikh, A.C. Bovik and G. de Veciana. (2005, Dec.). An information fidelity criterion for image quality assessment using natural scene statistics. *IEEE Trans. on Image Processing. .14(12)*, pp. 2117 – 2128.

[55] Available at http://www.utp.edu.my/index.php?option=com_content&view=article&id=52&Itemid=1907

[56] J. Mannos and D. Sakrison. (1974, Jul). The effects of a visual fidelity criterion of the encoding of images. *IEEE Transactions on Information Theory. 20(4)*, pp. 525 – 536.

[57] M. A. Khan, "A Novel Seed Based Random Interleaving for OFDM System and Its PHY Layer Security Implications," MSc Thesis, Department of Electrical and Electronic Engineering, Universiti Teknologi PETRONAS, Tronoh, Perak, Malaysia, 2008.

[58] M. Asim, "A Hybrid Chaotic Image Encryption Scheme Based on S-Box and ciphertext Feedback," MSc Thesis, Department of Electrical and Electronic Engineering, Universiti Teknologi PETRONAS, Tronoh, Perak, Malaysia, 2007.

[59] M. I. Khan, V. Jeoti, and M. A. Khan, "Perceptual Encryption of JPEG Compressed Images Using DCT Coefficients and Splitting of DC Coefficients into Bitplanes," In Proc. 3rd Int. Conf. on Intelligent & Advanced Systems 2010 (ICIAS), Kuala Lumpur, Malaysia, 15 – 17 June 2010.

[60] B. Yang, C. Busch, and Xiamu Niu, "Perceptual image encryption via reversible histogram spreading," In *Proc. of 6th Int. Symposium on Image and Signal Processing and Analysis (ISPA)*, 2009, pp.471 – 476.

[61] J. Fridrich, "Image encryption based on chaotic maps," In *Proc. IEEE International Conference on Computational Cybernetics and Simulation*, Orlando, 1997, vol.2, pp.1105 – 1110.

[62] X. Shi, F. Liu, D. Gong, and J. Jing, "An Authentication Watermark Algorithm for JPEG images," *In Proc. Int. Conf. on Availability, Reliability and Security (ARES)*, 2009, pp.584 – 588.

[63] H. Wang and C. Liao, "Compressed-domain fragile watermarking scheme for distinguishing tampers on image content or watermark," In *Proc. Int. Conf. on Communications, Circuits and Systems (ICCCAS)*, 2009, pp.480 – 484.

[64] X. Q. Zhou, H. K. Huang, and S. L. Lou. (2001, Aug). Authenticity and integrity of digital mammography images. *IEEE Trans. on Medical Imaging. 20(8)*, pp.784 – 791.

[65] U. Rajendra Acharya, D. Acharya, P. Subbanna Bhat, and U. C. Niranjan. (2001, Dec.). Compact storage of medical images with patient information. *IEEE Trans. on Information Technology in Biomedicine. 5(4)*, pp.320 – 323.

[66] H.-M. Chao, C.-M. Hsu, and S.-G. Miaou. (2002, Mar.). A data-hiding technique with authentication, integration, and confidentiality for electronic patient records. *IEEE Trans. on Information Technology in Biomedicine. 6(1)*, pp.46-53.

[67] W. E. Snyder, N C State University Image Analysis Laboratory Database. Department of Electrical and Computer Engineering, North Carolina State University, 2002. http://www.ece.ncsu.edu/imaging/Archives/ImageDataBase/index.html.

[68] *Subjective audiovisual quality assessment methods for multimedia applications*, ITU-T Recommendation P.911, December, 1998.

[69] *Methodology for the subjective assessment of the quality of television pictures*, Recommendation ITU-R BT.500-12, September 1, 2009.

[70] Mean Square Error, http://en.wikipedia.org/wiki/Mean_square_error

[71] Signal-to-Noise Ratio, http://en.wikipedia.org/wiki/Signal-to-noise_ratio

[72] C.N. Raju, G. Umadevi, K. Srinathan and C.V. Jawahar, "Fast and Secure Real-Time Video Encryption," In *Proc. 6th Indian Conf. on Computer Vision, Graphics & Image Processing (ICVGIP)*, 2008, pp.257–264.

[73] Extrapolation Using a Difference Table, http://uva.onlinejudge.org/external/3/326.html

[74] Linear Interpolation, http://en.wikipedia.org/wiki/Linear_interpolation

[75] Cubic spline interpolation, http://www.mathworks.com/help/techdoc/ref/spline.html

[76] Piecewise cubic Hermite interpolation, http://www.mathworks.com/help/techdoc/ref/pchip.html

[77] Y. V. S. Rao, A. Mitra, and S. R. M. Prasanna, "A Partial Image Encryption Method with Pseudo Random Sequences," In *Proc. of Int. Conf. on Information Systems Security (ICISS), LNCS*, 2006, vol. 4332, pp. 315 – 325.

[78] MATLAB implementation Available at http://www.csse.uwa.edu.au/~pk/Research/MatlabFns/

[79] M. Gaubatz, " MeTriX MuX Visual Quality Assessment Package", Available: http://foulard.ece.cornell.edu/gaubatz/metrix_mux/

[80] S. Li, 200 Test Images, Available: http://hooklee.com/Papers/Data/AC2DC/Images.zip

[81] T. Shi, B. King, and P. Salama, "Selective encryption for H.264/AVC video coding," In *Proc. of the SPIE, Security, Steganography, Watermarking Multimedia Contents VIII*, 2006, vol. 6072, pp. 461 – 469.

[82] M. Noorkami and R. M. Mersereau, "Compressed-domain video watermarking for H.264," In *Proc. of IEEE Conf. on Image Processing*, 2005, vol. 2, pp. 890 – 893.

List of Publications

Conferences Papers:

- **Muhammad Imran Khan**, Varun Jeoti and Muhammad Asif Khan, "Perceptual Encryption of JPEG Compressed Images using DCT Coefficients and Splitting of DC DCT Coefficients into Bit Planes", in proceedings of 3rd International Conference on Intelligent & Advanced Systems 2010 (**ICIAS 2010**), (15-17 June 2010), **Kuala Lumpur**, **Malaysia**.
  Available at:
  http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5716133

- **Muhammad Imran Khan** and Varun Jeoti, "A blind Watermarking Scheme Using Bitplane of DC Component for JPEG Compressed Images", in proceedings of 6th International Conference on Emerging Technologies 2010 (**ICET 2010**), (18-19 October 2010), **Islamabad**, **Pakistan**.
  Available at:
  http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5638498

- **Muhammad Imran Khan**, Varun Jeoti and Aamir Saeed Malik, "Designing a Joint Perceptual Encryption and Blind Watermarking Scheme Compliant with JPEG Compression Standard", International Conference on Computer Applications & Industrial Electronics (**ICCAIE 2010**), (05-07 December 2010), **Kuala Lumpur**, **Malaysia**.
  Available at:
  http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5735022

- **Muhammad Imran Khan**, Varun Jeoti and Aamir Saeed Malik, "A DC Component Based Blind Watermarking Scheme for Medical Images", **4th East Asian Pacific Student Workshop on Nano-Biomedical Engineering**, (15 - 16 December 2010), National University of Singapore (NUS), **Singapore**. (15-16 DEC 2010).

Book Chapters:

- **Muhammad Imran Khan**, Varun Jeoti and Aamir Saeed Malik, "On Perceptual Encryption: Variants of DCT Block Scrambling Scheme for JPEG Compressed Images", SIGNAL PROCESSING AND MULTIMEDIA, Communications in Computer and Information Science, 2010, **CCIS**, Volume 123, pp. 212-223.
  Available at:
  http://www.springerlink.com/content/w142157008548880/

Research Work Presented On Other Platforms:

- **Muhammad Imran Khan**, Varun Jeoti and Aamir Saeed Malik, "On the Design of Joint Perceptual Encryption and Watermarking techniques for Multimedia Content" presented at "Explorative Analysis and Visualization of Large Information Spaces", 27. September - 01. October 2010, Klausen, **South Tirol**, **Italy**. (Organized by **University of Konstanz, Germany**).

An updated list of publications can be found on my website:

www.signalimran.com

APPENDIX A

Chaotic Scrambler Demystified

A.1. Introduction

For the proposed schemes presented in this thesis, a chaotic scrambler is adapted from [57-58], to perform the permutation operations. Any scrambling algorithm can serve the purpose which generates a position vector and have acceptable cryptographic security.

A.2. The Scrambling Process

The basic idea of chaotic scrambler is the usage of chaotic logistic map as given in (1),

$$x_{n+1} = r x_n (1 - x_n) \qquad \text{(A.1)}$$

where $0 < x_n < 1$ and $3.47 < r < 4$. When the value of "r" is between 3.47 and 4, it generates random values. A position vector is obtained by using chaotic logistic map in (1). The whole process can be simplified and explained into following steps,

- Step 1: To generate a position vector the value "r" is to be specified, although it could be any value in between 3.47 to 4.
- Step 2: Value of "x_n" is then generated. This value is also known as initial condition (IC) and is derived from 128 bit key and should lie between 0 and 1.
- Step 3: Intervals are then specified based on the number of input values to be permuted, for "N" input values the interval size will be "1/N". The can be understood by a simple example, if there are 8 input values to be

permuted then the length of the interval will be 1/8 = 0.125 and there will be 8 intervals as described by the diagram.

- Step 4: Using Eq.1 the value of "x_{n+1}" is calculated and the first value of the input vector is placed in the interval where the value of "x_{n+1}" is falls. For example if first value obtained for "x_{n+1}" is 0.447 this will fall in 4th interval thus first value of input vector will take 4th position. Iteration equal to the number of input values will take place to generate a new position for the input value.

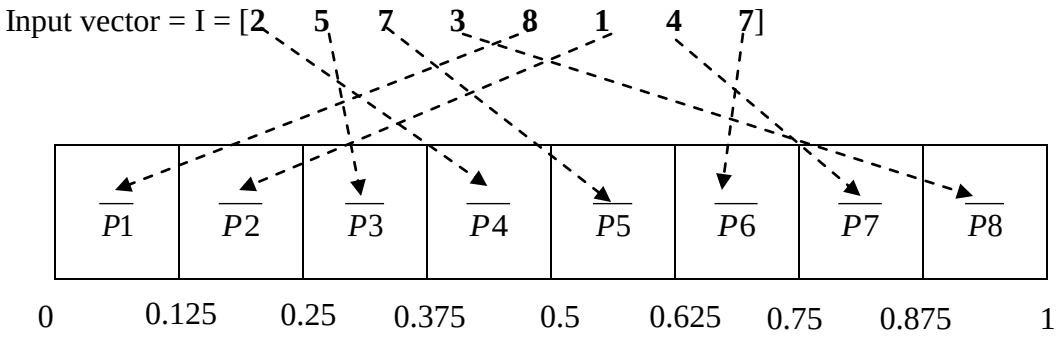


Figure A.1: The Scrambling Process.

APPENDIX B

Image Quality Assessment Metrics (IQA's) - Interpretation

B.1. Introduction

There are many image quality assessment metrics in the literature. However, the most commonly used metrics to measure the quality of the image are MSE and PSNR. But there metrics are not considered suitable in case of designing a perceptual encryption scheme and measuring the similarity between two images. As MSE and PSNR measure the errors introduced in the image they does not measure the perceptible similarity between the images [49]. Most reliable technique to measure the similarity between the images or to know the perceivable information through the image is to use subjective metrics which involve judgment of the human beings. Still efforts are going on to design objective metrics to measure the similarity between the images and videos. SSIM, MS-SSIM, VIF, VIFP and UQI are the results of this effort. These newly designed metrics are not yet widely used in the literature.

Due to the usage of these metrics in the proposed schemes, to clarify the proposed schemes and in order for better understanding, more information about these IQA's is provided by describing the how to interpret the obtained metric value. All the discussed objective image quality assessment metrics required original image to compare with thus making these metrics full reference quality assessment metrics. The MATLAB implementation of objective image quality assessment metrics in the package called MeTriX MuX Visual Quality Assessment (Version 1.1) can be found on [79].

B.1.1. SSIM (Structural SIMilarity)

Interpretation: If the value of SSIM is equal to '1' then both the compared images are same and if the value of SSIM is '0' then it means that both compared images are totally different have nothing in common. Mathematically,

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

Where *x* and *y* are two windows of size *M*×*M*. μ_x and μ_y are the *x* and *y*, respectively. σ_x^2 and σ_y^2 is the variance of *x* and *y*, respectively. σ_{xy} is the covariance of *xy*. C_1 and C_2 are variables to stabilize the division with weak denominator.

B.1.2. MS-SSIM (Multi-Scale Structural SIMilarity)

Interpretation: Alike, SSIM, if the value of MS-SSIM is equal to '1' then both the compared images are same and if the value of MS-SSIM is '0' then it means that both compared images are totally different.

B.1.3. MSE (Mean Squared Error)

Interpretation: Lower the MSE means image are similar, Higher the MSE mean the images are different or the resultant image has large amount or errors. Mathematically MSE is expressed as,

$$MSE = \frac{1}{l \times k} \sum_{i=0}^{l-1} \sum_{j=0}^{k-1} [img\_1(i,j) - img\_2(i,j)]^2$$

Where *img_1* and *img_2* are the images to be compared of size *l*×*k*.

B.1.4. SNR (Signal-to-Noise)

Interpretation: Similar to PSNR, VSNR and WSNR.

$$PSNR = 10\log_{10}\left(\frac{Mean(img\_1(i)^2)}{MSE}\right)$$

B.1.5. PSNR (Peak Signal-to-Noise Ratio)

Interpretation: Lower the PSNR value mean more errors and higher PSNR value means less errors. PSNR above 40 db for grey-scale image is considered good value. Mathematically PSNR can be defined as,

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)$$

255 is the maximum value in case of greyscale images.

B.1.6. VSNR (Visual Signal-to-Noise Ratio)

Interpretation: If the images are identical then the value of VSNR will be infinity and this values decreases with the increasing distortion in the image.

B.1.7. VIF (Visual Information Fidelity)

Interpretation: Alike, SSIM and MS-SSIM, if the value of MS-SSIM is equal to '1' then both the compared images are identical to each other and if the value of MS-SSIM is '0' then it means that both compared images are totally different.

B.1.8. VIFP (Pixel based VIF)

Interpretation: Similar to VIF, if compared images are same then it will return value equal to ‘1’ and if they are completely different then VIF will return value equal to ‘0’.

B.1.9. UQI (Universal Quality Index)

Interpretation: UQI also follows the same scale of measurement as in case of SSIM, MS-SSIM, VIF, VIFP, if images are same then UQI value will be ‘1’ and if completely different then it will be ‘-1’. UQI can be considered as a special case of SSIM in which C1 and C2 are zero.

B.1.10. IFC (Information Fidelity Criterion)

Interpretation: The value of IFC decreases with the increase in distortion in the image.

B.1.11. WSNR (Weighted Signal-to-Noise Ratio)

Interpretation: Similar to VSNR, the value, when the images are same is infinity and decrease with the increase on distortion.

APPENDIX C

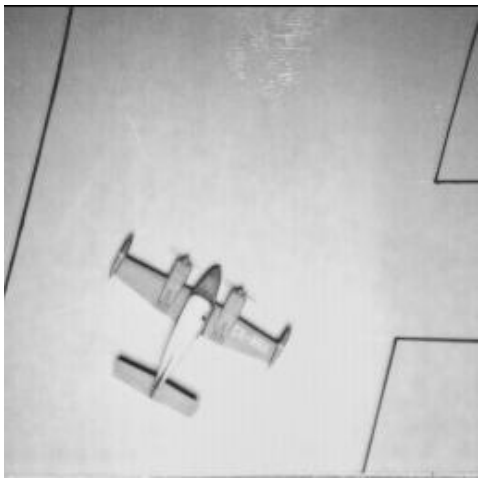
Standard Test Images
(Continuous-Tone Grey-Scale Images)

The images given below are some of the images used in presented research work. All of the following shown images are continuous-tone grey-scale images, having 8 bits per pixel (bpp). These images are of different sizes and most commonly used images and known as standard test images. These images can be found on [80]. The sizes of the images are reduced to that they can be easily be fitted. These images have different texture information, in which some have smooth background and some having small details.

256×256 grey-scale images having 8 bits per pixel (bpp)

Aerial

Airfield



Airplane

Birds

Girl 1

Bridge

Cameraman

Chemical Plant

Clock

Girl 2

Girl 3

Girl 4

House

Jelly Beans

Lena

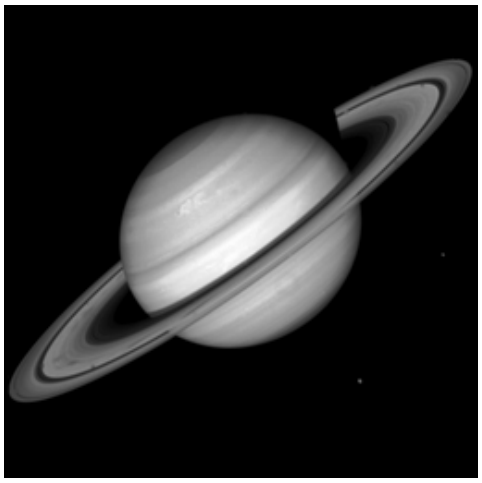
Man

Moon Surface

Panda

Pavilion

River

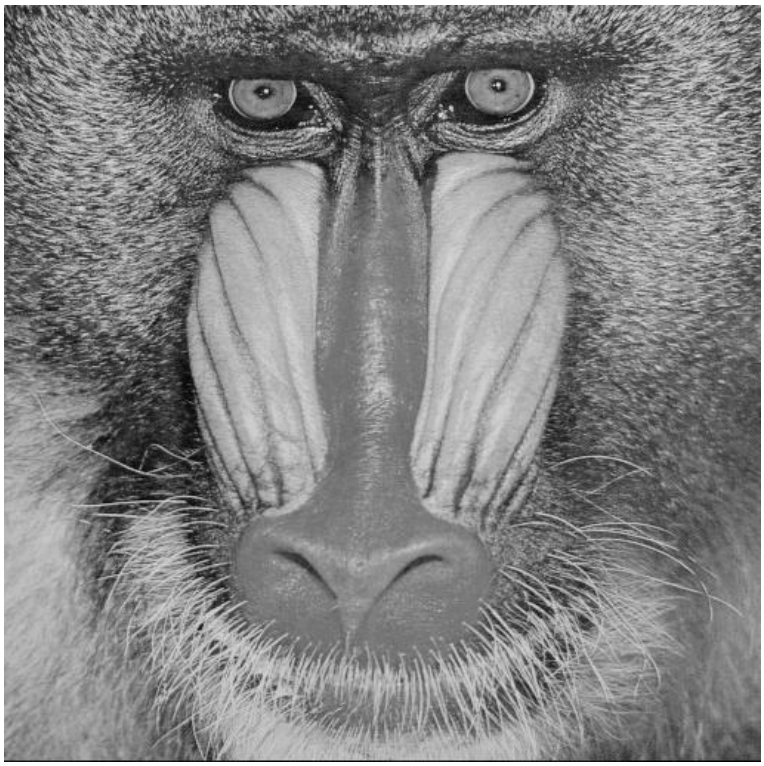


Saturn

Tree

Vulture

512×512 grey-scale images having 8 bits per pixel (bpp)



Baboon

Barbara

Boats

Bridge

Goldhill

House

Lake

Lena

Living Room

Man

Peppers

Plane

Women