

DIGITAL WATERMARKING USING PRINCIPAL COMPONENT ANALYSIS AND ARNOLD CAT MAP SCRAMBLING TECHNIQUE

A DISSERTATION
SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT
FOR THE AWARD OF THE DEGREE
OF

MASTER OF TECHNOLOGY
IN
SIGNAL PROCESSING AND DIGITAL DESIGN

Submitted by

TEMSHICHANG JONGKO

2K13/SPD/20

Under the supervision of

Mr. JEEBANANDA PANDA

(Associate Professor)



**DEPARTMENT OF ELECTRONICS AND
COMMUNICATION ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY**

(Formerly Delhi College of Engineering)

Bawana Road, Delhi-110042

2015

Certificate

This is to certify that the dissertation title “*Digital Watermarking Using Principal Component Analysis and Arnold Cat Map Scrambling technique*” submitted by **Mr Temshichang Jongko**, Roll. No. *2K13/SPD/20*, in partial fulfilment for the award of degree of Master of Technology in Signal Processing & Digital Design at **Delhi Technological University, Delhi**, is a bonafide record of student’s own work carried out by him under my supervision and guidance in the academic session 2013-15. To the best of my belief and knowledge the matter embodied in dissertation has not been submitted for the award of any other degree or certificate in this or any other university or institute.

Jeebananda Panda
Supervisor
Associate Professor
Dept. of ECE
Delhi Technological University

Acknowledgement

I am indebted to my thesis supervisor **Mr. Jeebananda Panda, Associate Professor** Department of Electronics and Communication, for his gracious encouragement and very valued constructive criticism that has driven me to carry out the project successfully.

I am greatly thankful to **Prof. Prem R. Chadda**, Head of Department (Electronics & Communication Engineering), entire faculty and staff of Electronics & Communication Engineering and friends for their continuous support, encouragement and inspiration in the execution of this “**thesis**” work.

Finally I express my deep sense of gratitude to my parents who bestowed upon me their grace and were source of my inspiration and encouragement.

Temshichang Jongko

M.Tech (SPDD)

2K13/SPD/20

CONTENTS

CERTIFICATE	i
ACKNOWLEDGEMENT	ii
LIST OF TABLES	v
LIST OF FIGURES	vi
LIST OF ABBREVIATIONS	viii
ABSTRACT	ix

1 INTRODUCTION

1.1 Introduction.....	2
1.2 Motivation.....	3
1.3 Watermarking Requirements	5
1.4 Classes of embedding Methods	7
1.4.1 Modulation based Watermarking Algorithm	7
1.4.2 Watermarking with Side Information	8
1.4.3 Game Theoretic Watermarking.....	9
1.5 Watermarking Attacks and Performance measurement.....	9
1.5.1 Classifications of Attacks	10
1.5.2 Performance Measurement	14

2 LITERATURE REVIEW

2.1 Wavelet Transform	17
2.1.1 Continuous Wavelet Transform.....	18
2.1.2 Discrete Wavelet Transform	21
2.2 Wavelet Transform in Two Dimensions.....	25
2.3 Wavelet Families	32
2.4 Haar Wavelet Transform.....	37
2.4.1 Haar Functions.....	37
2.4.2 Haar Wavelet Properties	39
2.5 Principal Component Analysis	40
2.5.1 Traditional Principal Component Analysis.....	42
2.5.2 Deriving the PCA Using Covariance Method.....	42
2.5.3 Reason Why we use PCA	44
2.6 Arnold Cat Map	44
2.6.1 Introduction.....	44
2.6.2 Arnold Cat Map	45

2.6.3 Periodicity of Arnold Cat Map	46
3 Digital Watermarking Using Principal Component Analysis and Arnold Cat Map scrambling technique	
3.1 Introduction.....	50
3.2 Algorithm Description	50
3.3 Experimental Work and Discussion.....	54
3.4 Comparison and Discussion.....	67
4 Conclusion	
4.1 Conclusion	85
4.2 Future Work.....	86
REFERENCES	

LIST OF TABLES

2.1 Pixel dimension and number of iterations required	48
3.1 PSNR and Bit error of Host and watermarked frame	62
3.2 Data collected from extracted watermark after various attacks	66
3.3 Bit error for binary watermark	80
3.4 Normalised correlation for binary watermark.....	81
3.5 Normalised correlation for color watermark.....	82

LIST OF FIGURES

1.1 General Scheme Watermarking	3
1.2 Relationship Between Robustness, Imperceptibility and Payload	6
1.3 Typical Modulation based Watermarking System	7
1.4 Watermarking Using Side Information	8
1.5 Quantization Index Modulation System	9
2.1 Heisenberg Boxes of Two Wavelets	21
2.2 Haar Scaling function in V_0 and V_1	22
2.3 Haar wavelet Function in W_0 and W_1	23
2.4 Relationship between Scaling and wavelet function	24
2.5 Inverse fast wavelet transform synthesis filter bank	27
2.6 The fast wavelet analysis filter	28
2.7 The two dimensional analysis filter bank	29
2.8 Resulting Decomposition of two dimensional filter bank	29
2.9 Two dimensional inverse fast wavelet transform synthesis filter bank	30
2.10 Daubechies scaling factor and corresponding wavelets	33
2.11 Coiflet Wavelet	33
2.12 Shannon Wavelet	34
2.13 Morlet Wavelet	35
2.14 Mexican Hat Wavelet	36
2.15 Spectrum of Meyer Wavelet	36
2.16 Meyer Scaling function	36
2.17 Meyer Wavelet	37
2.18 Cat Mapping	46
3.1 Embedding Algorithm of proposed scheme	51
3.2 Extraction Algorithm of Proposed scheme	53
3.3 Original watermark	54
3.4 Arnold Cat map on original watermark	55
3.5 Scrambled watermark image for embedding	55
3.6 Red color component of the host video frames	56
3.7 Result after 3 level DWT on Host video frame	57
3.8 Watermarked frame	58

3.9 Red color component of watermarked frame	58
3.10 Result after 3 level DWT on watermarked frame	59
3.11 Extracted watermark	59
3.12 original and watermarked frame	61
3.13 Results after noise attacks	63
3.14 Results after filtering attacks	64
3.15 Results after histo gram and gamma correction attacks	65
3.16 Result after mean filtering	65
3.17 Result after median filtering	66
3.18 Result analysis after various attacks	67
3.19 Embedding algorithm using only DWT	68
3.20 Extraction algorithm using only DWT	69
3.21 Embedding algorithm using on DWT on host video frame and PCA on binary watermark	70
3.22 Extraction algorithm using on DWT on host video frame and PCA on binary watermark	71
3.23 Embedding Algorithm using both DWT and PCA on Host video frame and only PCA on binary watermark	72
3.24 Extraction Algorithm using both DWT and PCA on Host video frame and only PCA on binary watermark	73
3.25 Embedding Algorithm using only DWT on host video frame and only PCA on RGB watermark	75
3.26 Extraction algorithm using only DWT on host video frame and only PCA on RGB watermark	76
3.27 Embedding algorithm using both DWT and PCA on host video frame and only PCA on RGB watermark	77
3.28 Extraction algorithm using both DWT and PCA on host video frame and only PCA on RGB watermark	78
3.29 Video Frame used for color watermark Algorithm	79
3.30 Color Watermark used	80
3.31 Analysis between the Proposed technique in terms of NC and the other algorithms	83
3.32 Analysis between the Proposed technique in terms of bit error and the other techniques	83

LIST OF ABBREVIATIONS

A/D	Analog to Digital
ACF	AutoCorrelation Function
BER	Bit Error Rate
CD	Compact Disc
D/A	Digital to Analog
DCT	Discrete Cosine Transform
DWT	Discrete Wavelet Transform
DSP	Digital Signal Processing
EOF	Empirical Orthogonal Function
FFT	Fast Fourier Transform
FUV	Fraction of Unexplained Variance
HVS	Human Visual System
IDWT	Inverse Discrete Wavelet Transform
JPEG	Joint Photographic Experts Group
JND	Just Noticeable Difference
LSB	Least Significant Bit
MPEG	Moving Picture Experts Group
MSE	Mean Square Error
NC	Normalised Correlation
PCA	Principal Component Analysis
PN	Pseudo Noise
PSNR	Peak Signal to Noise Ratio
QF	Quality Factor
QIM	Quantization Index Modulation
SNR	Signal to Noise Ratio
STFT	Short Time Fourier Transform
VLSI	Very Large Scale Integrated Circuit
WT	Wavelet Transform

Abstract

In recent years, the advancement in the digital multimedia technologies has brought many facilities in reproduction, transmission and data manipulation. However this advancement has also brought the problem such as copyright issues. For copyright protection of digital multimedia, watermarking has been proposed. A watermark is embedded into the data which will indicate whether the content is copyrighted or not. Digital watermarking is a vast research area which is gradually growing. Over the years, researcher in Digital watermarking community has developed numerous new techniques for watermark embedding and detection. For the analysis of these techniques different attacks and counter-measures were being performed, encouraging for development of better techniques. Digital watermarking may be distinguished according to visibility (visible and invisible), robustness level (fragile, semi-fragile and robust), media type (audio, image, video) and the need for original data (blind, semi-blind, non-blind). The main scope of this thesis is to provide a good trade-off between the perceptual quality of the video after watermarking and the robustness of the video against various attacks. In the work, a method known as Arnold Cat Map is used to scramble the watermark image before embedding to provide some level of security to the watermarking algorithm. Watermark is embedded into the new sub space obtain from principle component analysis. Here in the thesis different semi-blind and non-blind techniques are performed. The methods were tested in Matlab and were analysed using Peak Signal to Noise Ratio (PSNR) and Normalised correlation for similarity measure. The satisfactory outcome of the technique can be seen in the watermarked video and the extracted watermark.

CHAPTER 1

Introduction

Introduction

Motivation

Watermarking Requirements

Classes of embedding Methods

Watermarking Attacks and Performance measurement

CHAPTER-1

1.1 INTRODUCTION

In recent years, there is a vast advancement in the field of digital multimedia technologies and has brought many advanced techniques in reproduction, transmission and data manipulation. Compared to the earlier analog counterpart this technology offers so many new advantages. Ease in editing of the digital content, ease of transmission of data, capability of copying digital data without any loss in the quality of the content and many other advantages in VLSI, DSP and communication applications have made the digital technology superior to the analog system. The growth of digital multimedia technology has been reflected on Internet and wireless applications. At the same time the distribution and use of digital multimedia data has been made much faster and easier with the great success of the Internet.

Watermarking [4] is an act of embedding an information bearing signal within a host data signal such as image, audio or video [1 2 3]. While some watermark is visible, most of the watermark [40] of interest are invisible. The embedding should be in such a way that, it does not overly distort the host signal and at the same time, the embedding should be robust to unintentional or malicious operations. An analysis for the need of watermarking and also some of its requirements and applications.

Figure 1.1. Gives an illustration of digital watermarking. The secret data (watermark) is embedded to the host multimedia by using a secret key at the coder(C). And it is transmitted through the transmission channel. Possible Attacks such as the geometric distortions, lossy compression, digital–analog and analog-digital conversion, any signal processing operations etc. At the receiver, the message is tried to extract from the watermarked multimedia. It is not possible to retrieve the message (watermark) without the knowledge of the key, only the owner who knows the secret key.

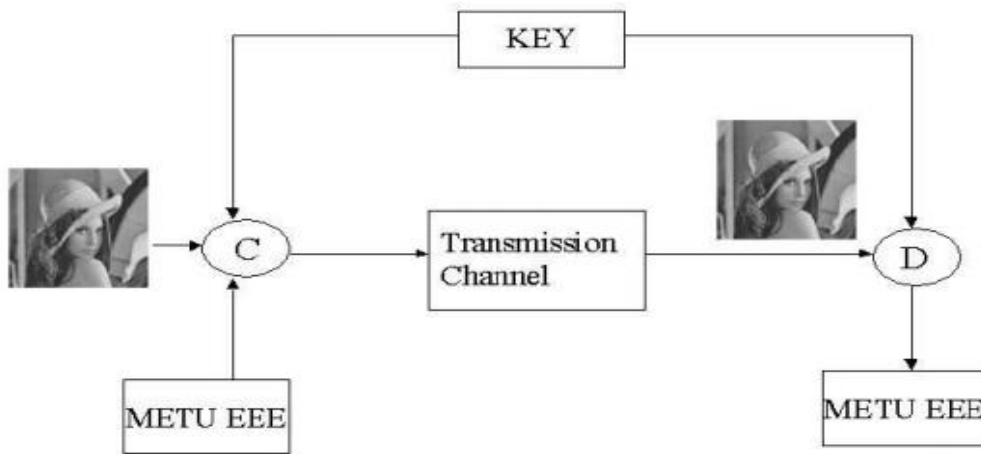


Figure.1.1. General Scheme watermarking

1.2 MOTIVATION

In the present digital world, the digital data has become massive popular due to the availability of inexpensive resources such as the computers, scanners, camcorder, cameras, software's and Internet. Now, it is possible to store and transmit digital media with high reliability. Modern signal processing tools has also made it possible to effortlessly modify and replicate digital media.

Some important application where the digital watermarking are used

1. Copyright protection: Associated with the widespread circulation of digital data arises the issues of copyright infringement. Digital watermarking is used for copyright protection, where the owner of the multimedia data embed a watermark in his data, the embedded watermark conveys the copyright and ownership information and can prove ownership in court.

Watermarking is used in conjunction with the encryption technique to provide an efficient copyright protection. Encryption [6 7] ensures that the multimedia data/ digital data is available only to the authorised users, or say the users who has the decryption key, which is vulnerable at some point in the system, since the data have to be decrypted to be used. Thus, in order to have some form of control by the owner

over their multimedia data, watermarking steps in i.e. digital watermarking can complement digital encryption.

2. Copy control: Digital watermarking can also be used in copy control system to enable or disable copying of multimedia data. Based on the information conveyed by the watermark, recording device may decide whether to allow or inhibit recording. Such a system has already been proposed for allowing a copy once features in digital video disc recorders [8] as well as in playback devices [9].
3. Fingerprinting: Digital watermarking can be used in fingerprinting where the owner of multimedia data embeds a unique information (watermark) to a particular copy/user of the work. Since the watermark is associated with a unique copy of the work it acts as a digital watermark. Which can be useful in tracing the source of illegal copies of the work. Further applications of fingerprinting is provided by cot et.al [5].
4. Broadcast monitoring: Digital watermarking can also be used in broadcast monitoring for keeping a control on the number of times an advertisement is aired in television by broadcasting television stations. In this, a watermark is embedded in the advertisement which is going to be aired and then an automated monitoring system is used to track the number of times the advertisement is aired. The information from the automated monitoring system can then be used by the advertisers for book keeping purposes.
5. Authentication: Digital watermarking can be used to ensure the authenticity or integrity of multimedia data in certain application such as legal cases and medical imaging. To indicate whether the data has been altered fragile watermarks [10] can be used. Fragile watermarks can also give information about the location of the host data that has undergone alterations. Robust watermarking to JPEG compression but not intentional tampering have been proposed [11 12].
6. Meta-data tagging: Meta-data describes or convey auxiliary information of the host multimedia data. Typical applications of meta-data are embedding information related to a patient in medical images or putting time stamp in photographs. Watermarking is a natural and effective way to transmit meta-data. A robust watermarking algorithm can guarantee to withstand tampering of the embedded data even after the host data undergoes alterations.
7. Error concealment in Images and Video: Robie and Mersereau [13] proposed a technique for error concealment, where the data or the information required for error correction is embedded as a watermark into the multimedia data and is transmitted to

the video decoder. The decoder then used this data along with some error concealment technique to remove channel errors.

The key element that distinguish digital watermarking from other multimedia security techniques such as forensics [42,43], steganography [45], biometrics, cryptographic hashing or perceptual hashing [45] and encryption is that in digital watermarking the content itself is purposefully altered to encode/embed additional information about the multimedia content.

1.3 Watermarking Requirements

The design of digital watermarking should in such a way that the embedded watermark are robust, secure and imperceptible. Usually, it involves a trade-off among the above requirements. A brief description of the algorithm requirements are as given below.

1. Imperceptibility: Applications involving multimedia data such as images, video and audio requires an unobtrusive watermark. The major requirement is that there should be perceptually indistinguishable between the watermarked data and the original data, in-order to preserve the perceptual quality at the same time the commercial value of the multimedia data. A method has been developed by Podilchuk and Zeng [14] to limit the changes made due to embedding in the host data below the threshold of perception by computing the Just Noticeable Differences (JND), rendering the watermark invisible. A research in perceptual watermarking is given in the paper by Vleshchouwer et.al [15].
2. Robustness: The ability of the watermark to withstand interference is referred to as robustness, the interference may be either advertently or inadvertently. The inadvertently interference may arise from processing of multimedia data such as compression, re-sampling, filtering, analog-to-digital (A/D) and digital-to-analog (D/A) conversions. Whereas advertently interference are put by knowledgeable attacker, who intentionally try to distort or completely destroy the watermark. Collusion and averaging attacks are some intentional attacks, where the attacker try to construct an unwatermarked data from several copies of watermarked data. The paper by voloshynovskiy et.al [16] gives a review on attacks modelling and countermeasures.

3. Payload: Depending on applications, the amount of watermarks or the information is embedded into the data. For finger-printing and data authentication only one bit of embedded information is required since it is only to verify whether a given watermark is present or not. For meta-data tagging and copyright protection more than one bit of watermark or information is required, some even suggested a minimum of 128 bits of information are needed for efficient copyright protection.
4. Oblivious and Non-Oblivious watermarking: Non-Oblivious watermarking refer to the case in which it is necessary to have the original (unwatermarked) data in order to extract the watermark, as in broadcast monitoring. It is also referred to as no blind watermarking or informed watermarking. Whereas if the watermark is extracted without the original data (unwatermarked) then it is referred to as blind watermarking or oblivious watermarking.

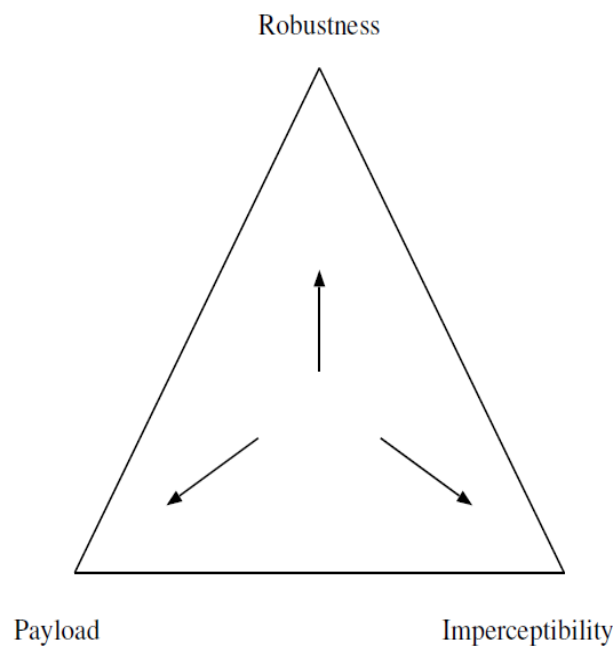


Figure.1.2. Figure illustrating the relationship between Robustness, Imperceptibility and Payload.

Figure shows the relationships between payload, imperceptibility and robustness. It is clear from the figure that in the design of watermarking algorithm it is difficult to simultaneously meet this conflicting requirements and it involves a trade-off between these requirements.

1.4 Classes of Embedding Methods

1.4.1 Modulation based Watermarking Algorithms

These are highly popular algorithms and are also referred to as spread spectrum methods [17]. The information to be embedded is modulated with a predefined signal to form the watermark. The signal used to modulate the watermark information is called the modulation signal and it is usually generated using a secret key. Figure 1.2 illustrates the typical modulation based watermarking. A channel is being shared by the image as well as the attacks. The information is extracted from the signal at the output of the channel. The function of secret key is to separate potential users by assigning a unique key to each user and to maintain secrecy. The method is as follows

$$I' = W + I \quad (1.1)$$

Where I' is the watermarked signal, W is the watermark and I is the unwatermarked signal. The algorithm proposed by Bender et.al [23], Cox et.al [17], Tirkel et.al [18] and Smith and Comiskey [22] belongs to additive class of embedding functions.

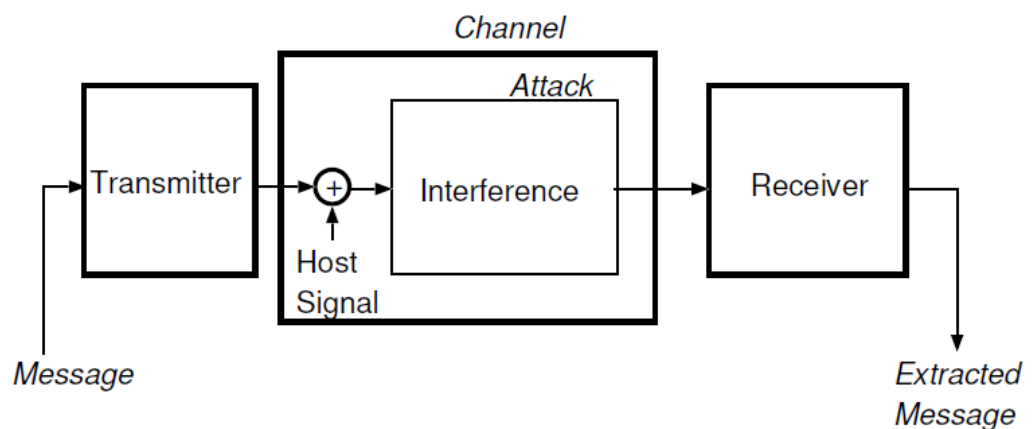


Figure.1.3. Block diagram of typical modulation based watermarking system

A number of modulation based methods have been proposed. A non-oblivious watermarking algorithm has been proposed by Cot et.al [17]. A method that exploits the human perceptual system to embed watermarks more efficiently has been proposed by Podilchuk and Zeng [19]. Many authors including Hosinger and Rabbani [20] and Hernandez et.al [21].

Watermark can also be embedded in transform domain such as discrete cosine transform and discrete wavelet transform [24, 25, 26]. In transform domain embedding a statistical description of the transform coefficient of multimedia is available, which is exploited to design optimal watermark detector for discrete cosine transform (DCT) domain watermarking.

1.4.2 Watermarking with side information

This type of approach have been first proposed by Chen and Wornell [28 29 30] and Cox et.al[27] , in this blind watermarking is treated as communication with side information at the transmitter. Figure 1.3 shows the block diagram of such system. Costa [31] shows figure1.3 is independent of the interference under certain conditions by deriving an expression for the capacity of the communication system/channel with a known source of interference. Chen and Wornell [28 29 30 32 33] proposed an algorithm by extending the Costa’s result and they call it Quantization Index Modulation (QIM). A number of schemes have been proposed based on Costa’s result by Miller et.al [36] and Eggers and Girod [34 35].

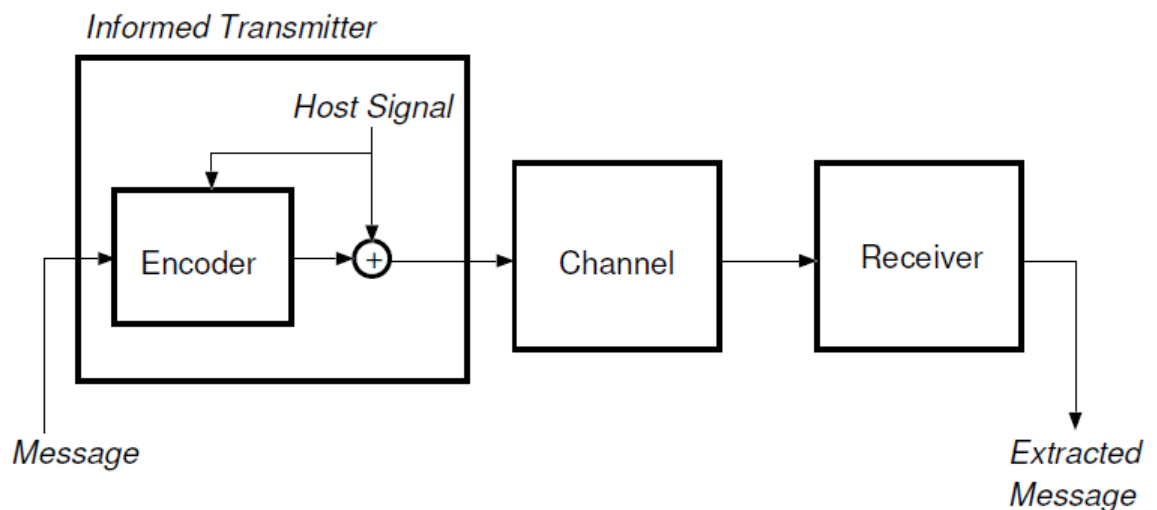


Figure.1.4. Block diagram of watermarking system that uses side information during embedding process.

In the Quantization Index Modulation the information is embedded into the multimedia host through the choice of quantizer. To embed ‘0’ the host is quantized by the quantizer P while it is quantized by the quantizer Q to embed ‘1’. Figure 1.4 shows binary dither modulation.

The quantizer is dithered pseudo randomly with a dither sequence which is known only to the encoder and decoder and provides the security needed for watermarking applications. At the receiver side the signal received is quantized to the nearest point of reconstruction on the set $\{P \cup Q\}$. A point belonging to P indicates that '0' was hidden while a point belonging to Q indicates that '1' was hidden. The distortion introduced in the embedding is only by the noise introduced by the quantization process. In order to obtain better rate-distortion trade-offs Multidimensional lattice are used.

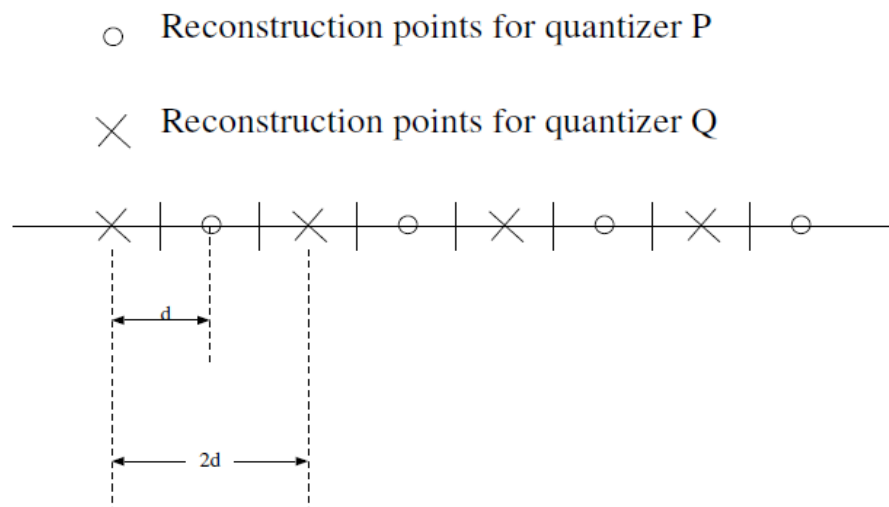


Figure.1.5. Quantization Index Modulation system (QIM).

1.4.3 Game Theoretic Watermarking

This approach has been proposed by Eggers and Girod [38] and by Moulin and O'Sullivan [37]. In this, watermarking is being viewed as a game between the embedder and the attacker. Where the embedder tries to maximize the amount of information conveyed by the watermark which has been embedded while the attacker tries to minimize it. Moulin et.al [39] and su et.al [38] brought some interesting extension to the above result.

1.5 Watermarking Attacks and Performance Measurements.

Attack is any signal processing that weakens the detection of the embedded watermark or the information conveyed by the watermark. Watermarking attacks aims at diminishing the

watermarking algorithm. The main aim of watermarking algorithm is to provide some security and the aim of attacks is to nullify that purpose. The processed watermarked data after attacks is known as attacked watermarked data. The research on watermarking algorithm enables us to

- Determine the flaws of a watermarking algorithm
- Introduce an improved watermarking algorithm
- Analyse the effects of current technology in watermarks

Watermarking may be thought of as a communication problem, in which the owner of the multimedia data tries to communicate through a hostile channel where there is intentional and non-intentional attacks from the channel. It can also be thought as a game played between the owner and attacker, where the owner tries to communicate as much watermark information as possible at the same time maintaining high data quality, whereas, on the contrary, the attacker tries to impair the watermark information without impairing the data quality. So the more the researcher know about the possible attacks the better they can design a watermarking system that can resist the attacks.

1.5.1 Classification of Attacks.

Watermarking attacks can be broadly classified into malicious (intentional) and non-malicious (unintentional). Unintentional attacks usually occur from common signal processing operations for example compression of a multimedia content which has watermark in it. It usually occurs when legitimate users performed some signal processing in the obtained watermarked multimedia. The malicious attacks are performed by an attacker who tries to destroy the watermark information embedded in the watermarked multimedia so that it can be prevented from tracing of illegal copies of the watermarked multimedia.

Malicious attacks

The sole reason of this attacks is to remove watermark intentionally or the attacker makes the watermark unrecoverable. Malicious attacks are further classified into two classes.

Blind watermarking attacks

In this kind of attacks, the attacker without exploiting the knowledge of the particular algorithm tries to remove the watermark or make the watermark unrecoverable. One example

of this attack is the copy attack where the attacker tries to estimate the watermark information with the intent to copy it to another asset.

Informed watermarking attacks

In this, the attacker exploits the knowledge of the particular watermarking algorithm and then tries to remove the watermark or even make it unrecoverable. The attacker first tries to obtain some secret information of the watermarking algorithm for some publicly data and then tries to nullify the watermarking algorithm.

Some few examples of malicious attacks

- Printing and Rescanning
- Re-watermarking
- Collusion: where a number of authorised recipients of the multimedia tries to generate an unwatermarked multimedia by taking the average of all the watermarked content.
- Forgery: In this, a number of authorised recipients try to form a copy of watermarked content with the valid watermark embedded of someone else with the intention of framing 3rd party.
- IBM attack [41]: Attacks which is able to produce fake originals and which is as good as the original one, and can be used to extract the watermark for claiming ownership by the holder of the fake original.

Malicious attacks can be further classified into

Removal attacks

This type of attacks aims at complete removal of the watermark which cracking the security or without exploiting the knowledge of watermarking algorithm. Which means that no processing, even if its prohibitively complex can recover the watermark form the attacked watermarked data. This category of attacks includes quantization (for example compression), denoising, collusion attacks and re-modulation. It does not mean that all of the above mention methods remove the watermark information but they nevertheless damage the watermark significantly. Attackers now try to optimize operations like quantization and denoising to remove the watermark information as much as possible keeping the quality of the attacked watermarked data as high enough. Collusion attacks is performed when a number of copies of a multimedia each signed with different watermark are obtain by the attacker or group of

attackers by averaging all the differently watermarked multimedia copies or by taking only a small part of the each of the watermarked multimedia. Survey shows that only a small number of copies about 10 are sufficient to successfully remove watermark.

Geometric attacks

A variation from the removal attacks is the geometric attacks, geometric attacks does not actually remove the watermark information but intend to distort the synchronization with the embedded watermark in the watermark detector. As a result the detector could recover the watermark information only when the perfect is synchronization is achieved which is practically highly complex. Benchmarking tools such as Unzign and Stirmark have a variety of geometric attacks for image watermarking. Local pixel jittering has been introduce by Unzign which is very efficient in attacking watermarking schemes in spatial domain. Local and global geometric distortion has also been introduced in Stirmark. However, due to use of special synchronization techniques most of the watermarking schemes survive these attacks. For global geometric attacks, the robustness of a watermarking scheme relies on the use of either additional template, transform invariant domain (for e.g Fourier-Melline) or by designing periodic watermark through which we can estimate the geometric distortion from it autocorrelation function (ACF). Resistance to global affine transformation is more or less a solved issue. However robustness to random alterations in Stirmark is still an open problem. Recent watermarking schemes are able to resist the random bending attacks which is integrated in Stirmark. Random bending attacks exploits the fact that Human visual systems (HVS) are not very sensitive to local shifts and affine modifications. Hence the pixels are locally scaled, shifted and rotated without significant visual distortion.

Cryptographic attacks

Cryptographic attacks aims to remove the watermark information or to add misleading information in the already watermarked data by cracking the security of the watermarking algorithm. Brute-force search technique is one such attack which tries to search for the embedded watermark information. Another category of such attacks is the oracle attack which tries to create a non-watermarked data when the detector is available. But due to its high computational complexity practical applications of such attacks is restricted.

Protocol attacks

Protocol attacks aims at dismantling the entire concept of the watermarking scheme. Invertible watermark is one type of protocol attacks, where the attackers subtract its own watermark from the watermarked data from claiming its ownership illegally. For that reason watermarking for copyright application watermarks needs to be non-invertible, which implies that one cannot extract watermark from a non-watermarked data. One solution for this problem is to use one-way functions in order to make the watermark signal dependent. Another such type of attack is the copy attack which aims to estimate a watermark from a watermarked data and copy it to some out document called the target data without removing the watermark or impairing its detection. To obtain imperceptibility the estimated watermark is adapted to the local features of the target data. The copy attack is successful only when a valid watermark is generated in the target data without exploiting the watermarking algorithm or the watermarking key of the already watermarked data. Robustness to copy attacks can be obtain by using signal-dependent watermarks.

Non-malicious attacks

Non-malicious attacks results mainly due to common signal processing operations or it also results from normal operations such as storage, transmission etc. Depending on the application where the watermarking systems are used, the nature and strength of such attacks may vary.

Examples of non-malicious attacks

Lossy Compression

This kind of attacks occurs in multimedia applications. When multimedia such as audio, video and image are being compressed and are being distributed via internet. Compression techniques such as JPEG and MPEG can degrade the quality of the multimedia such that the watermark becomes irretrievable. In order to resist compression, it is advised to insert the watermark in the same domain where the compression takes place.

Geometric Distortion

Geometric Distortion occurs in video and images. It occurs when the authorised recipient perform operations on the watermarked content. Common operations are cropping or scaling, rotation and translation.

Common signal processing operation

Attacks which results from common signal operations such as linear filtering(high pass and loss pass), non-linear filtering such as the median filtering, A/D conversion, D/A conversion, re-quantization, re-sampling, addition of constant offset to the pixel values, contrast adjustment, dithering distortion, addition of noise (Gaussian and non-Gaussian), gamma correction.

So the attacks can be classified into four classes of attacks: removal attacks, cryptographic attacks, geometric attacks, and protocol attacks.

1.5.2 Performance Measures Of Watermarking Algorithms

The watermarking algorithm is evaluated based on a number of measures. Not all the measures are appropriate for a given application because of the psychological nature of problem. Some most popular metrics are discuss, with the assumption that the host and watermarked signal are images.

Perceptual quality

Perceptual quality refers to the imperceptibility of the watermarked data after the watermark has been embedded into it. Efficient watermarking is complete only when the watermarking scheme didn't bring much change in perception of the human eye after the host data has been watermarked. For Invisible watermark it is important that the watermark is imperceptible. Peak signal to noise ratio (PSNR) of the watermarked data with the host data is used for quality measure to ensure that the quality of the host data is not perceivably distorted.

$$\text{PSNR} = 10\log_{10}\left(\frac{255 \times 255}{\text{MSE}}\right) \quad (1.2)$$

$$\text{MSE} = \frac{1}{MN} \sum_{j=1}^M \sum_{j=1}^M (X(m, n) - X_w(m, n))^2 \quad (1.3)$$

Where X is the host signal, X_w is the watermarked signal and MN is the total number of pixels in X and X_w . Unit is in dB.

Correlation coefficients

The correlation coefficients are used to measure the similarity between the extracted watermark and the original watermark and is defined as

$$NC = \frac{\sum_i \sum_j w(i,j)w'(i,j)}{\sqrt{\sum_i \sum_j W(i,j) \sum_i \sum_j W(i,j)}} \quad (1.4)$$

Where w and \hat{w} is the original and the extracted watermark

Bit Error Rate

Bit rate is the measure of the amount of watermark data/information that may be embedded within a host signal per unit space or time. Units of bit rate are bits per second or bits per pixel. Bit rate varies for different applications, usually for copyright protection higher bit rate is preferred so that more number of watermark information can be embedded. Reliability of a watermarking scheme is usually messed in terms of bit error rate. The bit error rate for a sequence of length B bits of the embedded and extracted watermark is given by

$$BER = \frac{100}{B} \sum_{n=0}^{B-1} \begin{cases} 1 & \hat{w}(n) \neq w(n) \\ 0 & \hat{w}(n) = w(n) \end{cases} \quad (1.5)$$

Computational Complexity

This refers to the complexity of the watermarking algorithm to embed the watermark into the host signal and to extract the watermark from it. For choice of DSP architecture or implementation structure it is necessary to know the watermarking algorithm complexity. To measure algorithm complexity there are many ways such as the 'Big-0' analysis. For practical applications more quantitative values are required.

CHAPTER 2

LITERATURE REVIEW

Wavelet Transform

Wavelet Transform in Two Dimensions

Wavelet Families

Haar Wavelet Transform

Principal Component Analysis

Arnold Cat Map

CHAPTER-2

LITERATURE REVIEW

2.1 Wavelet Transform

Wavelets are a set of non-linear bases. There are many different wavelet basis functions, according to the function to be approximated i.e. to project a function in terms of wavelet, the wavelet basis function is chosen. Wavelets uses a dynamic set of basis function to project the function in the most efficient way unlike the linear bases which uses a static set of basis function. WT gives a new way of describing nature and makes it possible to mathematically formulate scientific problems. It has no doubt brought a lot of possibilities into the science. Wavelet analysis generally arose from Short Time Fourier Transform (STFT) by varying the time-window. The plus point of wavelet transform is that it can be used to analyse the signal both in time and frequency domain. By shifting the wavelet along the time axis analysis in time domain done, while for frequency analysis the wavelet is scaled. Wavelet is used for representation of a signal in Time-frequency domain. This representation gives a better view of different frequency component of the signal. For analysing a signal, Wavelet Transform not only transforms a signal from time domain to frequency domain, but preserves the spatial information in the transform, which helps in enhancement of image quality for low bit rate representation.

This dual time-frequency approach for signal analysis has found plenty of ways for real time applications. Typical ways of Wavelet transform utilization mainly belongs to signal processing such as i) Trend detection, ii) detection of signal discontinuities, iii) particular frequency detection, iv) Signal denoising, v) detection of self-similarities, vi) data compression and vii) signal suppression, although application of Wavelet transform are not limited to them at all. There are several kinds of wavelet functions each possessing different desired and useful properties.

A fundamental form of wavelet transform is the discrete wavelet transform has been built on a Hilbert space of complex sequence of N-dimensional vectors and defined on $\ell^2(Z_N)$. The simplicity of this form lies in the finite dimension of space $\ell^2(Z_N)$ Next form is defined on $\ell^2(Z)$ which has a Hilbert space of infinite and which is generally not periodic ,complex signal. The difference of this form with the earlier one is its infinite dimensionality, making

the theory more demanding. The third form of wavelet transform is the continuous wavelet transform which is a Hilbert space of complex square-integrable functions and is defined on $\ell^2(\mathbb{R})$. In this form the construction of wavelets is usually reduced to the construction of Multi resolution Analysis.

The main concept of discrete wavelet transform is to decompose the original Hilbert space $\ell^2(\mathbb{Z}_N)$ into two subspaces, namely the space of approximation v and the space of details ω , which is known as 1st level analysis. The space of approximation is closed and has countable basis so it can be separated and can be decomposed further. This decomposition in general is known as the p^{th} level analysis. If v_j and ω_j denotes the j^{th} level space of approximation and the space of details. Then we can write as

$$\begin{aligned} \ell^2(\mathbb{Z}_N) &= v_1 \oplus \omega_1 \\ v_1 &= v_2 \oplus \omega_2 \\ &\cdot \\ &\cdot \\ v_{p-1} &= v_p \oplus \omega_p \end{aligned} \tag{2.1}$$

or more compact form

$$\ell^2(\mathbb{Z}_N) = v_p \oplus \omega_p \oplus \omega_{p-1} \oplus \dots \oplus \omega_1 \tag{2.2}$$

the subspace v_j, ω_j have the same dimension $N/2^j$ for some j . where N is to be divisible by 2^p where p is the maximum level of analysis.

2.1.1 Continuous Wavelet Transform

It is required to use time-frequency atoms having different time supports, in order to analyse signals having different sizes. In wavelet transform the signal is decomposed over dilated/scaled and translated functions called the wavelets, as a result it transforms a continuous function into highly redundant function. Some examples of continuous wavelet transform are shown in the next section.

A wavelet is a function of zero average

$$\int_{-\infty}^{+\infty} \Phi(t) dt = 0 \quad (2.3)$$

Which is normalised $\|\Phi(t)\|=1$ and is centered at $t=0$. A time- frequency atoms is obtained by scaling $\Phi(t)$ by s and translating by μ .

$$\Phi_{\mu,s}(t) = \frac{1}{\sqrt{s}} \Phi\left(\frac{t-\mu}{s}\right) \quad (2.4)$$

The wavelet transform of $f \in L^2(\mathbb{R})$ at time μ and scale s can now be written as

$$W\{f(\mu, s)\} = \langle f, \Phi_{\mu,s} \rangle = \int_{-\infty}^{+\infty} f(t) \frac{1}{\sqrt{s}} \Phi^*\left(\frac{t-\mu}{s}\right) dt \quad (2.5)$$

We can now define a variable C_Φ , which is given as

$$C_\Phi = \int_0^{+\infty} \frac{|\widehat{\Phi}(\omega)|^2}{\omega} d\omega \quad (2.6)$$

If $C_\Phi < +\infty$, is satisfied then any $f \in L^2(\mathbb{R})$ has its inverse wavelet transform, which is called the wavelet admissibility condition

$$f(t) = \frac{1}{C_\Phi} \int_0^{+\infty} \int_{-\infty}^{+\infty} W\{f(\mu, s)\} \frac{1}{\sqrt{s}} \Phi\left(\frac{t-\mu}{s}\right) du \frac{ds}{s^2} \quad (2.7)$$

it is necessary that $\widehat{\Phi}(0) = 0$ in order to guarantee that the integral of C_Φ is finite scaling function

To recover f when $W\{f(\mu, s)\}$ is known only for $s < s_0$ we need to complement information of $W\{f(\mu, s)\}$ for $s > s_0$ which is obtained by scaling function Φ , and can be defined as

$$|\widehat{\Phi}(\omega)|^2 = \int_1^{+\infty} |\widehat{\Phi}(s\omega)|^2 \frac{ds}{s} = \int_\omega^{+\infty} \frac{|\widehat{\Phi}(\zeta)|^2}{\zeta} d\zeta \quad (2.8)$$

Which can be verified that $\|\Phi\| = 1$ and from admissibility condition we can derive that

$$\lim_{\omega \rightarrow 0} |\widehat{\Phi}(\omega)|^2 = C_\Phi \quad (2.9)$$

Thus, the scaling function can be taken as impulse response of the low pass filter and the low-frequency approximation of f scaled at s can be written as

$$L\{f(\mu, s)\} = \langle f, \Phi_{\mu,s} \rangle = \int_{-\infty}^{+\infty} f(t) \frac{1}{\sqrt{s}} \Phi^*\left(\frac{t-\mu}{s}\right) dt \quad (2.10)$$

And the inverse wavelet transform can be written as

$$f(t) = \frac{1}{c_\Phi} \int_0^{s_0} w\{f(\cdot, s)\} * \Phi_{\mu, s}(t) \frac{ds}{s^2} + \frac{1}{c_{\Phi s_0}} L\{f(\cdot, s)\} * \Phi_{\mu, s}(t) \quad (2.11)$$

Heisenberg boxes of wavelet atoms

Analytic wavelet is used to analyse time evolution of frequency tones in order to separate the phase and amplitude information of the signal. A function can be analytic only when its Fourier transform for negative frequency is zero.

$$\hat{f}_a(\omega) = 0 \quad \omega < 0 \quad (2.12)$$

Fourier transform can be decompose as a sum of analytic function

$$\hat{f}_a(\omega) = \frac{\hat{f}_a(\omega) - \hat{f}_a^*(-\omega)}{2} \quad (2.13)$$

Which can be inverted as

$$\hat{f}_a(\omega) = \begin{cases} 2\hat{f}(\omega) & \text{if } \omega \geq 0 \\ 0 & \text{if } \omega < 0 \end{cases} \quad (2.14)$$

The analytic part $f_a(\omega)$ of signal $f(t)$ which is the inverse fourier transform of $\hat{f}_a(\omega)$ and is called the pre-envelope of the signal $f(t)$. The time- frequency spread of the wavelet atoms $\Phi_{\mu, s}$ is responsible for the time-frequency resolution of the analytic wavelet transform. If Φ is centred at 0, then it implies that $\Phi_{\mu, s}$ is cantered at $t=\mu$. Changing variable $v = \frac{t-\mu}{s}$, it can be verified that

$$\int_{-\infty}^{+\infty} (t - \mu)^2 |\Phi_{\mu, s}(t)|^2 dt = s^2 \sigma_t^2 \quad (2.15)$$

Where $\sigma_t^2 = \int_{-\infty}^{+\infty} t^2 |\Phi(t)|^2 dt$. Since $\hat{\Phi}(\omega)$ is zero at negative frequencies, the centre frequency η of $\hat{\Phi}(\omega)$ is

$$\eta = \frac{1}{2\pi} \int_{-\infty}^{+\infty} \omega^2 |\hat{\Phi}(\omega)|^2 d\omega \quad (2.16)$$

It was found that the found that the Fourier transform of $\Phi_{\mu, s}$ is a dilation of $\hat{\Phi}(\omega)$ by $\frac{1}{s}$

$$\widehat{\Phi}_{\mu, s}(\omega) = \sqrt{s} \hat{\Phi}(s\omega) \exp(-i\omega\mu) \quad (2.17)$$

The centre frequency is therefore $\frac{\eta}{s}$ and the spread around $\frac{\eta}{s}$ is

$$\frac{1}{2\pi} \int_0^{+\infty} (\omega - \frac{\eta}{s})^2 |\widehat{\Phi}_{\mu,s}(\omega)|^2 d\omega = \frac{\sigma_\omega^2}{s^2} \quad (2.18)$$

With

$$\sigma_\omega^2 = \frac{1}{2\pi} \int_0^{+\infty} (\omega - \eta)^2 |\widehat{\Phi}(\omega)|^2 d\omega \quad (2.19)$$

Figure show the Heisenberg box centered at $(\mu, \frac{\eta}{s})$ of size $s\sigma_t$ along time and $\frac{\sigma_\omega}{s}$ along frequency which corresponds to the energy spread of a wavelet time-frequency atom $\Phi_{\mu,s}$

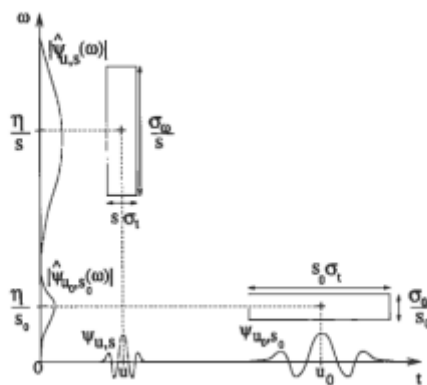


Figure.2.1. Heisenberg boxes of two wavelets. Smaller scales decrease the time spread but increase the frequency support and vice versa.

From the figure it is seen that the area of box remains $\sigma_t \sigma_\omega$ and the resolution of the time and frequency is depending on s , which is different from the Heisenberg box of windowed Fourier transform.

2.1.2 Discrete Wavelet Transform

In Discrete Wavelet Transform, different frequencies can be analysed by different resolutions thus Discrete Wavelet Transform is a multi-resolution technique. Applying Discrete Wavelet

transform to a signal resembles the process of applying fast Fourier transform to a set of sample signals. The main difference is that the Fourier transform decomposes the signal into cosines and sines, which means that the functions localized in Fourier space, whereas the Wavelet Transform uses functions that are localized in both the real and Fourier space.

If we uniformly sample a function $f(t)$ at an intervals N^{-1} over $[0,1]$. By changing of variable, the wavelet transform of $f(t)$ is

$$W\{f(\mu, s)\} = N^{-\frac{1}{2}}W\{f(N\mu, Ns)\} \quad (2.20)$$

The discrete wavelet transform is computed at scales $s=a^j$. By choosing $a=\frac{1}{2}$, we can define a discrete wavelet set $\{\Phi_{j,k}(x)\}$ where

$$\Phi_{j,k}(x) = 2^{\frac{j}{2}}\Phi(2^j x - k) \quad (2.21)$$

For all $j, k \in Z$ and $\Phi(\omega) \in L^2(\mathbb{R})$. the scaling function can be also written as

$$\Phi_{j,k}(x) = 2^{\frac{j}{2}}\Phi(2^j x - k) \quad (2.22)$$

Here, k determines the position of Basic wavelets and their properties $\Phi_{j,k}(x)$ and $\phi_{j,k}(x)$ along the x -axis and $2^{\frac{j}{2}}$ controls their height/amplitude. Figures below show some example of scaling and wavelet functions

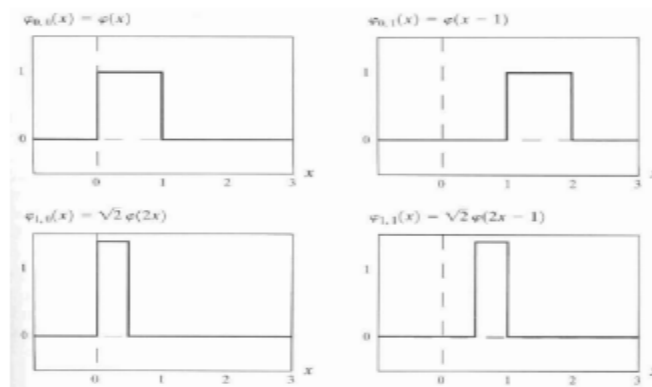


Figure.2.2 Haar scaling function in V_0 and V_1

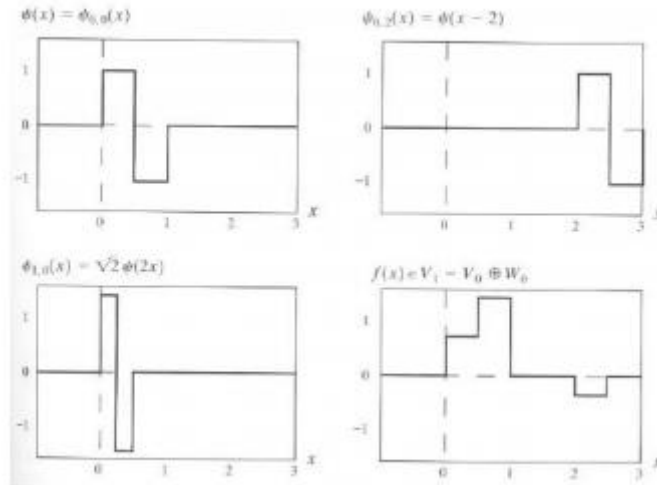


Figure.2.3. Haar wavelet functions in W_0 and W_1

General, subspace spanned over k for any j is denoted as

$$V_j = \overline{\text{span}\{\phi_{j,k}(x)\}} \quad (2.23)$$

For finer details the size of V_j is increased by increasing j . There are four fundamental requirements of multi resolution analysis that scaling function and wavelet function must follow:

- The scaling function is orthogonal to its integer translates.
- The subspaces spanned by the scaling function at low resolutions are contained within those spanned at higher resolutions.

$$V_{-\infty} \subset \dots \subset V_{-1} \subset V_0 \subset V_1 \subset V_2 \subset \dots \subset V_{+\infty}$$

- The only function that is common to all V_j is $f(x) = 0$. That is

$$V_{-\infty} = \{0\} \quad (2.24)$$

- Any function can be represented with arbitrary precision. As the level of the expansion function approaches infinity, the expansion function space V contains all the subspaces.

$$V_{+\infty} = \{L^2(\mathbb{R})\} \quad (2.25)$$

Under these condition the expansion functions of subspace V_j can be expressed as a weighted sum of the expansion functions of subspace V_{j+1}

$$V_{+\infty} = \{L^2(\mathbb{R})\} \quad (2.26)$$

$$\phi_{j,k}(x) = \sum_n a_n \phi_{j+1,k}(x) \quad (2.27)$$

Substituting for $\phi_{j+1,k}(x)$ and changing variable a_n to $h_\phi(n)$, this becomes

$$\phi(x) = \sum_n h_\phi(n) \sqrt{2} \phi(2x - n) \quad (2.28)$$

where $h_\phi(n)$ are called the scaling function coefficients and h_ϕ is known as scaling vector.

The subspace spanned by discrete wavelet is denoted as

$$V_j = \overline{\text{span}\{\phi_{j,k}(x)\}} \quad (2.29)$$

The discrete wavelet set $\phi_{j,k}(x)$ spans difference between any adjacent scaling subspaces V_j and V_{j+1} as shown in figure and is related by

$$V_2 = V_1 \oplus W_1 = V_0 \oplus W_0 \oplus W_1$$

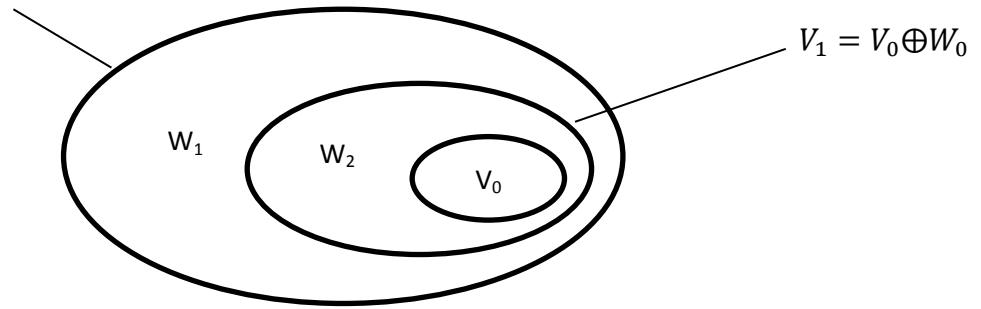


Figure.2.4. The relationship between scaling and wavelet function space

$$V_{j+1} = V_j \oplus W_j \quad (2.30)$$

Where \oplus denotes the union of spaces. The space of $L^2(\mathbb{R})$ can be expressed as

$$L^2(\mathbb{R}) = V_0 \oplus W_0 \oplus W_1 \oplus \dots \quad (2.31)$$

The equation can be extended as

$$L^2(\mathbb{R}) = \dots \oplus W_{-2} \oplus W_{-1} \oplus W_0 \oplus W_1 \oplus W_2 \oplus \dots \quad (2.32)$$

Which represents the function in terms of wavelet alone by eliminating the scaling function. If the function is an element of V_1 , an expression contains the approximation of $f(x)$ using V_0 and the difference between this approximation and the actual function is encoded by the wavelet from W_0 . Generally it starts from the arbitrary scale j_0 and can be written as

$$L^2(\mathbb{R}) = V_{j_0} \oplus W_{j_0} \oplus W_{j_0+1} \oplus \dots \quad (2.33)$$

Any wavelet function can be expressed as a weighted sum of shifted, double-resolution scaling functions and can be written as

$$\Phi(x) = \sum_n h_\phi(n) \sqrt{2} \phi(2x - n) \quad (2.34)$$

Where $h_\phi(n)$ are the called the wavelet function coefficients and h_ϕ is the wavelet vector. If the function results in the sequence of number, like the samples of a continuous function $f(x)$, the resulting coefficient are called the Discrete wavelet transform $f(x)$. After applying a principle of series expansion, the Discrete wavelet coefficients of $f(x)$ is defined as

$$W_\phi(j_0, k) = \frac{1}{\sqrt{M}} \sum_x f(x) \phi_{j_0, k}(x) \quad (2.35)$$

$$W_\phi(j_0, k) = \frac{1}{\sqrt{M}} \sum_x f(x) \phi_{j_0, k}(x) \quad (2.36)$$

For $j \geq j_0$ and the parameter M is the power of 2 which range from 0 to $J-1$. The function $f(x)$ can be expressed as

$$f(x) = \frac{1}{\sqrt{M}} \sum_k W_\phi(j_0, k) \phi_{j_0, k}(x) + \frac{1}{\sqrt{M}} \sum_{j=j_0}^{\infty} \sum_k W_\phi(j, k) \phi_{j, k}(x) \quad (2.37)$$

Where $\frac{1}{\sqrt{M}}$ as the normalizing factor.

2.2 Wavelet Transform in Two Dimensions

The two dimensional wavelet transform are widely used in image processing application and are slightly different from the one dimensional wavelet transform. Two dimensional wavelet are obtained by simply multiplying the scaling and the wavelet functions. For two dimensional wavelet transform, one two-dimensional scaling function $\phi(x,y)$ and three two dimensional wavelet functions $\phi^H(x, y)$, $\phi^V(x, y)$ and $\phi^D(x, y)$ are needed. The product of one dimensional scaling function Φ and corresponding wavelet ϕ is shown below

$$\Phi(x,y) = \Phi(x)\Phi(y) \quad (2.38)$$

$$\phi^H(x, y) = \phi(x)\phi(y) \quad (2.39)$$

$$\phi^V(x, y) = \phi(x)\phi(y) \quad (2.40)$$

$$\Phi^D(x, y) = \Phi(x)\Phi(y) \quad (2.41)$$

For image processing, these functions measure the variation of intensity for the image along different directions: Φ^V measure variations along rows, Φ^H measures variation along columns and Φ^D measure the variation along diagonals. The approximation which is as same as the one-dimensional one is given by the scaling function Φ . To convert from one-dimensional to two-dimensional is very straightforward if the scaling function and the wavelet function is given. The basis functions are defined as

$$\Phi_{j,m,n}(x, y) = 2^{\frac{j}{2}}\Phi(2^j x - m, 2^j y - n) \quad (2.42)$$

$$\Phi_{j,m,n}^i(x, y) = 2^{\frac{j}{2}}\Phi^i(2^j x - m, 2^j y - n), \quad i = \{H, V, D\} \quad (2.43)$$

Where the index I defines the direction of the wavelet functions. The discrete wavelet transform of function f(x,y) of size M×N is

$$W_{\Phi}(j_0, m, n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y)\Phi_{j_0,m,n}(x, y) \quad (2.44)$$

$$W_{\Phi}^i(j, m, n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y)\Phi_{j,m,n}^i(x, y) \quad i = \{H, V, D\} \quad (2.45)$$

$W_{\Phi}(j_0, m, n)$ gives the approximation of f(x,y) and j_0 is the arbitrary starting scale. The inverse wavelet transform is defined as

$$f(x, y) = \frac{1}{\sqrt{MN}} \sum_m \sum_n W_{\Phi}(j_0, m, n)\Phi_{j_0,m,n}(x, y) + \frac{1}{\sqrt{MN}} \sum_{i=H,V,D} \sum_{j=j_0}^{\infty} \sum_m \sum_n W_{\Phi}^i(j, m, n)\Phi_{j,m,n}^i(x, y) \quad (2.46)$$

An efficient way to implement discrete wavelet transform is the fast wavelet transform. The computational complexity can be reduced by finding the relationship between the coefficients at the adjacent scales. Considering the multi resolution refinement equation

$$\Phi(x) = \sum_n h_n(n)\sqrt{2}\Phi(2x - n) \quad (2.47)$$

By scaling of x by 2^j , translation of x by k units, and letting $m=2k+n$, we get

$$\phi(2^j x - k) = \sum_n h_\phi(n) \sqrt{2} \phi(2(2^j x - k) - n) \quad (2.48)$$

$$= \sum_m h_\phi(m - 2k) \sqrt{2} \phi(2^{j+1} x - m) \quad (2.49)$$

And similarly

$$\varphi(2^j x - k) = \sum_m h_\varphi(n) \sqrt{2} \varphi(2^{j+1} x - m) \quad (2.50)$$

Now considering the coefficients of discrete wavelet transform $W_\varphi(j, k)$. By changing variable we get

$$W_\varphi(j, k) = \frac{1}{\sqrt{M}} \sum_x f(x) 2^{\frac{j}{2}} \varphi(2^j x - k) \quad (2.51)$$

Which, upon replacing $\varphi(2^j x - k)$, it becomes

$$W_\varphi(j, k) = \frac{1}{\sqrt{M}} \sum_x f(x) 2^{\frac{j}{2}} [\sum_m h_\varphi(m - 2k) \sqrt{2} \varphi(2^{j+1} x - m)] \quad (2.52)$$

Rearranging the terms we get

$$W_\varphi(j, k) = \sum_m h_\varphi(m - 2k) [\frac{1}{\sqrt{M}} \sum_x f(x) 2^{\frac{(j+1)}{2}} \sqrt{2} \varphi(2^{j+1} x - m)] \quad (2.53)$$

Which can be written as

$$W_\varphi(j, k) = \sum_m h_\varphi(m - 2k) W_\varphi(j + 1, k) \quad (2.54)$$

Similarly, the approximation coefficients is written by

$$W_\phi(j, k) = \sum_m h_\phi(m - 2k) W_\phi(j + 1, k) \quad (2.55)$$

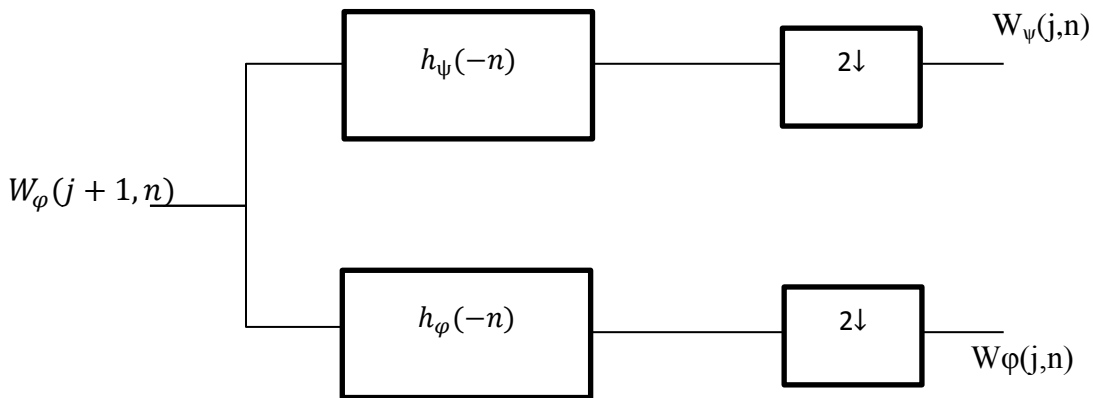


Figure.2.5. The inverse fast wavelet transform synthesis filter bank

$W_\psi(j, k)$ and $W_\phi(j, k)$ both can be found by convolving $W_\phi(j + 1, k)$ with time reverse scaling and wavelet vector $h_\psi(-n)$ and $h_\phi(-n)$ and then down sampling by 2. The construction of the fast wavelet transform is as shown in figure.

In inverse fast wavelet transform, $f(x)$ can be reconstructed by using the scaling and the wavelets employed in the fast wavelet transform. $j+1$ approximation coefficient is generated a little different to that of fast wavelet transform. The approximation and the detail coefficient of level j is first up sampled and then summing the results that were passed through scaling and wavelet vector $h_\psi(n)$ and $h_\phi(n)$ as shown in figure

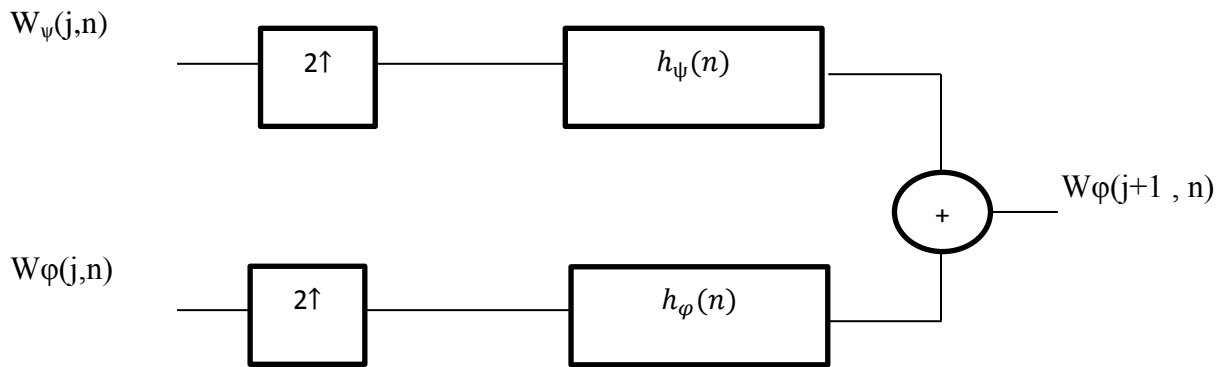


Figure.2.6. The fast wavelet analysis filter

Two dimensional fast wavelet transform can be obtained by simply taking one-dimensional fast wavelet transform of the rows of $f(x,y)$, followed by one-dimensional fast wavelet transform of the columns. The process is as shown in figure

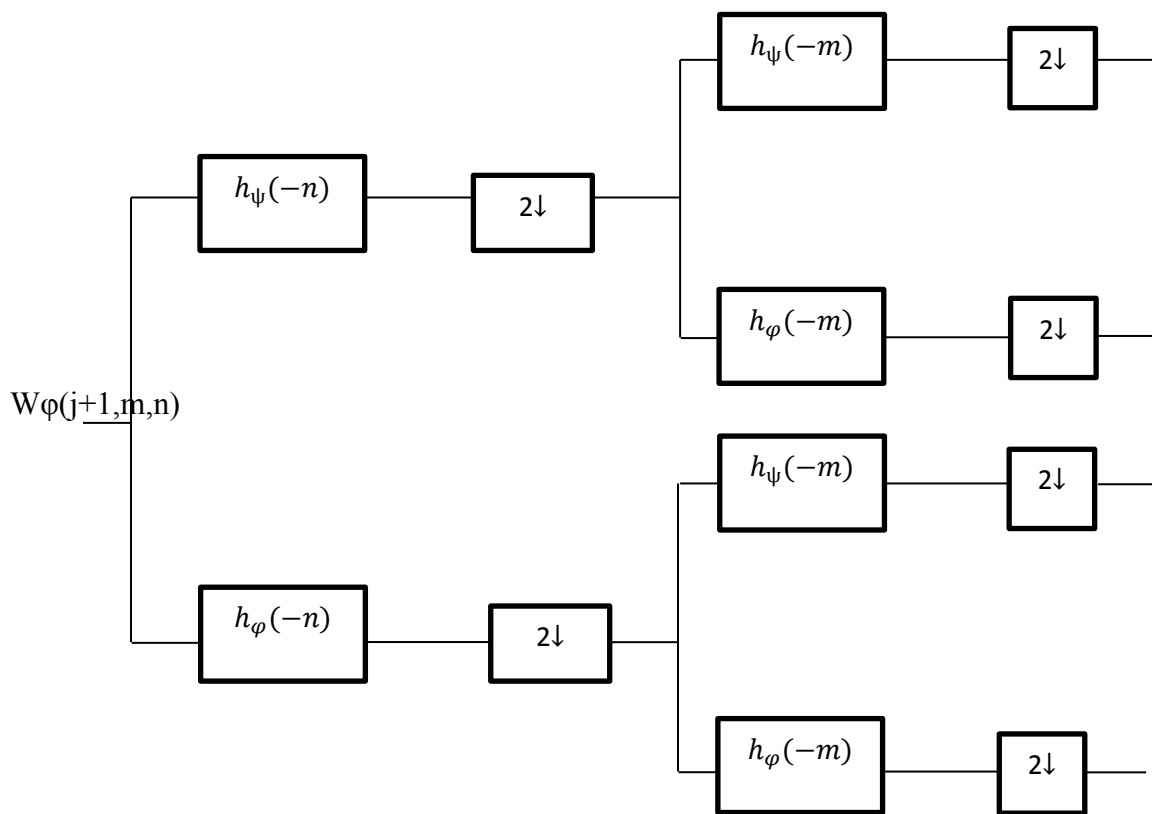


Figure.2.7. The two-dimensional analysis filter bank

As seen in figure, the two-dimensional fast wavelet transform is constructed of the detail and approximation part similar to the one-dimensional. Using two-dimensional fast wavelet transform in an image, we get four sub images as shown in figure, which are W_{φ} , W^H_{φ} , W^V_{φ} and W^D_{φ}

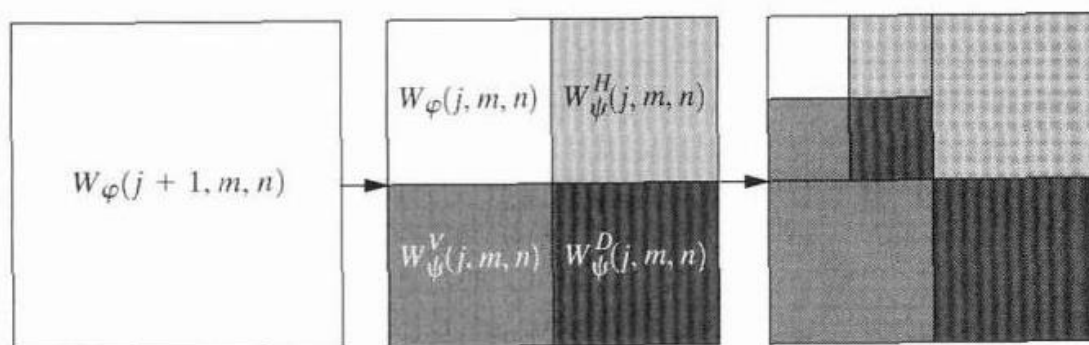


Figure.2.8. The resulting decomposition

Further the scale $j+1$ approximation coefficient can be divided into four smaller parts, which means that the $j+1$ approximation coefficients are constructed by the scale j approximation and detail coefficients. The inverse two-dimensional wavelet transform reconstruction

algorithm is as same as the one-dimensional. At each iteration four scale j approximation and detail coefficients are upsampled and convolved with two one-dimensional filters (one for the sub-images row and the other for the column) and adding the results from the filters we can get the $j+1$ approximation coefficients . The process is repeated to get the original image, as shown in figure

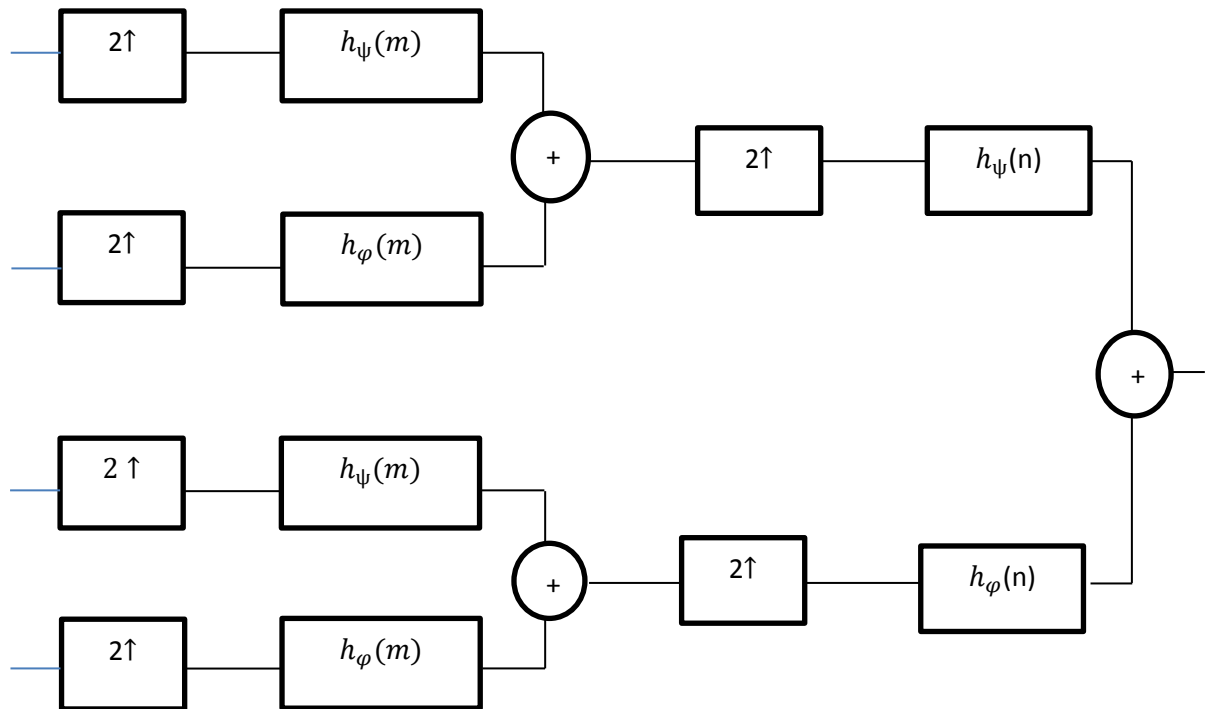


Figure.2.9. The two-dimensional inverse fast wavelet transform synthesis filter banks

A number of wavelet functions have been developed. More precisely, a number of method were developed each of them producing different set of wavelet functions which is usually specified by a parameter for example length of wavelet filter support. These sets are called wavelet families. The wavelet families are classified based on the based on their properties. Some of the wavelet parameters are

Wavelet filter support

Compact (finite) support is one of the most sought wavelet properties mainly because it results in a finite multiplication of the discrete wavelet transform which yields simple practical implementation of wavelet analysis. All the computations are exact as there is no

need to approximate wavelet function. Secondly it has a good time localisation of the wavelet.

Symmetry and Antisymmetry

Phase characteristic plays an important role since both scaling function and the mother wavelet is taken as a filter and the negative derivative is a group delay. In signal processing applications it is desired for the filter to have a linear phase, which means a constant group delay. For image restoration this issue is very crucial. the scaling function should be symmetric or antisymmetric for a linear phase wavelet filter.

Orthogonality

This property give some specific kind of exclusivity in signal analysis by guaranteeing the independence of wavelets in time. One example of orthogonal wavelet is symlets Daubechies et.al[1]. It is such a hurdle to design orthogonal wavelet which are symmetric to the degree possible since there is always a trade-off between orthogonality and symmetry of wavelets. Nonetheless it is also possible to exploit wavelets which are non-orthogonal which is built on Riesz's base but it is much complicated. Moreover there is always an error between the original signal and the reconstructed signal, which means that the wavelet synthesis is not perfect.

Number of vanishing moments

Moment functions are suppress by some wavelets, as a result polynomial functions of certain order are also suppressed as well. Which results in more sparse representation of the wavelet analysis and which in turn saves the memory space significantly while implementation. But there is a trade-off between the vanishing moments and the length of the wavelets.

Existing of scaling function

This property gives a simple rule that when the scaling function does not exist the wavelet analysis is not orthogonal. Which is rather theoretical as the orthogonality property of a wavelet is always known. So the rule does not much impact on the choice of wavelet family.

Expression for faster computation of the elements and the coefficients of wavelet analysis, explicit representation of wavelet is usually sought. But the explicit formulated wavelets have infinite support due to the exponential function in the expression, so the wavelets are not well

localised in time. Two of the wavelet families which does not have infinite support but a explicit wavelet are Haar wavelet and B-spline wavelets.

Time-frequency localisation

To detect particular phenomena in corresponding domain a good localisation of the wavelet both in time and frequency is required. However because of uncertainty principle there is a trade-off between the compact support and the band-limitation property. If we restrict more in frequency which means larger support of wavelet , than worst time resolution occurs.

2.3 Wavelet families

It is required to choose wavelet families according to the applications. Different application requires different properties of the wavelet. It is not reasonable to pick a wavelet and used it for all applications expecting a good result. An overview of wavelet families are given in the following

Orthogonal wavelets

The property of orthogonality has already been discussed in the earlier section. It is important to know that orthogonality is an presumption in wavelet theory. Possibility for perfect reconstruction is made possible by orthogonal wavelets as well as the possibility of orthogonal multi resolution analysis. By using orthogonal wavelets, the signal energy is preserved both time and frequency domain due to parseval's theorem. To top the most orthogonal wavelet have compact support which makes the most sought wavelets in DWT.

Daubechies wavelet

Mathematician Ingrid Daubechies gives this wavelet family and it usually denoted by dbN, where N is the order. The wavelet properties is usually determined by order N. The wavelet of dbN has N vanishing moments and has the support of length of 2N. This wavelet family is not symmetric and do not possess an explicit expression. A special case of daubechies wavelet is Haar wavelet and it occurs at N=1. The Haar wavelet is the simplest wavelet and it resembles a step function. It has an excellent time localisation which comes at the expense of resolution in frequency.

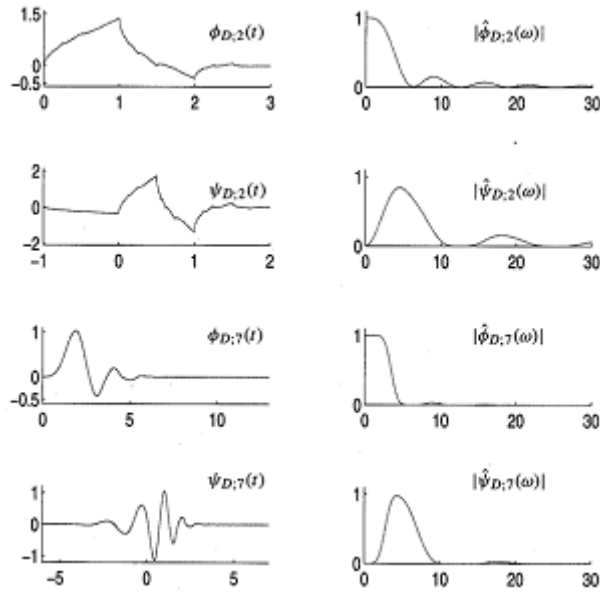


Figure.2.10. Daubechies scaling factor and their corresponding wavelets and magnitude spectra

Symlet wavelet

This wavelet family is also developed by Ingrid Daubechies. The main advantage of this wavelet is that it is more symmetric than the Daubechies. This wavelet is denoted by symN and has the same property as the dbN, where the 2N is the support length and the N is the vanishing moments.

Coiflet wavelet

This wavelet family is also developed by Ingrid Daubechies at the request of Ronald Coifman. And it is denoted by coifN and have 6N-1 length and 2N(mother wavelet) and 2N-1 (father wavelet) vanishing moments. Which means that Coiflet have less number of vanishing moments than the Daubechies and Symlet wavelets.



Figure.2.11. Coiflet with two vanishing moments

Crude wavelets

Crude wavelet usually has explicit expression therefore they have infinite support as well as it results in very smooth representation. It has good localisation in frequency as it uses explicit expressions. Crude wavelets are used continuous wavelet transform. Although it possible to obtain a discrete-time approximation by evaluating the explicit formula in equispaced points in time, it cannot be used in discrete wavelet transform as the crude wavelet are not orthogonal.

Shannon wavelets

Shannon wavelets are the dual wavelet of Haar and is defined by a rectangular bandpass filter in the frequency domain, as a result of which it has a perfect resolution and localisation in frequency. On the other hand it has a very poor localisation in time as it leads to sinc function in time domain. This wavelets are indefinitely differentiable and has a infinite number of vanishing moments and there integer shifts are orthogonal to each other. Shanaon wavelets is defined as

$$\Phi(t) = \text{sinc}(t/2)\cos(3\pi t/2) \quad (2.56)$$

$$\hat{\Phi}(f) = \begin{cases} 1 & 0.5 \leq |f| \leq 1 \\ 0 & \text{otherwise} \end{cases} \quad (2.57)$$

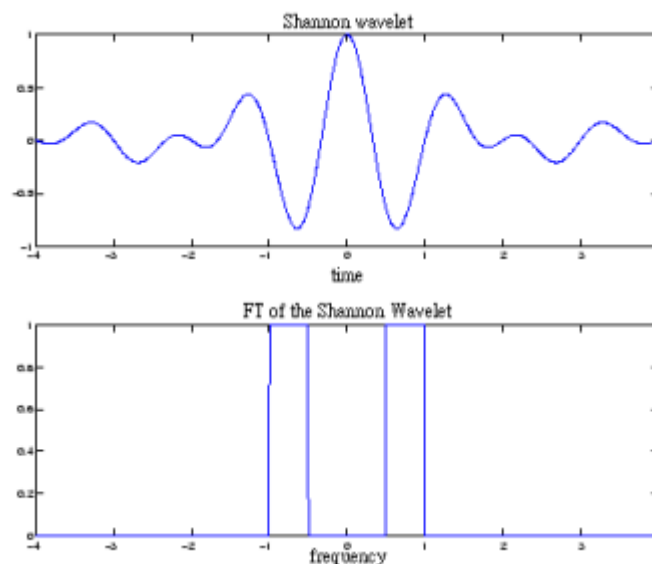


Figure.2.12. Shannon wavelets in time and frequency domain

Morlet wavelets

This wavelet family is a harmonic function multiplied by Gaussian window and they are symmetrical having an effective support from -4 to +4. It is the most commonly used continuous wavelet transform and is defined as

$$\Phi(t) = \pi^{-1/4} e^{int} e^{-\frac{t^2}{2\sigma^2}} \quad (2.58)$$

$$\hat{\Phi}(\omega) = \frac{-1}{\pi^4} U(\omega) e^{-\frac{(\omega-n)^2}{2}} \quad (2.59)$$

Where U is the step function, and n is the adjustable parameter of wave number that allows perfect signal reconstruction. The time and frequency plot is shown in figure. The white curve is the real component and the cyan curve is the complex component

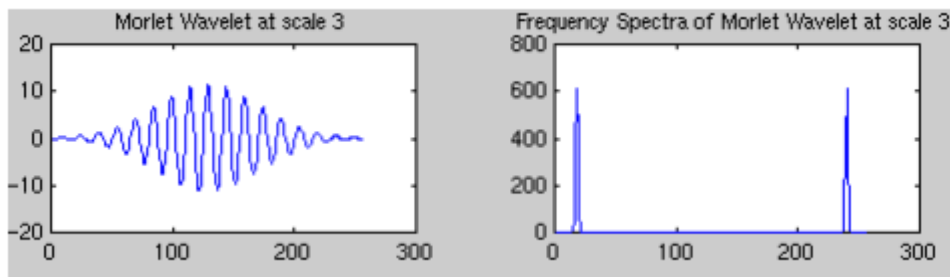


Figure.2.13. Morlet wavelet with m=3

Gaussian wavelets

This type of wavelet family is derived as a derivative of a single Gaussian function e^{-t^2} . These wavelets are either symmetrical or antisymmetrical. They have a very explicit expression and have infinite number of vanishing moments. They have a very good time resolution at the low order/ small number of derivatives.

Mexican hat

This wavelet is one of the most known representatives of Gaussian wavelet, it is computed by taking the negative second derivative. The wavelets are symmetrical and have a support length from -5 to +5. It has a very rapid decay and a narrow localisation in time as a result human eye somewhat works like a Mexican hat. This type of wavelet are a unique choice for vision analysis. This type of wavelet is define as the second derivative of the Gaussian function

$$h(t) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{t^2}{2\sigma^2}} \quad (2.60)$$

Which is

$$\Phi(t) = \frac{1}{\sqrt{2\pi}\sigma^3} \left[e^{-\frac{t^2}{2\sigma^2}} \left(\frac{t^2}{\sigma^2} - 1 \right) \right] \quad (2.61)$$

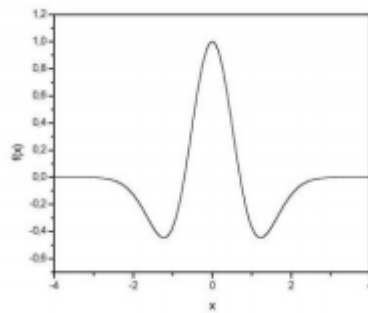


Figure.2.14. The Mexican Hat Wavelet

Meyer wavelet

Similar to the Shannon wavelet, meyer wavelet are also defined in frequency domain. But the difference here in meyer wavelet to that of the Shannon wavelet is, the sharp edges in frequency produced in Shannon wavelet is replaced by a smooth function. The effective support of this wavelet is from -8 to +8.

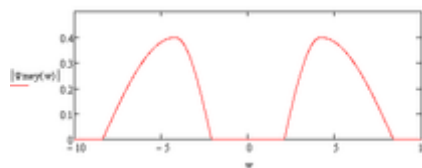


Figure.2.15 Spectrum of Meyer wavelet

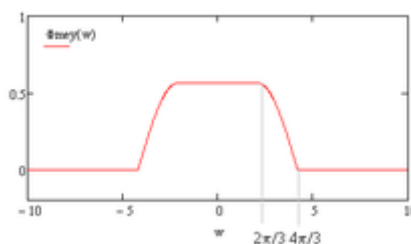


Figure.2.16. Meyer scale function

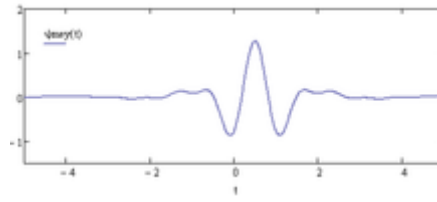


Figure.2.17. Meyer wavelet

Bi-orthogonal wavelets

Bi-orthogonal wavelets are mainly developed due to the requirements of both symmetry and perfect reconstruction and these properties are not compatible in one wavelet filter. These wavelets use different filters for decomposition and reconstruction.

2.4 Haar Wavelet Transform

The haar wavelet transform was introduced by Hungarian mathematician Alfred Haar [46] and this transform have been used from 1910. The transform is one of the simplest and earliest examples of what is known now as dyadic, compact, orthonormal wavelet transform [47,48]. The Haar function being an odd rectangular pair of pulse is useful for a quite a variety of applications like edge extraction, image coding and binary logic design. For application of Haar in logic design, efficient ways is needed to calculate the Haar spectrum from the reduced form of Boolean functions such as the disjoint cubes [49, 50] and different decision diagram[51,52,53,54]. Haar wavelet is a sequence of rescaled 'square-shaped' functions which form a wavelet family or basis.

2.4.1 Haar Functions

Alfred Haar defined a complete orthogonal system of function in $L_p[0,1]$, $p \in [1, \infty]$ taking values in the set $\{0, \sqrt{2}i\}$, $i \in \mathbb{N}_0$. Haar functions, has property that each function continuous on $[0, 1]$ can be represented by a uniformly convergent series in terms of system elements.

Definition 1. The Haar function can be defined as

$$\text{har}(0,\theta) = 1, \quad 0 \leq \theta \leq 1, \quad (2.62)$$

$$\text{har}(1,\theta) = \begin{cases} 1, & 0 \leq \theta < 1/2, \\ -1, & 1/2 \leq \theta < 1, \end{cases} \quad (2.63)$$

$$\text{har}(2,\theta) = \begin{cases} \sqrt{2}, & 0 \leq \theta < 1/4, \\ -\sqrt{2}, & 1/4 \leq \theta < 1/2, \\ 0, & 1/2 \leq \theta \leq 1, \end{cases} \quad (2.64)$$

$$\text{har}(3,\theta) = \begin{cases} 0, & 0 \leq \theta < 1/2, \\ \sqrt{2}, & 1/2 \leq \theta < 3/4, \\ -\sqrt{2}, & 3/4 \leq \theta < 1, \end{cases} \quad (2.65)$$

$$\text{har}(2^p+n,\theta) = \begin{cases} \sqrt{2^p}, & n/2^p \leq \theta < (n+1/2)/2^p, \\ -\sqrt{2^p}, & (n+1/2)/2^p \leq \theta < (n+1)2^p, \\ 0, & 0 < \theta < n/2^p \text{ and } (n+1)2^p < \theta < 1, \end{cases} \quad (2.66)$$

$p=1, \dots; n=0, \dots, 2^p-1.$

In his original work, Haar defined the Haar function as

$$\text{har}(k,0) = \lim_{\theta \rightarrow 0, \theta > 0} \text{har}(k, \theta), \quad (2.67)$$

$$\text{har}(k,1) = \lim_{\theta \rightarrow 1, \theta < 0} \text{har}(K, \theta), \quad (2.68)$$

and the points of discontinuity within the interior (0,1) of the interval [0,1]

$$\text{har}(k,\theta) = \frac{1}{2}(\text{har}(k,\theta-0) + \text{har}(k, \theta+0)). \quad (2.69)$$

Where some authors use

$$\text{har}(k,\theta) = \text{har}(k, \theta+0), \quad (2.70)$$

In practice, it is assumed that the haar function takes zero value at the points of discontinuity.

Two parametric notations for the Haar function $\text{har}(i,j,\theta)$ or $H_i^{(j)}(\theta)$ is used oftenly, where

$$H_0^{(0)}(\theta) = \text{har}(0,\theta), \quad (2.71)$$

$$H_i^{(j+1)} = \text{har}(2^{i-1} + j, \theta), \quad i \in \mathbb{N}_0, j=1, \dots, 2^i. \quad (2.72)$$

The parameter i is called the power of Haar function and which is used to denote the subset of Haar functions with the same number of zero crossings on the interval of the length $1/2^i$.

Definition 2. The Haar functions are defined as

$$\text{har}(0,0,\theta) = 1, 0 \leq \theta \leq 1, \quad (2.73)$$

$$\text{har}(i,j,\theta) = \begin{cases} \sqrt{2^i}, & (j-1)/2^i \leq \theta < (j-1/2)/2^i, \\ -\sqrt{2^i}, & \frac{j-1/2}{2^i} \leq \theta < \frac{j}{2^i}, \quad i = 0,1,2, \dots; \quad j = 1, \dots, 2^i. \\ 0, & \text{otherwise} \end{cases} \quad (2.74)$$

Haar functions are orthogonal functions, therefore

$$\int_0^1 \text{har}(m,\theta) \text{har}(n,\theta) d\theta = \begin{cases} 1, & n = m, \\ 0, & n \neq m. \end{cases} \quad (2.75)$$

The completeness for the system of Haar functions has been proof by Haar himself [46]. It was proved by Uljanov [55] that uniform convergence of series in terms of the Haar functions will be missing, if zero is taken at the points of the discontinuity. Which means that the basic motive for introduction of the Haar functions in mathematical analysis, i.e., for uniform approximation in $L_p [0,1]$, is not preserved. However, other properties of Haar functions, which make them applicable in engineering practice, and resulting advantages in numerical computations, make this assumption acceptable and justified. An outstanding property of the Haar functions is that except $\text{har}(0,\theta)$, the i th Haar function can be obtained by the restriction of the $(i-1)$ th function to the half of the interval where it is different from zero, by multiplication with $\sqrt{2}$ and by scaling over the interval $[0,1]$.

2.4.2 Haar Wavelet Properties

- Any continuous real function with compact support can be approximate uniformly by linear combination of $\Phi(t), \Phi(2t), \Phi(4t), \dots, \Phi(2^n t)$ and their shifted functions. This extends to those function spaces where any function therein can be approximated by continuous function.
- Any continuous real function on $[0, 1]$ can be approximated uniformly on $[0, 1]$ by linear combinations of the constant function 1, $\Psi(t), \Psi(2t), \Psi(4t), \dots, \Psi(2^n t), \dots$ And their shifted functions.
- Orthogonality in the form

$$\int_{-\infty}^{+\infty} 2^{\frac{n+n_1}{2}} \Psi(2^n t - k) \Psi(2^{n_1} t - k_1) dt = \delta_{n,n_1} \delta_{k,k_1}. \quad (2.76)$$

Here the $\delta_{i,j}$ represents the kronecker delta. The dual function of $\Psi(t)$ is $\Psi(t)$ itself.

The wavelet/ scaling functions with different scale n have a functional relationship, since

$$\Phi(t) = \Phi(2t) + \Phi(2t-1) \quad (2.77)$$

$$\Psi(t) = \Phi(2t) - \Phi(2t-1), \quad (2.78)$$

It follows that coefficients of scale n can be calculated by coefficients of scale $n+1$

$$\text{If } \chi_w(k,n) = 2^{n/2} \int_{-\infty}^{+\infty} x(t) \Phi(2^n t - K) dt$$

$$\text{And} \quad (2.79)$$

$$X_w(k,n) = 2^{n/2} \int_{-\infty}^{+\infty} x(t) \Psi(2^n t - K) dt \quad (2.80)$$

Then

$$\chi_w(k,n) = 2^{-1/2} (\chi_w(2k,n+1) + \chi_w(2k+1, n+1)) \quad (2.81)$$

$$x_w(k,n) = 2^{-1/2} (\chi_w(2k,n+1) - \chi_w(2k+1, n+1)) \quad (2.82)$$

2.5 Principal Component Analysis

Principal component analysis is a mathematical procedure that is concerned with data reduction and interpretation by explaining the variance-covariance structure of the data with the help of linear combination of the original variables. For data reduction, principal component analysis acts as a tool to reduce large set of data variable to a smaller set retaining most of the important information in the larger set. Moreover, principal component analysis can also be thought as a mathematical tool that transform a number of correlated variable into uncorrelated variables called the principal components. The main purpose of principal component analysis is to derive new variables (in the decreasing order of importance) which are in linear combination of the original data. Most of the variance in the original data are held account by the first few components, and this are used to reduce the dimensions of the data. Principal component analysis is often confused with the factor analysis. The principal

component analysis can be thought as a rotation of axes of the original variable coordinate system to new orthogonal axes in such a way that the new axes coincide with the direction of the maximum variation of the original observation.

Principal component analysis is widely used in meteorology. An explanation for this is shown by an example. Consider x denotes a typical meteorological dataset, where the numbers of observation features are label as m and the number of discrete observation times as n . Observation features have the following records such as the highest temperature, lowest temperature, dew point, sun rise time, sun set time , humidity and so on...and these are called the feature variables.

$$X = \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{m1} & \cdots & x_{mn} \end{pmatrix} \text{ (observation features)}$$

The column represents the observation times, so each column represents a data point in the original state space. Thus in X , x_{ij} stands for the j -th observation of the i -th feature, where $i=1,2,\dots,m$ and $j=1,2,\dots,n$

It is expected that when the sampling instance for observation is sufficiently small, the feature values observed at different instance are correlated. The data points are not evenly scattered through the m -dimensional state space and tends to cluster around lower dimensional hyper surface. Thus X is describe in the following model

$$X^{(j)} = f\{s_f[X^{(j)}]\} + \vec{\epsilon} = \hat{X}^{(j)} + \vec{\epsilon} \quad (2.83)$$

Where $X^{(j)}$ is the j -th column vector X , and $\hat{X}^{(j)} = f\{s_f[X^{(j)}]\}$

$s_f: \mathfrak{R}^m \rightarrow \mathfrak{R}^p$, $1 \leq p < m$, function having a lower dimension than the dimension of $X^{(j)}$

$f: \mathfrak{R}^p \rightarrow \mathfrak{R}^m$ that maps the lower dimensional space to the original data space X , since $X^{(j)} \in X$ and $\vec{\epsilon}$ is the residual of the approximation of $X^{(j)}$. the functions s_f and f are both chosen to be linear function in principal component analysis.

To determine s_f an optimality criterion is used which minimised the sum squares of the residuals. For that the m -dimensionality of $X^{(j)}$ as a superficial signal such as noise or due to the influence of weak, extraneous phenomena and lives on p -dimensional subspace of \mathfrak{R}^m . After we found f and s_f we can concentrate and work on data of lower dimensional space \mathfrak{R}^p , instead of working on signal in \mathfrak{R}^m . Which simplifies the analysis procedure.

2.5.1 Traditional Principal Component Analysis

Traditional principal component analysis can be used for feature-extraction problem as a special case. Where the data $X^{(j)}$ is fit to the linear p-dimensional model $X^{(j)} = \sum_{k=1}^p [X^{(j)} \cdot e_k] e_k + \epsilon^{(j)}$, for vectors $e_k \in \mathbb{R}^m$.

Let $\hat{X}^{(j)} = \sum_{k=1}^p [X^{(j)} \cdot e_k] e_k$, such that the sum of squares of the residuals $J = \langle \|X - \hat{X}\|^2 \rangle$ is a minimum, here the angle brackets denote a sample average. The vector e_k is known both as the principal component direction and the EOF(empirical orthogonal function) and the projection of $X^{(j)}$ on e_k is the k-th Principal Component(PC). The product of the k-th PC mode. The Principal component analysis approximation lead to the projection $\hat{X}^{(j)}$ which passes roughly through the ‘middle’ of the data cloud and lie on the p-dimensional hyper plane. The Principal component analysis approximation minimizes the variance of the original data, hence, it is the optimal linear approach. The relation is given as

$$\sum_{i=1}^m \text{var}(X_i) = \sum_{i=1}^m \text{var}(\hat{X}_i) + \sum_{i=1}^m \text{var}(X_i - \hat{X}_i) \quad (2.84)$$

Where X_i represents the i-th row of X. $\hat{X}^{(j)}$ explains a little fraction of of the variance of $X^{(j)}$. $\hat{X}^{(j)} = [X^{(j)} \cdot e_1] e_1$ Explain the highest percentage of the variance and is the one dimensional approximation of $X^{(j)}$. to measure the effectiveness of principal component analysis, the fraction of unexplained variance (FUV) is used, which is given by

$$\text{FUV} = \left| \frac{\sum_{i=1}^m \text{var}(X_i) - \sum_{i=1}^m \text{var}(\hat{X}_i)}{\sum_{i=1}^m \text{var}(X_i)} \right| \quad (2.85)$$

the principal component analysis approximation \hat{X} explained by the fraction of variance is a nondecreasing function of the approximation dimension p. Therefore increasing the dimensionality of the principal component analysis approximation, increases the fidelity of the original data, thus improving the accuracy of approximation.

2.5.2 Deriving The PCA By Using Covariance Method

Let $X^{(j)}$ be an m-dimensional random vector expressed as a column vector and has zero mean. We want to find an $m \times m$ orthonormal projection matrix P such that

$$Y^{(i)} = p^T X^{(j)} \quad (2.86)$$

Where $P^{-1} = P$, such that $\text{cov}(Y^{(j)})$ is a diagonal matrix.

By calculation, we obtain

$$\begin{aligned} \text{Cov}(Y^{(j)}) &= E[Y^{(j)} Y^{(j)T}] \\ &= E[(P^T X^{(j)})(P^T X^{(j)})^T] \\ &= E[(P^T X^{(j)})(X^{(j)T} P)] \\ &= P^T E[X^{(j)} X^{(j)T}] P \\ &= P^T \text{cov}(X^{(j)}) P \end{aligned} \quad (2.87)$$

We now have

$$\begin{aligned} P \text{cov}(Y^{(j)}) &= P P^T \text{cov}(X^{(j)}) P \\ &= \text{cov}(X^{(j)}) P \end{aligned} \quad (2.88)$$

Notice that $P = [P^{(1)}, P^{(2)}, \dots, P^{(m)}]$, with $P^{(j)}$ the columns of P , for $j=1, 2, \dots, m$

And $\text{cov}(Y^{(i)})$ as:

$$\text{Cov}(Y^{(i)}) = \begin{pmatrix} \lambda_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda_m \end{pmatrix} \quad (2.89)$$

Substituting equation (2.89) in equation (2.88) we get

$$[\lambda_1 P^{(1)}, \lambda_2 P^{(2)}, \dots, \lambda_m P^{(m)}] = [\text{cov}(X^{(j)}) P^{(1)}, \dots, \text{cov}(X^{(j)}) P^{(m)}] \quad (2.90)$$

Notice that

$$\lambda_i P^{(i)} = \text{cov}(X^{(j)}) P^{(i)} \quad (2.91)$$

$P^{(i)}$ is an eigenvector of $\text{cov}(X^{(j)})$.

Therefore, by finding the eigenvectors of $\text{cov}(X^{(j)})$, we obtain the projection matrix P that satisfies the constraints, and we find the principal components by finding the column vectors of matrix $Y^{(j)}$.

2.5.3 The Reason Why We Need Principal Component Analysis

There are many reason of using the principal component analysis. One of the major important application is to produce a low-dimensional representation of the original data with minimum loss of information so that the data can be easily understood and the structure of the data can be easily identified.

2.6 Arnold Cat Map

2.6.1 Introduction: Chaos

First a working understanding of chaos is discussed before undertaking Arnold's cat map. We already had an idea about Chaos, some nebulous sense that it involves randomness, disorder, entropy, disorganization etc. Over time, systems tend to be chaotic and disorder. For example with indifferent cleaning bedroom changes from initial state if order to disorder. A jar of marbles containing two different colors which has been grouped by colors are randomly distributed when vigorously shaken. Infact, the sacrosanct and inviolable second Law of Thermodynamics tells us much about the random nature of universe over time. The chaos to be discussed is inextricably tied to the above and is because of the fledgling science of chaos. The science of chaos came into the public domain in the recent years after the popularization of the motion pictures such as the Jurassic park and books such as Chaos: Making a new science by James Gleick's. Chaos came into being in 1960 from the works of Edward Lorenz who is a meteorologist in Massachusetts Institute of technology. He created a simulation of weather in his newly purchased computer, using simple system of equations. His computer does not have the computational power or the memory for a sophisticated system. When the initial conditions were entered, the weather conditions would unfold such as the blizzards, downpours, droughts and other meteorological adversities. With the urge to examine a particular run with greater details, he re-enter its initial conditions. However, he discovered that the data from the first run has six decimal places of accuracy whereas the second only has three, which should have been virtually identical. Surely a small error by truncating the initial conditions by three decimal places could not have introduced this troubling behaviour, but it did. Complex systems or even the simplified complex systems such as Lorenz's are extremely sensitive to initial conditions. Small error propagates through such systems. And Lorenz's called this the butterfly effect. The word Chaos was coined mathematically in 1975 after the publication of "Period Three implies Chaos" by James Yorke and Tien-Yien Li.

Broadly defined, Chaos refers to the mathematical or physical phenomena that are random yet they possess some order.

2.6.2 Arnold Cat Map

It was discovered by Russian mathematician Vladimir I. Arnold in 1960. He demonstrated its effect using the image of a cat, hence the name Arnold Cat Map. It is a simple and elegant demonstration and illustration of the principles of chaos. An image when it is hit with a transformation that randomizes the original organization of its pixels. However, when iterated enough times, as though by magic, the original image reappears.

If we let $X = \begin{bmatrix} x \\ y \end{bmatrix}$ be an $n \times n$ matrix of some image, Arnold's Cat map transformation is given as

$$\Gamma \begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x + y \\ x + 2y \end{bmatrix} \text{mod } 1$$

Where mod is the modulo of the $\begin{bmatrix} x + y \\ x + 2y \end{bmatrix}$ and 1.

This can also be put as

$$\Gamma \begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \text{mod } 1$$

The determinant of the transformation is

$$\begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix} = (1)(2) - (1)(1) = 1$$

which confirms that the Arnold Cat Map transformation preserves area. By factoring the Arnold's Cat Map we can get a glimpse of the geometric aspects of the transformation.

$$\Gamma \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \text{mod } 1$$

From this we can get that the Arnold Cat Map is a composed of a shear in the x-direction by a factor 1, and a shear in the y-direction by a factor 2 and the mapped back to the same area as shown in figure.

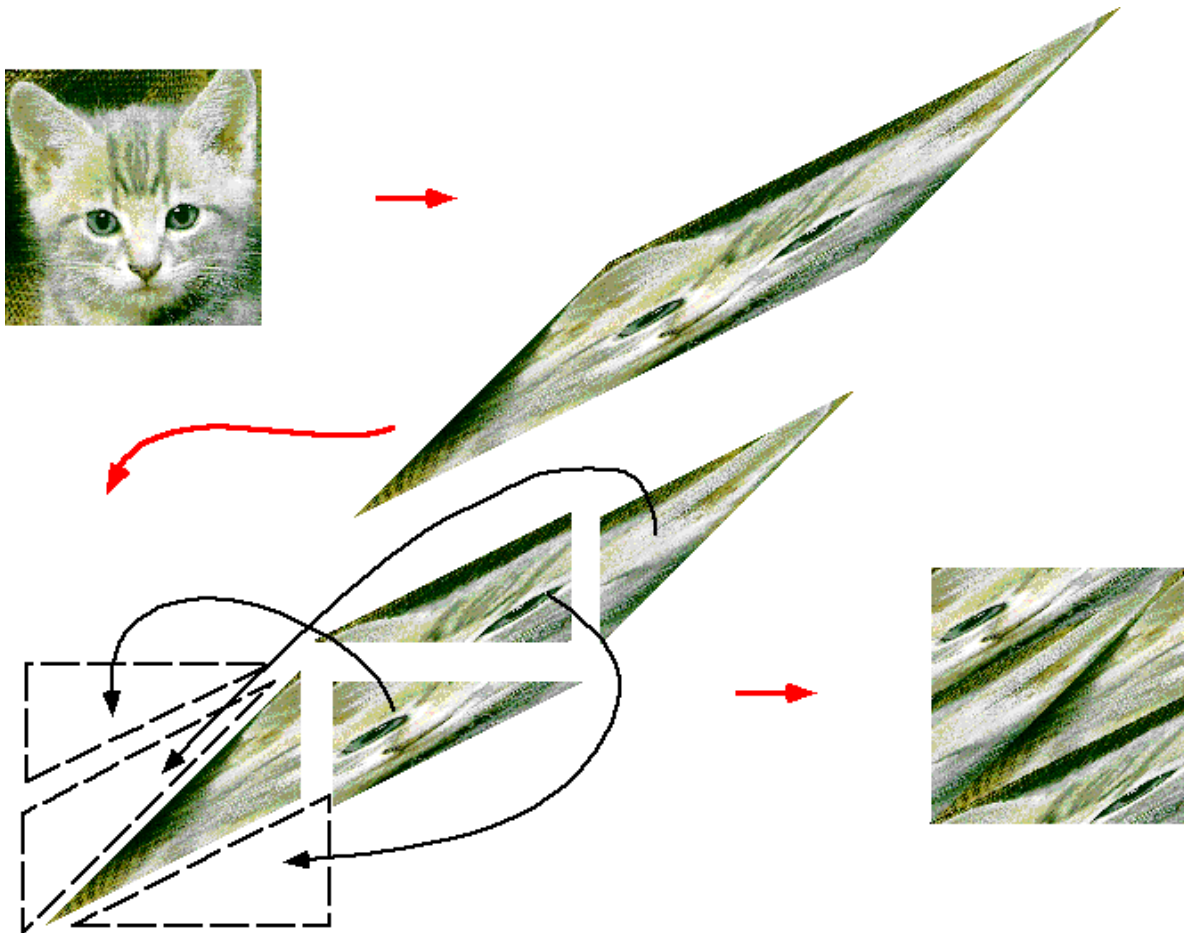


Figure.2.18. Cat Mapping

2.6.3 Periodicity of Arnold Cat Map

Periodic points

Arnold's Cat Map is a chaotic transformation we observed how it maps a set of points over a period of time. Observing an image after each transformation iterations, we notice two striking facts, one the number of iterations produce a pattern of directional strikes and the other is that, the image come to its initial state after a certain number of iterations. And this number of iteration taken by the image to return to its initial state is called the period of Arnold Cat Map.

An overview of the periodic mapping of points as the transformation is iterated is discussed in the following. Individual points in an image is referred to as pixels and the xy-plane where it lies is called the pixel map. The position of the pixels in an image is given by the pixel coordinate system of S which is along the rows and columns of the map. Fro example a pixel map of 250 by 250 will have coordinates $(\frac{m}{250}, \frac{n}{250})$ where m is the column number and n is

the row number. In general if the number of pixel is p then the coordinates are $(\frac{m}{p}, \frac{n}{p})$ with a range and domain of $\{0,1,2, \dots, p - 1\}$. Arnold cat map is the transformation that maps a set of pixel points in S to another set of pixel coordinate in S . It follows that Arnold cat map requires a maximum of p^2 iterations for the image to reappear to its initial state. Howard Anton and Chris Rorres gives an example that if $p = 76$, then the transformation becomes

$$\Gamma\left(\begin{bmatrix} \frac{m}{76} \\ \frac{n}{76} \end{bmatrix}\right) = \begin{bmatrix} \frac{m+n}{76} \\ \frac{m+2n}{76} \end{bmatrix} \text{ mod } 1$$

The successive iterations for the points $(\frac{27}{76}, \frac{58}{76})$ are

$$\begin{array}{ccccccccc} 0 & & 1 & & 2 & & 3 & & 4 \\ \begin{bmatrix} \frac{27}{76} \\ \frac{58}{76} \end{bmatrix} & \rightarrow & \begin{bmatrix} \frac{9}{76} \\ \frac{67}{76} \end{bmatrix} & \rightarrow & \begin{bmatrix} \frac{0}{76} \\ \frac{67}{76} \end{bmatrix} & \rightarrow & \begin{bmatrix} \frac{67}{76} \\ \frac{58}{76} \end{bmatrix} & \rightarrow & \begin{bmatrix} \frac{49}{76} \\ \frac{31}{76} \end{bmatrix} \\ & & & & & & & & \\ & & 5 & & 6 & & 7 & & 8 & & 9 \\ & \rightarrow & \begin{bmatrix} \frac{4}{76} \\ \frac{35}{76} \end{bmatrix} & \rightarrow & \begin{bmatrix} \frac{39}{76} \\ \frac{74}{76} \end{bmatrix} & \rightarrow & \begin{bmatrix} \frac{37}{76} \\ \frac{35}{76} \end{bmatrix} & \rightarrow & \begin{bmatrix} \frac{72}{76} \\ \frac{31}{76} \end{bmatrix} & \rightarrow & \begin{bmatrix} \frac{27}{76} \\ \frac{58}{76} \end{bmatrix} \end{array}$$

From the transformation we can see that the points have 9 cycle, because after 9 iterations the points returns to its initial position. Therefore, in general the period of n will have n -cycle, which means that it will require n distinct iterations to bring back to its original position.

Pixel Width vs. period

Using Arnold Cat Map, eventually every points/ pixel will return to its original state/position after a number of iterations. Mathematically it occurs at the multiple of each different period point in the image. Which means that if every pixel in an image has a period of q_1 and q_2 then at every multiple iterations of q_1q_2 the image will return to its initial state. The period of pixel map is represented as $\Pi(p)$ where p is the number of pixels. Interestingly there is no equation that shows the relationship between the period of pixel map and the number of pixels. Although a comparison graph between the p and $\Pi(p)$ we see that there is a gradual climb in the period of pixel map as the pixel increases, but there is lots of irregularities. It is also came to know that as the number the pixels in an image increase, it is not necessarily for the period of pixel to increase as well. From the table we came to see this

Pixel dimension of image ($N \times N$)	Iterations to restore image (period)
300×300	300
257×257	258
183×183	60
157×157	157
150×150	300
147×147	56
124×124	15
100×100	150

Table.2.1 Pixel dimension and number of iterations required

CHAPTER 3

PROPOSED TECHNIQUE

Introduction

Algorithm Description

Experimental Work and Discussion

Comparison and Discussion

Chapter-3

Watermarking Using Principal component analysis and Arnold Cat Map

3.1 Introduction

In this a robust video watermarking scheme is discuss. Following transform has been used: Discrete Wavelet transform (DWT), Principal Component Analysis (PCA). A chaotic technique called the Arnold cat map is also used in the scheme, which is used to scramble the watermarked image before it is embedded in each video frames. Here, in the scheme Haar 2-D wavelet transform is used. The Haar wavelet transform is characterized by its reality and orthogonality. The reason of using Haar wavelet transform is because of its simplicity and good performance in terms of computational time as Haar wavelet transform is very fast. Moreover it has perfect reconstruction property. The Wavelet transform decompose each video to 4 sub-images, 3 details and 1 approximation. The lower resolution approximation image (LL) gives the approximation sub-image. And the horizontal (HL), vertical (LH) and diagonal (HH) sub-images gives the detail components. The main reason of using the wavelet transform is because it has high compatibility with the model aspect of the Human visual system (HVS) comparing with the FFT and DCT. Moreover it also allows higher energy to be embedded in the region such as high resolution detail band where the HVS is less sensitive. In the proposed algorithm, the watermark is embedded in the diagonal (HH) detailed component. Also Principal component analysis is also used in the proposed algorithm. The principal component analysis is an orthogonal transformation that changes a set of observations which is possibly correlated to a new set of uncorrelated variables called the principal components. Arnold cat map scrambling technique is also used in the technique which is used to scramble the watermark to provide security. The number of iterations and the initial values are used as the secret key to provide security. In the proposed algorithm the scrambled watermark image is embedded into the block based PCA and is extracted in the similar way.

3.2 Algorithm Description

In the proposed scheme, we denote the host video frame by $X(m,n)$ and the binary watermark image by $w(m,n)$. The watermark used in the algorithm is a 2-Dimensional array

of real elements and is visually recognizable binary image. The size of the watermark used in the algorithm is 32×32 and is much smaller than the host video frame dimension. Usually it is required that the watermark size is smaller than the host data by a factor of 2^M where M is an integer greater than or equal to 1 in order to avoid loss of generality.

Watermark Embedding Method

The proposed techniques consist of 9 stages for watermark embedding. The following is the detail description of the procedure.

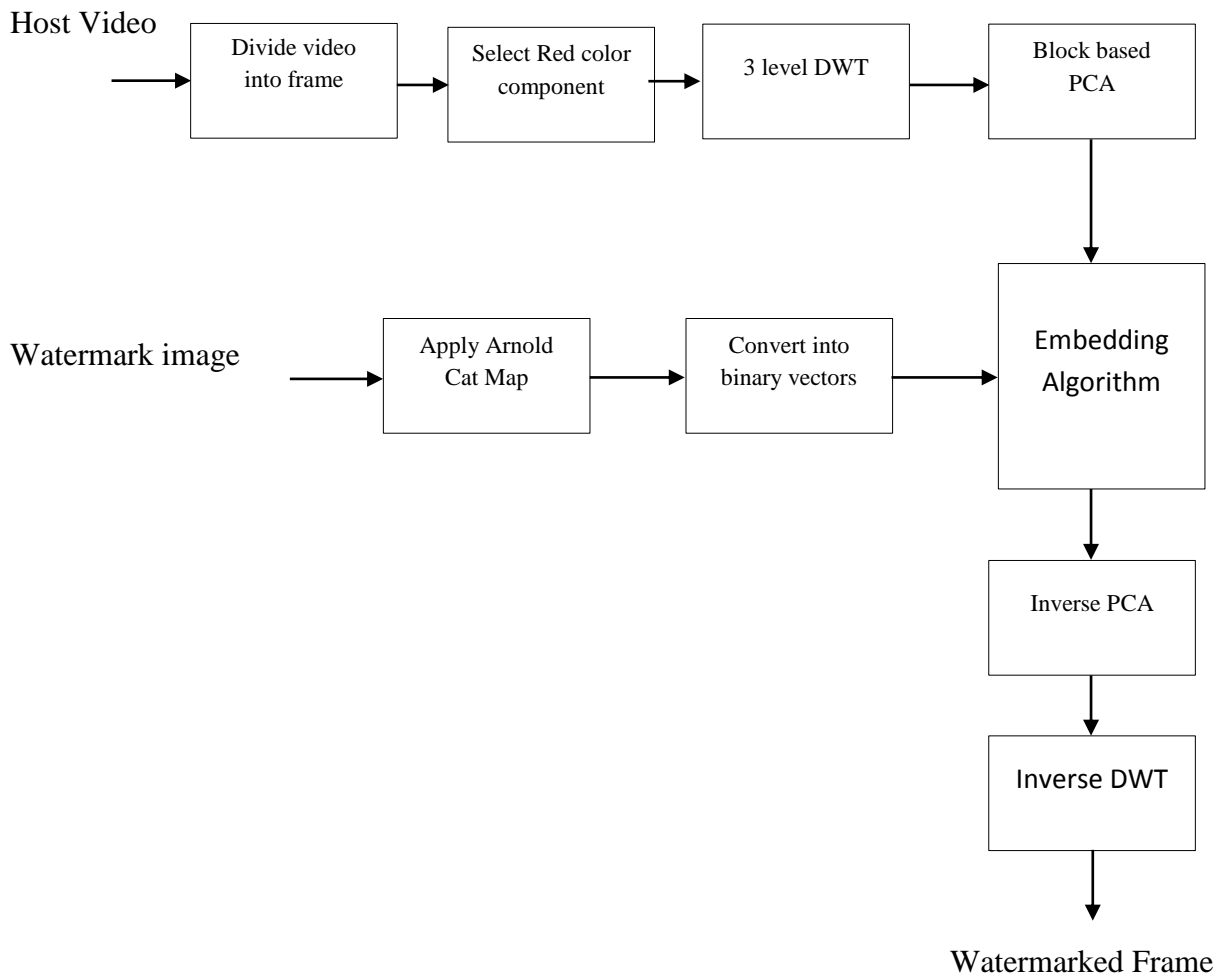


Figure.3.1. Embedding stages

Stage1. The Host video is read and is divided into video frames.

Stage2. From each frame the RGB color component is separated and from there the red component is selected for embedding the watermark.

Stage3. A 3 level DWT is performed on the red color component of the video frame. The diagonal (HH) detailed component of the wavelet transform is selected to embedding the watermark.

Stage4. The diagonal (HH) detailed component is divided into non-overlapping blocks and PCA is applied to obtain the Principal components for embedding the watermark.

Stage5. The binary watermark image BW is read and Arnold Cat Map is perform on the watermark image. The initial value and the number of iterations is hold as the security for the proposed watermarking algorithm.

Stage6. Convert the scrambled binary watermark into a vector of $BW' = \{bw_1', bw_2', \dots, bw_{m,n}'\}$ of '0's and '1's.

Stage7. The watermark is embedded into the Principal components PCB obtained from PCA using the following equation.

$$PCB'(m,n) = PCB(m,n) + k.w(m,n) \quad (2.92)$$

Where, k is the embedding strength.

Stage8. Apply inverse PCA on the modified Principal components of the HL band to obtain the modified wavelet coefficients.

Stage9. Apply inverse DWT to obtain the Red component of the frame. Then reconstruct the watermarked frame X_w .

Watermark extraction method

The objective of the extraction process is to reliably extract the embedded watermark from the possibly corrupted or distorted watermarked video frame X_w , in the proposed algorithm the reconstruction process requires the knowledge of the original Host video frame. There are 7 stages used in the proposed technique for extracting the watermark from the watermarked video fames which is discuss in the following.

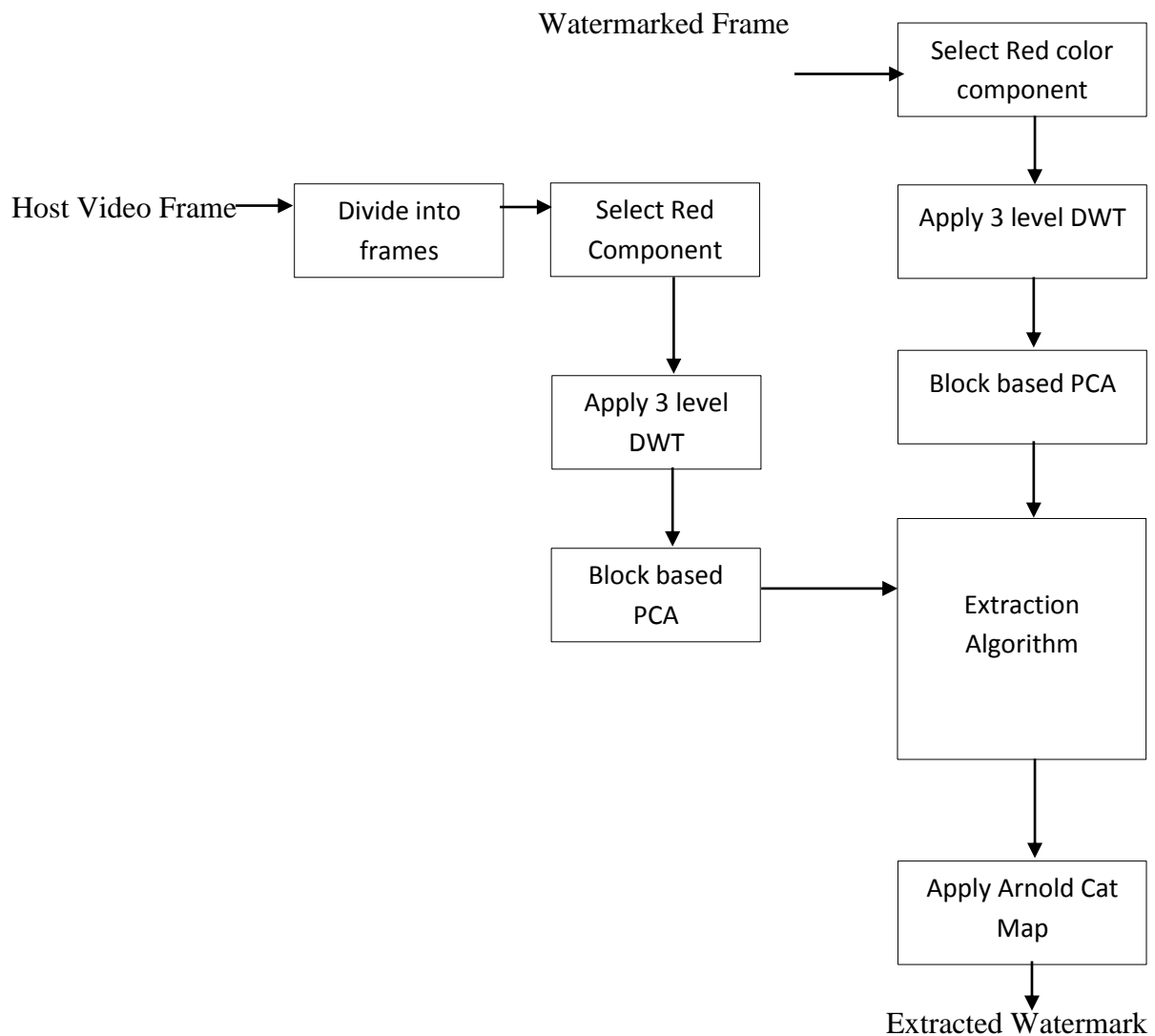


Figure.3.2. Watermark extraction flowchart

Stage1. Read the watermarked video and divide it into video frames.

Stage2. From each watermarked frame the RGB color component is separated and from there the red component is selected for extracting the watermark.

Stage3. Apply 3 level DWT on the red component of the watermarked video frame. The multi-level DWT is applied on the HH detailed component as same as in the embedding procedure.

Stage4. Divide the sub band HH into $n \times n$ non overlapping block.

Stage5. Block based PCA is applied the non overlapping block of HH band to obtain the watermarked Principal components PCB’.

Stage6. The watermark is extracted using the following equation

$$BW' = (PCB' - PCB) / k. \quad (2.93)$$

Where PCB is the principal components of host video frame and k is the embedding strength.

Stage7. Apply Arnold Cat map on the extracted watermark and apply thresholding to obtain the embedded watermark image.

3.3 Experimental work and Discussion

For the experimental work the video sample ‘xylophone.avi’ which is of dimension 512×512 and has 69 frames, 24 bits per pixel, 14.9850 frame rate and is used. A gray scale watermark image ‘apple.gif’ of 32×32 is used as shown in figure.



Figure.3.3. Original watermark image

The original watermark is being scrambled before embedding using Arnold Cat Map. Where the Arnold Cat Map is given by the equation

$$x' = [x + py] \text{mod}(n) \quad (2.94)$$

$$y' = [qx + (pq + 1)y] \text{mod}(n) \quad (2.95)$$

In the work, the initial values is chosen as p=1 and q=1. It being found that for the given watermark image after applying Arnold Cat Map it reappears after 24 numbers of iterations. As shown in figure. Thus, in the experiment the scrambled watermark image for embedding in the video sample is obtained by iterating the watermark image for 10 numbers of iterations. The scrambled watermark image is as shown in figure.



Figure.3.4.(a)

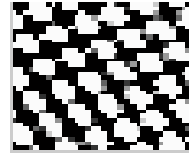


Figure.3.4.(b)

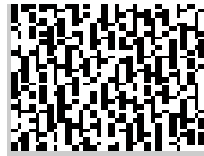


Figure.3.4.(c)

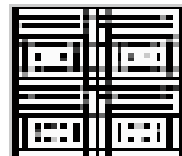


Figure.3.4.(d)



Figure.3.4.(e)



Figure.3.4.(f)

Figure.3.4. Periodic phenomenon in Arnold's cat map.(a) the original watermark image ;(b),(c),(d),(e) are the scrambled images after iterations $k=8$, $k=10$, $k=12$ & $k=22$;(f) the watermark image reappears after a period of 24.



Figure.3.5. Scrambled watermark image for embedding

The host video is read and the video is divided into frames and from each frame the red color component as shown in figure is chosen for embedding the watermark.

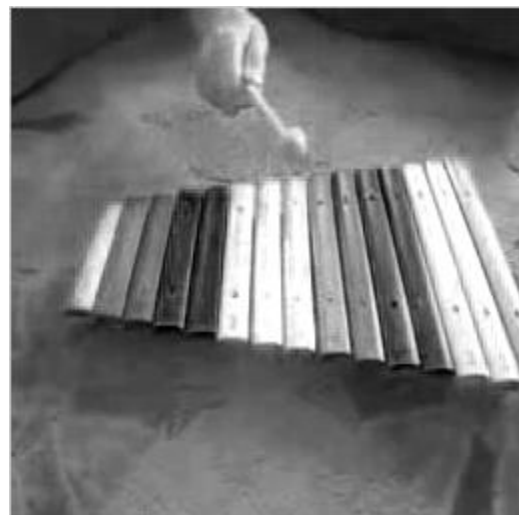


Figure.3.6. (a)

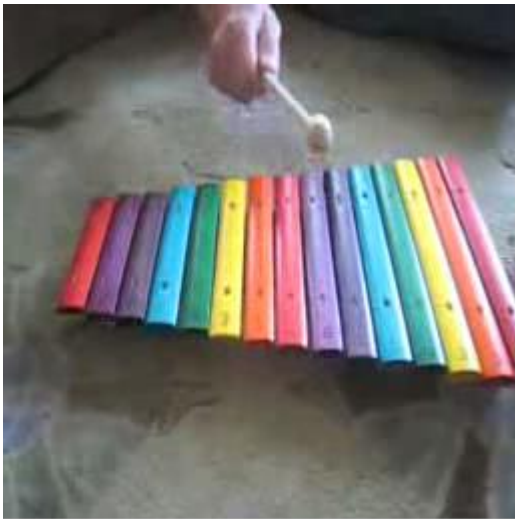


Figure.3.6.(d)



Figure.3.6.(b)

Figure.3.6.(e)



Figure.3.6.(c)

Figure.3.6.(f)

Figure.3.6. (a),(b)&(c) the host video frames, frame number 30,35,50; (d),(e)&(f) their resulting red color component for watermark embedding.

A three level 2-D Haar discrete wavelet is applied on the red color component of each video frames and the HH band is chosen for inserting the watermark as shown in figure. The HH band after applying Haar discrete wavelet is then divided into 4 non-overlapping block and

the principal component analysis is applied on the 4 non-overlapping to obtain the Principal components to embed the watermark bits.

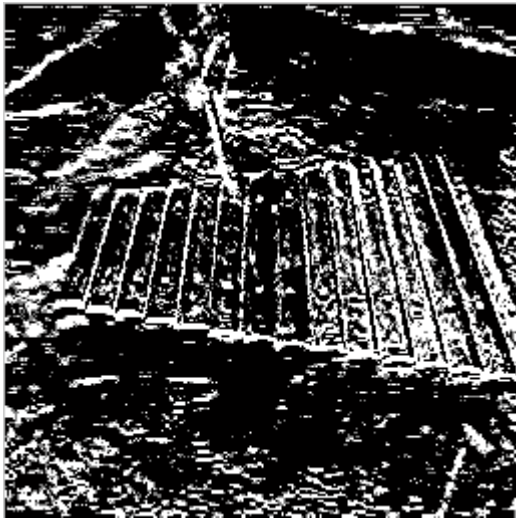


Figure.3.7.(a)

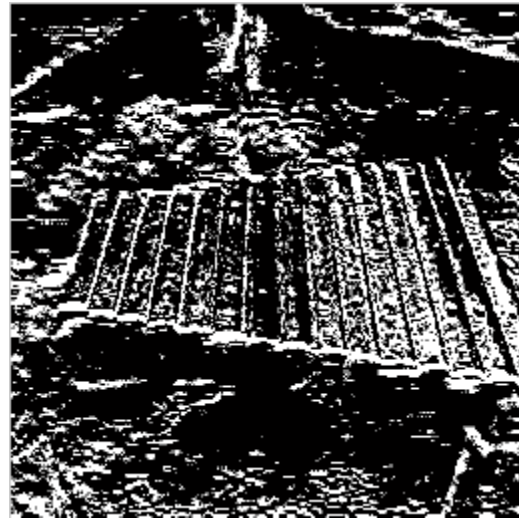


Figure.3.7.(d)

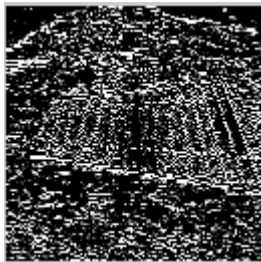


Figure.3.7.(b)



Figure.3.7.(e)



Figure.3.7.(c)

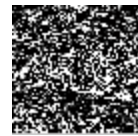


Figure.3.7.(f)

Figure.3.7. (a),(b)&(c) the HH band obtained after applying 3 level DWT on the red color component of frame number 35; (d),(e)&(f) on frame number 60.

After obtaining the principal components the watermark is inserted, in the experiment the watermark embedding strength is used as 22. The inverse PCA and inverse DWT is applied

after the insertion of watermark bits on the principal components to obtain the watermarked frame as shown in figure



Figure.3.8.(a)



Figure.3.8.(b)

Figure.3.8. (a) & (b) watermarked video frame number 15 and 65

For the extraction of watermark, the knowledge of the host video is required. The watermarked video is decomposed in the similar way as it was done for the insertion process. The Red color component of the watermarked video frame is obtained as shown in figure. and the HH band of the watermarked video is obtained after applying 3 level DWT as shown in figure for extraction of watermark.

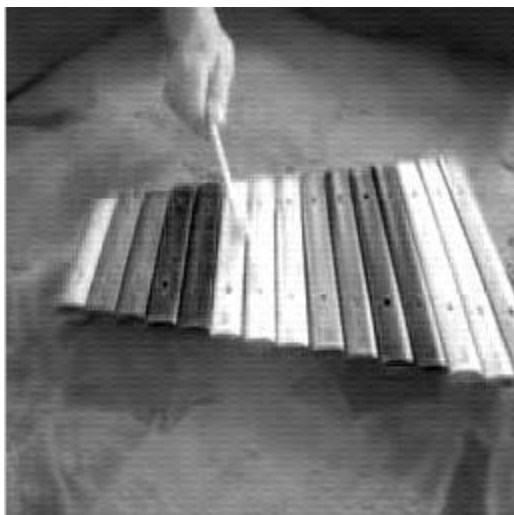


Figure.3.9.(a)

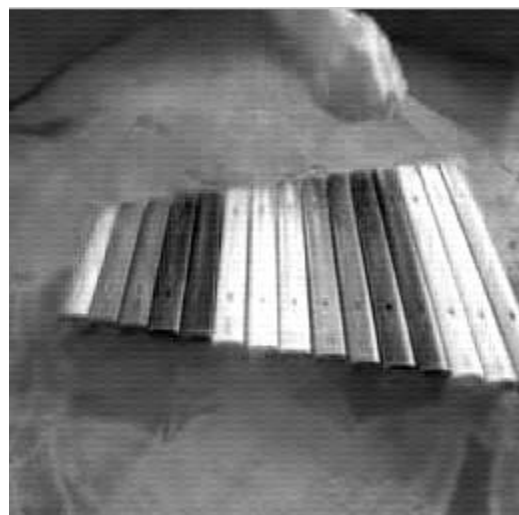


Figure.3.9.(b)

Figure.3.9. (a) & (b) Red color component of the watermarked video frame 24 and 47

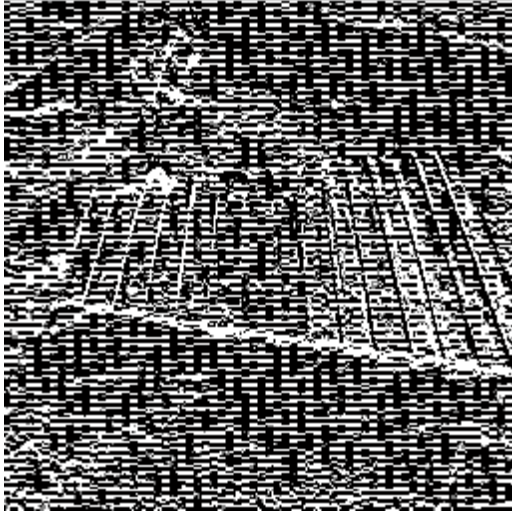


Figure.3.10.(a)

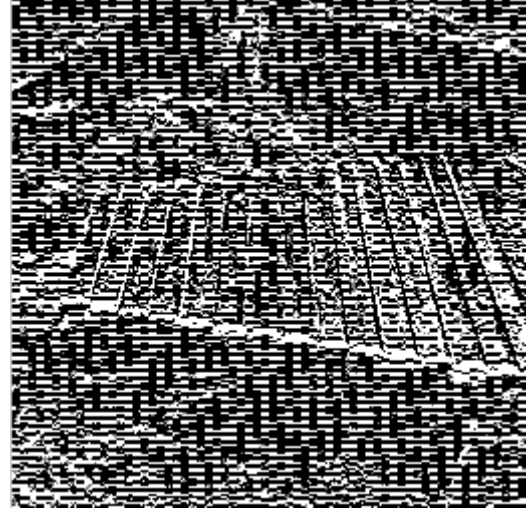


Figure.3.10.(d)

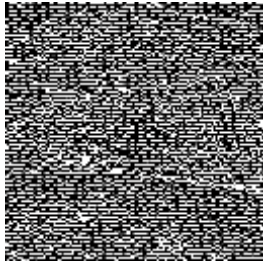


Figure.3.10.(b)



Figure.3.10.(e)



Figure.3.10.(c)

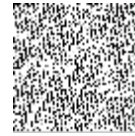


Figure.3.10.(f)

Figure.3.10.(a),(b)&(c) HH band obtained by applying 3 level DWT on watermarked frame 18; (d),(e)&(f) HL bands from watermarked frame 60.

The watermark image is estimated by using the equation discussed above. the extracted watermark bits is in scrambled form as shown in figure of that original watermark image , to estimate the watermark image, the Arnold Cat Map is applied to the scrambled watermark bits. The estimated watermark image after extraction is as shown in figure.



Figure.3.11.(a)



Figure.3.11.(d)



Figure.3.11.(b)



Figure.3.11.(e)



Figure.3.11.(c)



Figure.3.11.(f)

Figure.3.11. (a),(b)&(c) The extracted watermark bits from frame 1,34&69; (d),(e)&(f) the extracted watermark image from frame 1,34&69 after Arnold Cat Map.

The performance of the proposed algorithm is measured in terms of its imperceptibility and robustness against various possible attacks such as noise addition, filtering and geometric attacks etc. For measure of visual quality of watermarking scheme Peak Signal to Noise Ratio (PSNR) is calculated, for calculation of PSNR first the Mean Square Error (MSE) between the original and watermarked frame is computed as follows.

$$MSE = \sum_{i=1}^M \sum_{j=1}^N [I(i,j) - I'(i,j)]^2 \quad (2.96)$$

Where M,N is the size of the frame. $I(i,j)$ & $I'(i,j)$ are the original and watermarked video frame pixel value at location(i,j).

The PSNR is defined by

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (2.97)$$

The red color component of 69 frames of the xylophone video sequence are watermarked. The watermarked frames are of 512×512 frame size. The original sample and the corresponding watermarked sample are as shown in figure. The measured PSNR value is 44.3db and the watermarked frame appears very identical to the original frame. The PSNR value tested for all the frames appears nearly to be a constant value which means that the error between the original and the watermarked frame is very low thus obtaining a high visual quality.



Figure.3.12.(a)



Figure.3.12.(c)



Figure.3.12.(b)



Figure.3.12.(d)

Figure.3.12. (a) & (c) the original frame and corresponding watermarked frame number 25;
 (b) & (d) the original frame and corresponding watermarked frame number 55.

The similarity measure between the original watermark and the extracted watermark is measured by pixel-wise comparison between the original watermark and the extracted watermark and also by using the Normalised correlation which is given by

$$NC = \frac{\sum_i \sum_j W(i,j) W_E(i,j)}{\sqrt{\sum_i \sum_j W(i,j) \sum_i \sum_j W_E(i,j)}} \quad (2.98)$$

Where W & W_E are the original and extracted watermark. The Normalised correlation peak value is 1. i.e the NC value is 1 when the original and the extracted watermarks are identical and zero when if the original and the extracted watermark are different from each other. The

similarity measure between the original video frame and the video frame after watermark is measure using the structural similarity index given as.

$$SSIM = \frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \quad (2.99)$$

where $\mu_x, \mu_y, \sigma_x, \sigma_y$ and σ_{xy} are the local means, standard deviations, and cross-covariance for image X,Y, $C_1=(K_1L)^2$ and $C_2 = (K_2L)^2$ two variables to stabilize the division by weak denominator. L is the dynamic range of the pixel-values.. $K_1=0.01$ and $K_2=0.02$

The table shows the PSNR values and the Bit error of the original video frame and the watermarked frame for the 1st frame.

Parameter	PSNR(dB)	Bit error rate
Video frame (without watermark)	56.62	0.0013
Watermarked video frame	44.37	0.0138

Table.3.1. PSNR and Bit error of Host and watermarked frame.

For measuring the robustness and imperceptibility of the discussed algorithm, some common signal processing operations are applied to the watermarking schemes and check the robustness of the watermarking algorithm in extracting the watermark. DWT and PCA inherits many advantages in resisting attacks in the watermarked frames Figure shows the watermarked video after applying some common signal processing operations.



Figure.3.13.(a)



Figure.3.13.(d)



Figure.3.13.(b)



Figure.3.13.(e)



Figure.3.13.(c)



Figure.3.13.(f)

Figure3.13. (a), (b) & (c) watermarked frame after salt and pepper , poisson, speckle noise attack; (d), (e) & (f) and their corresponding extracted watermarks.



Figure.3.14.(a)



Figure.3.14.(b)



Figure.3.14.(c)



Figure.3.14.(d)



Figure.3.14.(e)



Figure.3.14.(f)

Figure.3.14.(a), (b) & (c) watermarked frame after Gaussian noise, Gaussian filter and cropping attack;(e), (f) & (g) their corresponding extracted watermarks



Figure.3.15.(a)



Figure.3.15.(c)



Figure.3.15.(b)



Figure.3.15.(d)

Figure.3.15. (a) & (b) watermarked frames after gamma-correction and histogram-equalisation attack; (c) & (d) their corresponding extracted watermarks.



Figure.3.16.(a)



Figure.3.16.(b)

Figure.3.16. (a) watermarked frame after mean filtering attack; (b) its corresponding extracted watermark.



Figure.3.17.(a)



Figure.3.17.(b)

Figure.3.17. (a) watermarked frame after median filter attack, (b) its corresponding extracted watermark.

Attacks	Extracted watermark	
	PSNR	NC
Salt & Pepper Noise(0.01)	35.22	0.9186
Poisson Noise	37.57	0.9584
Speckle Noise(0.01)	35.87	0.9638
Gaussian Noise(0.001)	39.01	0.9765
Gaussian Filter[2 2]	42.16	0.9620
Median Filter[2 2]	37.04	0.8825
Mean Filter[2 2]	37.21	0.9620
Gamma-Correction	38.52	0.9928
Histogram-Equalisation	37.39	0.8011
Cropping(10%)	35.75	0.9641

Table.3.2. Shows the value of the data collected from extracted watermark after performing various attacks.

It is found that the proposed scheme is robust against various attacks like the poisson noise , speckle noise, Gaussian noise, salt and pepper noise, median filtering, mean filtering ,

Gaussian filtering, gamma-correction, histogram-equalisation, Cropping, contrast-stretching. It is observed that the proposed scheme shows great robustness against earlier DWT based schemes. The plot of the proposed scheme against various attacks are shown in figure .

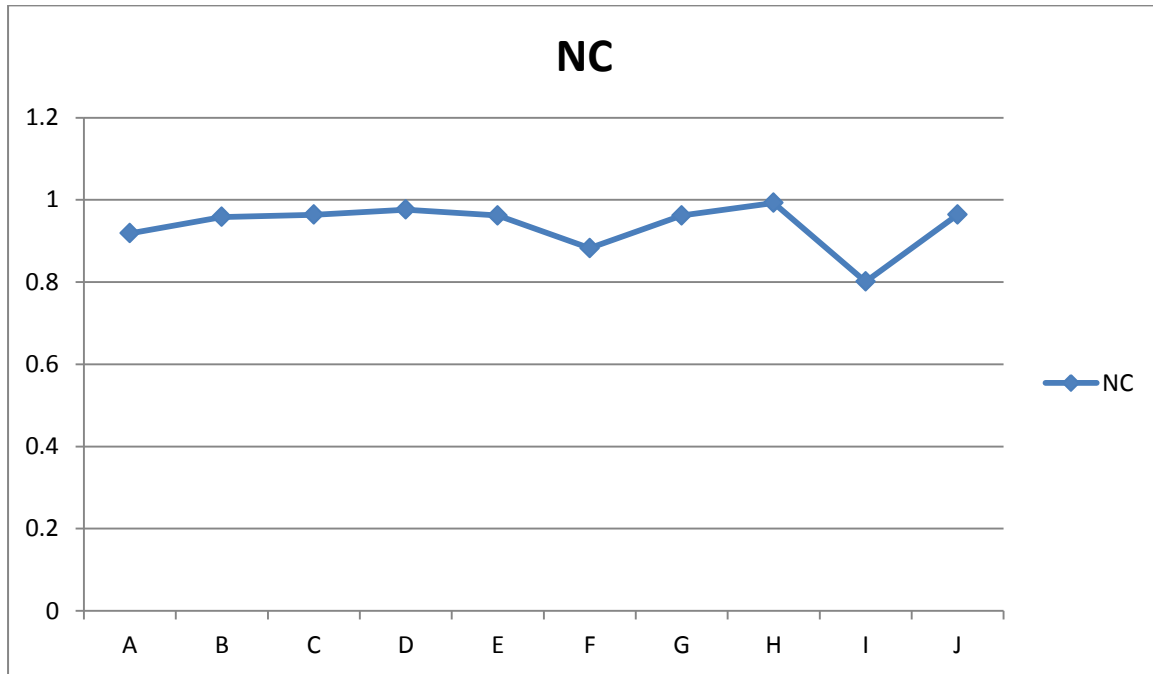


Figure.3.18. Result analysis of various attacks on Watermarked Video Frame of proposed scheme.

In figure the notation used A as salt and pepper noise attack, B as Poisson noise attack, C as Speckle noise attack, D as Gaussian noise, E as Gaussian filter attack, F as Median filter attack, G as mean filter, H as Gamma-correction attack, I as Histogram-equalisation attack, J as Cropping attack.

3.4 Comparison and Discussion

The proposed watermark has been compared to a number of algorithms such as 1). Embedding the watermark only on the DWT coefficients of the host video frame, 2). Applying Principal component analysis on the watermark before embedding on the discrete wavelet transform coefficients of the Host video frame and 3). Applying Principal component analysis on the watermark before applying on the Principal component coefficients of the host video frame. Also some work has been done to the proposed scheme for allowing to work with color watermark by putting Principal component analysis on the watermark embedding procedure and the result were being compared with the those where the

watermark is embedded only on the discrete wavelet components. The brief description of the algorithms are discussed in depth below.

Algorithm1.

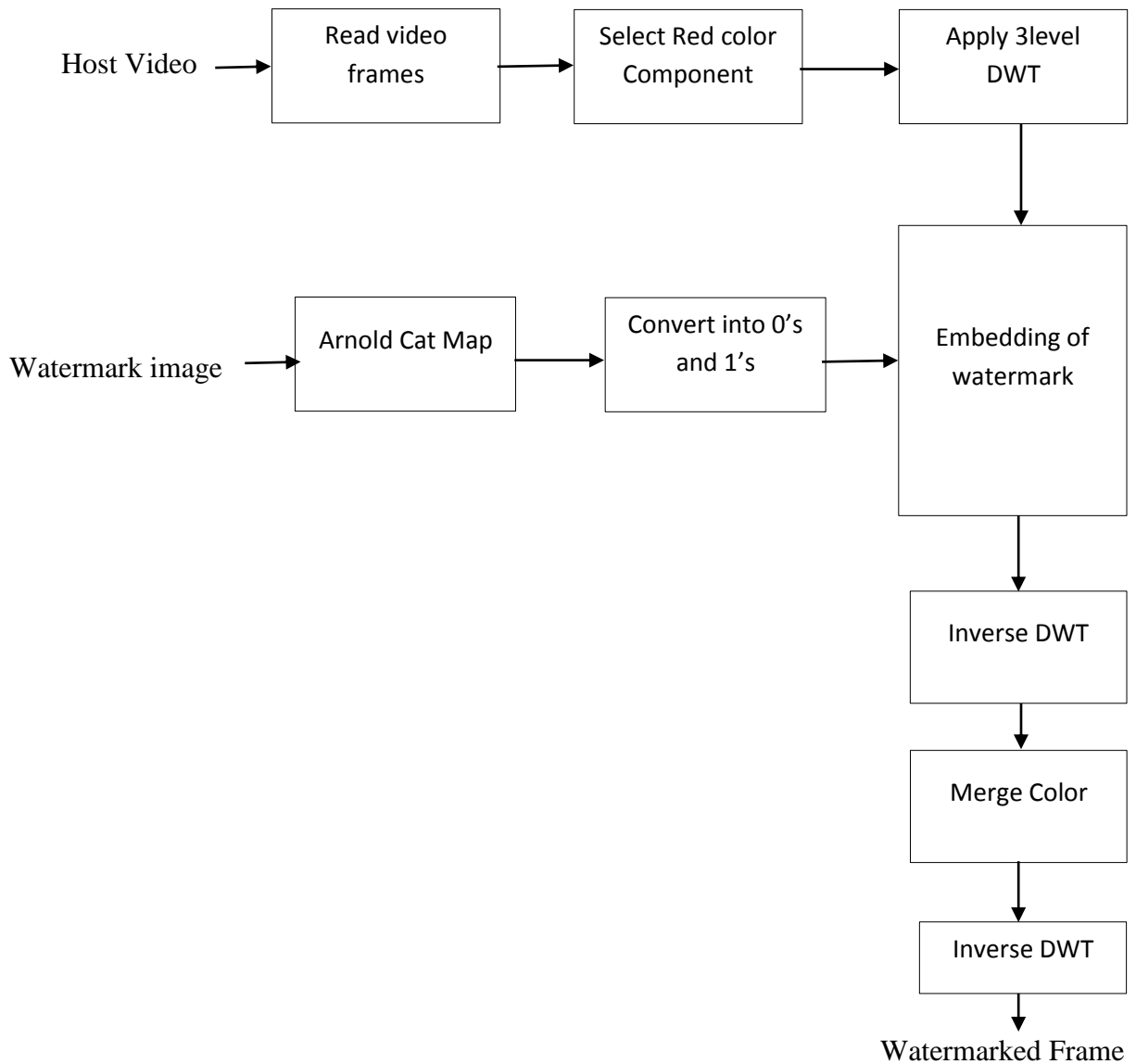


Figure.3.19. Embedding Flowchart using only DWT on Host video frame

Watermark embedding Algorithm

Step1. Read the video frames and select the red component for embedding the watermark.

Step2. Apply 3 level DWT on the Red component of the video frame select HH_{34} subband for embedding watermark.

Step3. Read the binary watermark image.

Step4. Apply Arnold Cat Map on the binary image.

Step5. The watermark bits is inserted on the discrete wavelet coefficients as.

$$cH' = cH + \alpha.W$$

where cH is the wavelet coefficient obtained after apply 3 level DWT . α is the embedding strength and W is the watermark bit obtained after scrambling. cH' is the modified wavelet coefficient.

Step6. Apply inverse 3 level DWT

Step7. Merge color component to obtain the watermarked frame.

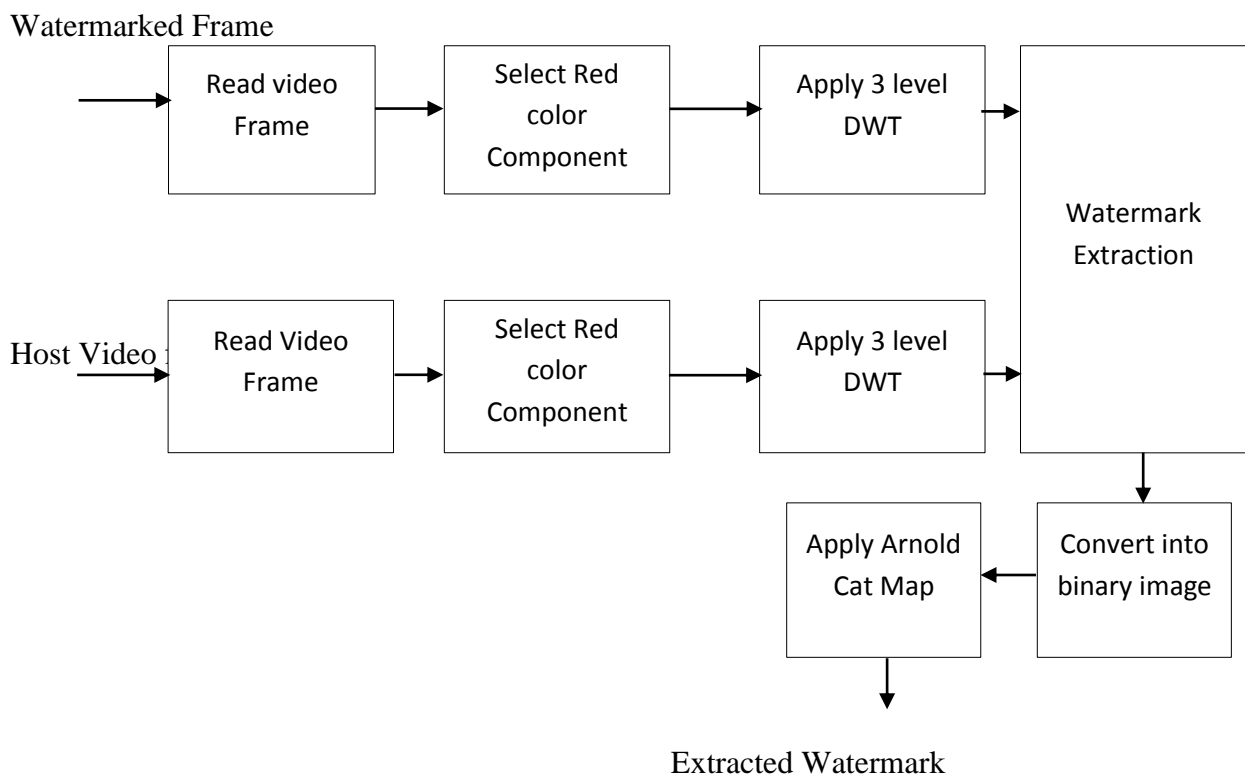


Figure.3.20. Extraction Flowchart for watermarking using only DWT on Host video
Watermark

Extraction Algorithm

Step1. Read the watermarked Frame and select the Red color component for extraction.

Step2. Apply 3 level DWT on the Red color Component and select HH_{34} sub band for extraction.

Step3. The watermark bits is extracted by as

$$W' = (cH_w - cH) / \alpha.$$

Where cH_w is the Discrete wavelet coefficient obtained after applying 3 level DWT. And cH is the Discret Wavelet coefficient of the Host video frame.

Step4. Apply Arnold Cat map to the extracted watermark bits to obtain the watermark image.

Algorithm 2.

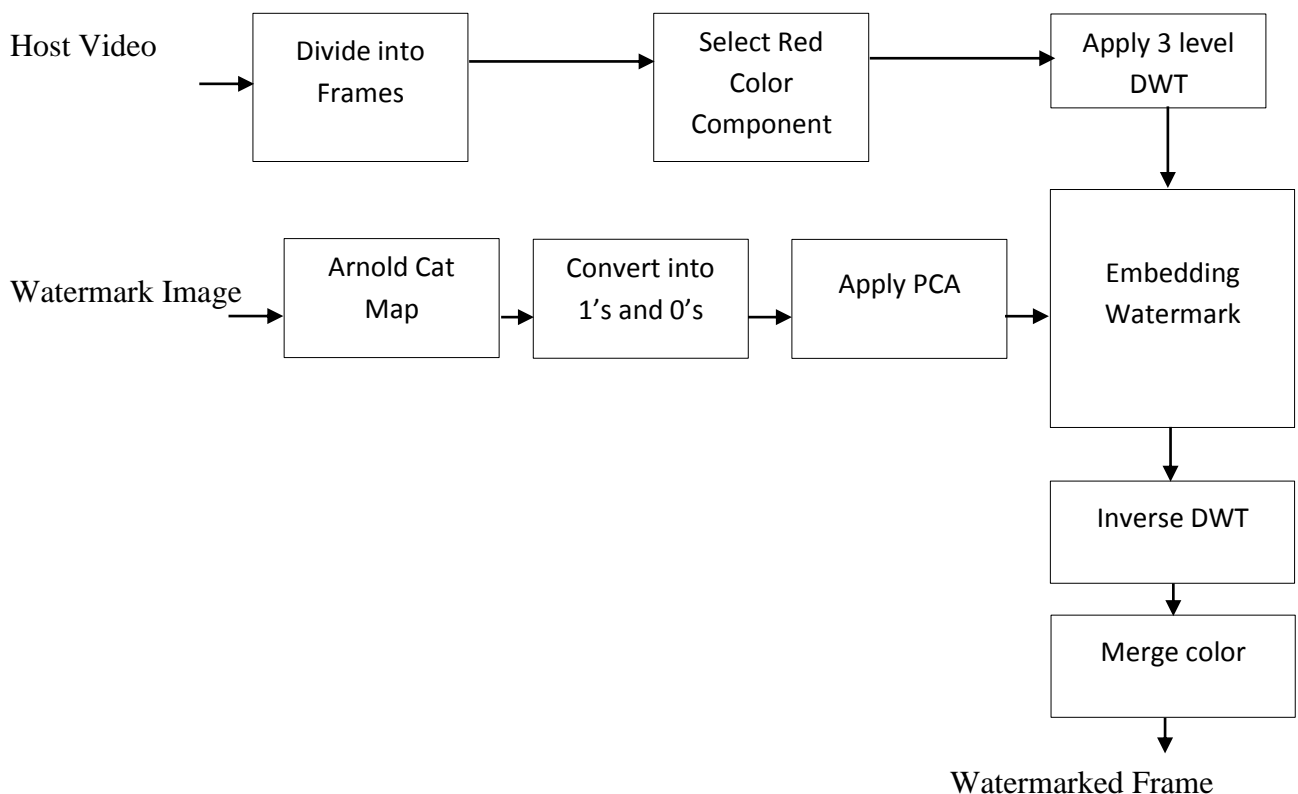


Figure.3.21. Embedding Flowchart for watermarking using only DWT on Host video frame and PCA on binary watermark

Watermark embedding Procedure

Step1. Read the video frame and select Red color component for embedding.

Step2. Apply 3 level DWT to the Red component of the video frame and select HH_{34} sub band for watermark insertion.

Step3. Read the binary Watermark.

Step4. Apply Arnold Cat map to watermark image and convert it into 0's and 1's.

Step5. Apply PCA on the scrambled watermark bits.

Step6. The watermark bits is embedded into the Discrete wavelet coefficients as

$$cH' = cH + \alpha \cdot W_{Pca}$$

where cH is the wavelet coefficient after 3 level DWT, W_{Pca} is the principal components after applying PCA in scambled watermark bits and α is the embedding strength.

Step7. Apply inverse 3 level DWT

Step8. Merge color to obtain the watermarked frame.

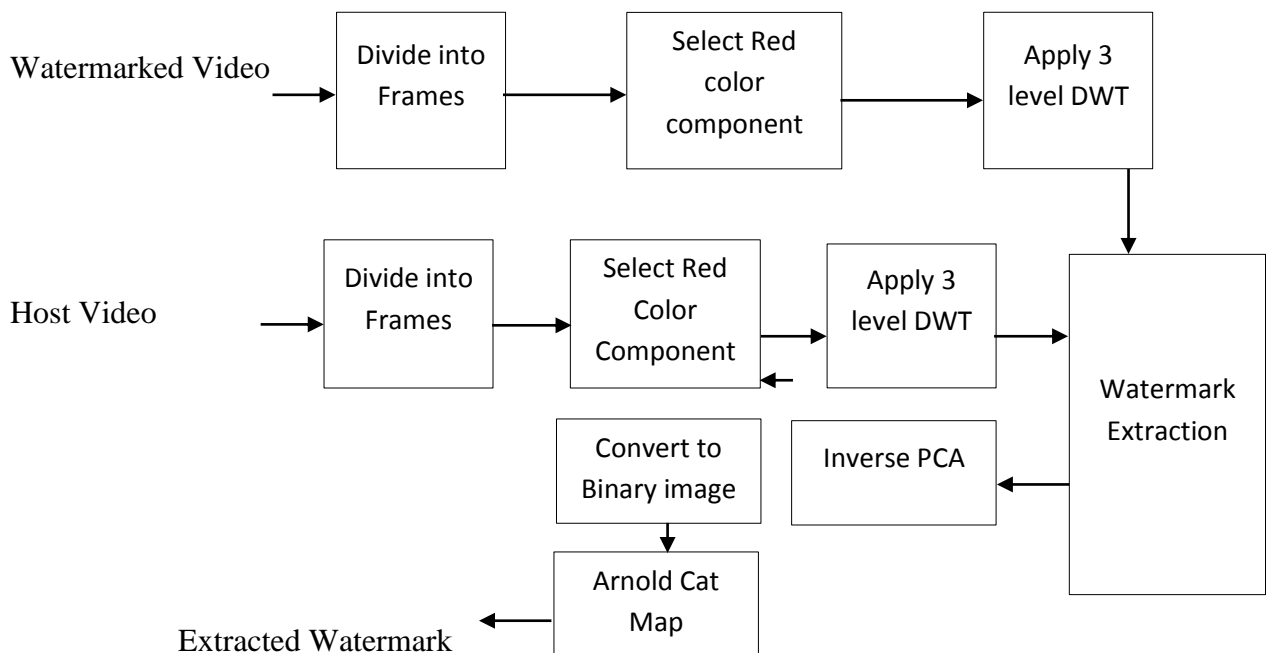


Figure.3.22. Extraction Flowchart for watermarking using only DWT on Host video frame and PCA on binary watermark.

Extraction algorithm

Step1. Read the watermarked frame and select the red color component for watermark extraction.

Step2. Apply 3 level DWT on the red color component and select the HH₃₄ sub band for watermark extraction.

Step3. The watermark bits is extracted using the equation as

$$W'_{PCA} = (cH_w - cH) / \alpha.$$

Where cH_w is the coefficient obtain after DWT on the watermarked frame and cH is the coefficient obtain after DWT on the original video frame.

Step4. Apply inverse PCA.

Step5. Convert the extracted watermark into binary image.

Step6. Apply Arnold cat map to obtain the watermark image.

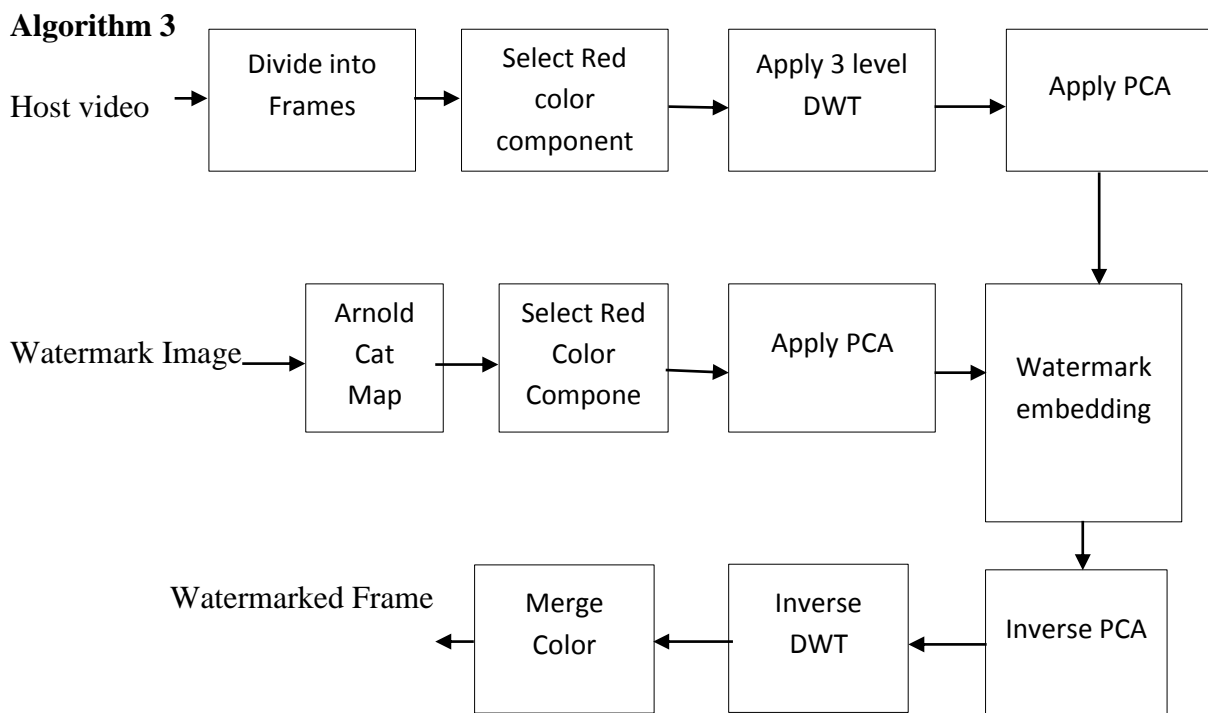


Figure.3.23. Embedding Flowchart for watermarking using both DWT and PCA in host video frame and only PCA in binary watermark.

Watermark embedding procedure

Step1. Read the Video Frames and select red color component for watermark insertion.

Step2. Apply 3-level Dwt on the red color component .

Step3. Apply PCA on the HH_{34} sub-band .

Step4. Read the binary watermark and convert it into 0's and 1's.

Step5. Apply Arnold Cat Map on the watermark image.

Step6. Apply PCA on the scrambled watermark image.

Step7. The watermark bits are inserted using the equation

$$PCA' = PCA + \alpha.W_{Pca}.$$

Where PCA' is the modified Principal components and PCA is the principal components obtain after applying PCA on the HH_{34} sub-band. α is the embedding strength.

Step8. Apply inverse PCA on the modified Principal components.

Step9. Apply inverse DWT on the obtained.

Step10. Merge the color component to obtain the watermarked frame.

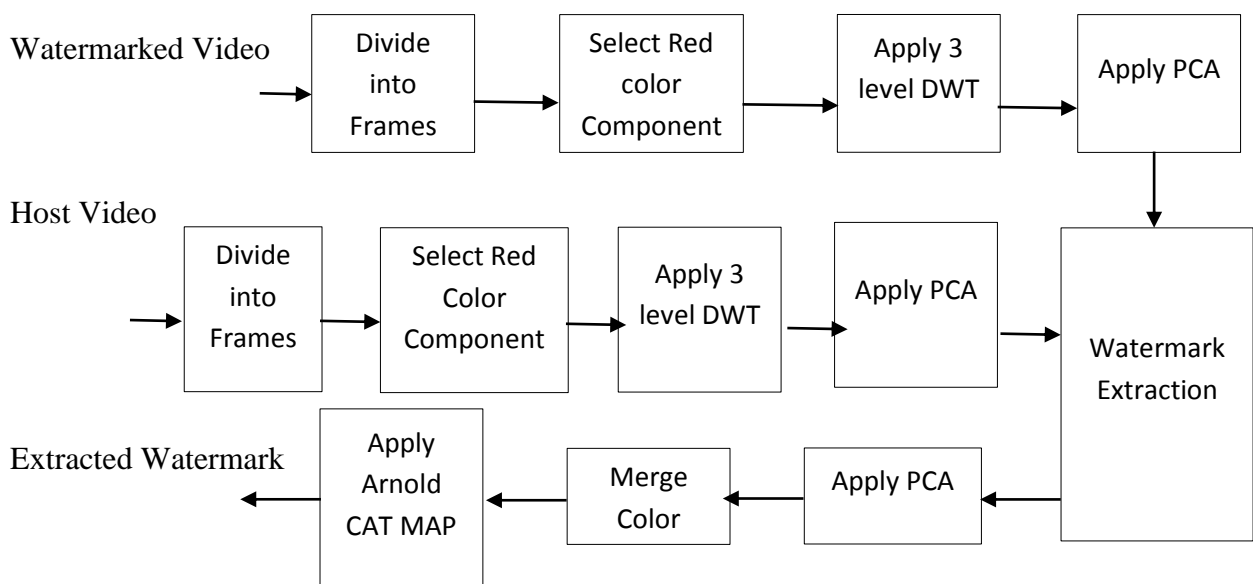


Figure.3.24. Extraction Flowchart for watermarking using both DWT and PCA in Host video frame and only PCA in binary watermark.

Extraction Procedure

Step1. Read the watermarked video frame and select the red color component for watermark extraction.

Step2. Apply 3 level DWT on the red color component and select the HH₃₄ sub band for watermark extraction.

Step3. Apply PCA on the HH₃₄ sub band and obtain the principal component PCA_w.

Step4. The watermark bit are extracted using the equation

$$W'_{pca} = (PCA_w - PCA) / \alpha.$$

Where PCA_w is the Principal component obtained after applying PCA on the watermarked frame. And PCA is the Principal components of the original Video frame.

Step5. Apply inverse PCA on the extracted watermark bits.

Step6. Convert the bits into binary image and apply Arnold Cat map to obtain the watermark image to obtain the extracted watermark.

Algorithm for color watermark is also proposed. The algorithm that were tested for color watermark is as given below. Algorithm 4 is used to embed the color watermark in the wavelet coefficients and Algorithm 5 is used to embed the color watermark in the principal components of the wavelet coefficients. The algorithm is discussed in depth in the following

Algorithm 4.

Embedding Procedure

Step1. Read the video frame and select the red color component for insertion of watermark.

Step2. Apply 3 level DWT on red color component and select the HH₃₄ sub band for insertion of watermark.

Step3. Read the color Watermark image

Step4. Apply Arnold Cat Map to the watermark image

Step5. Extract the blue color component and apply PCA .

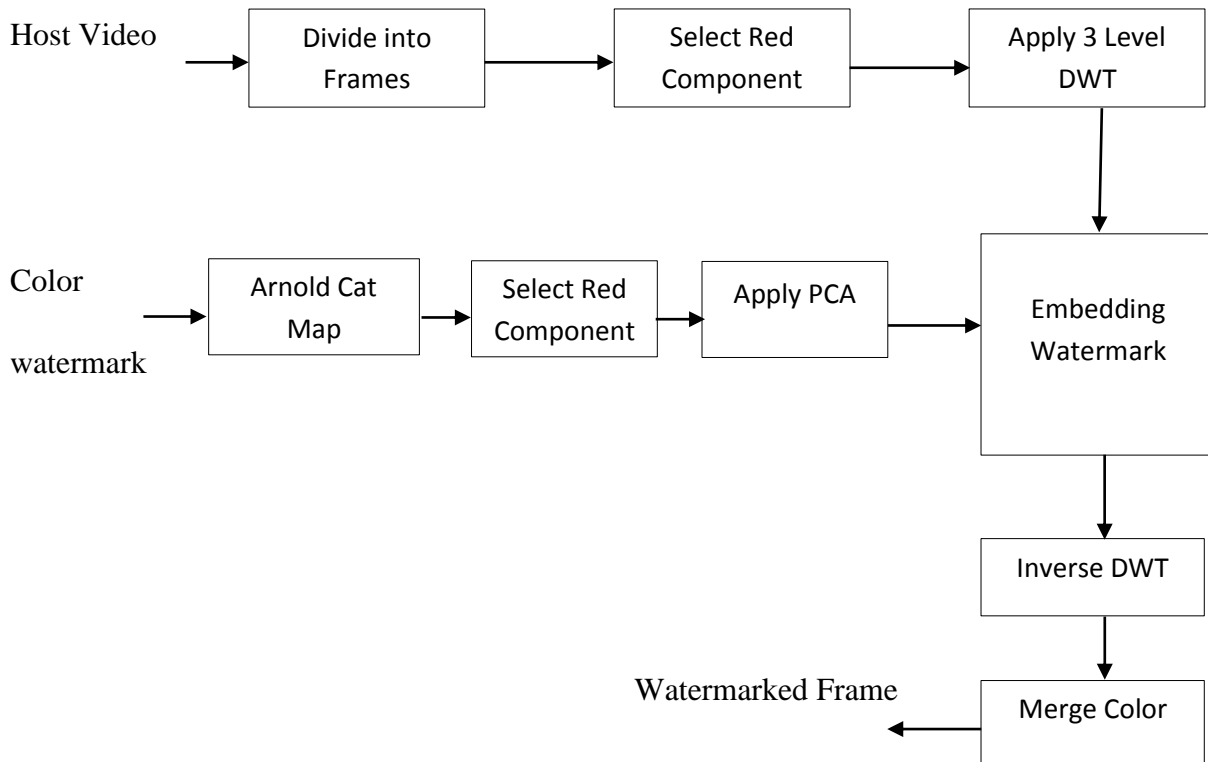


Figure.3.25. Embedding Flowchart for watermarking using only DWT in Host video frame and PCA in RGB watermark

Step6. The principal components of the watermark image is embedded into the discrete wavelet coefficient using the equation

$$cH' = cH + \alpha \cdot W_{Pca}.$$

Where cH is the discrete wavelet coefficient and cH' is the modified discret wavelet coefficient and W_{Pca} is the principal components of the watermark image. α is the embedding strength.

Step7. Apply inverse DWT on the modified cH' sub band.

Step8. Merge color component to obtain the watermarked video frame.

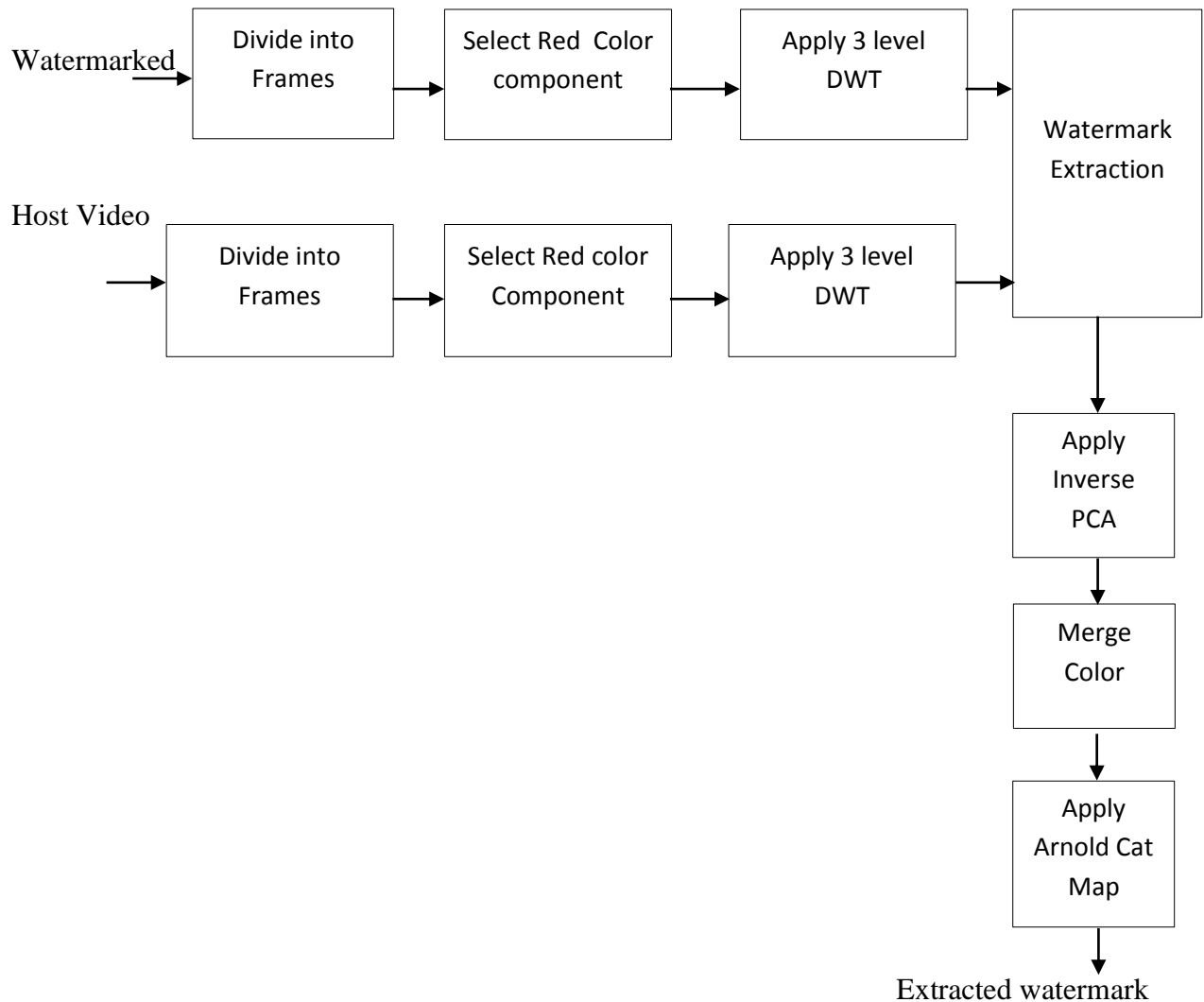


Figure.3.26 Extraction Flowchart for watermarking using only DWT on host video frame and

Extraction Procedure

Step1. Read the watermarked video frame and select the red color component for watermark extraction.

Step2. Apply 3 level DWT on the red color component and select the HH_{34} sub band for extraction of watermark.

Step3. The watermark is extracted using the following equation

$$W'_{Pca} = (cH_w - cH)/\alpha.$$

Step4. Apply inverse PCA on the extracted Principal components.

Step5. Merge the color component and apply Arnold cat map to obtain the watermark image.

Algorithm 5 (Proposed Technique)

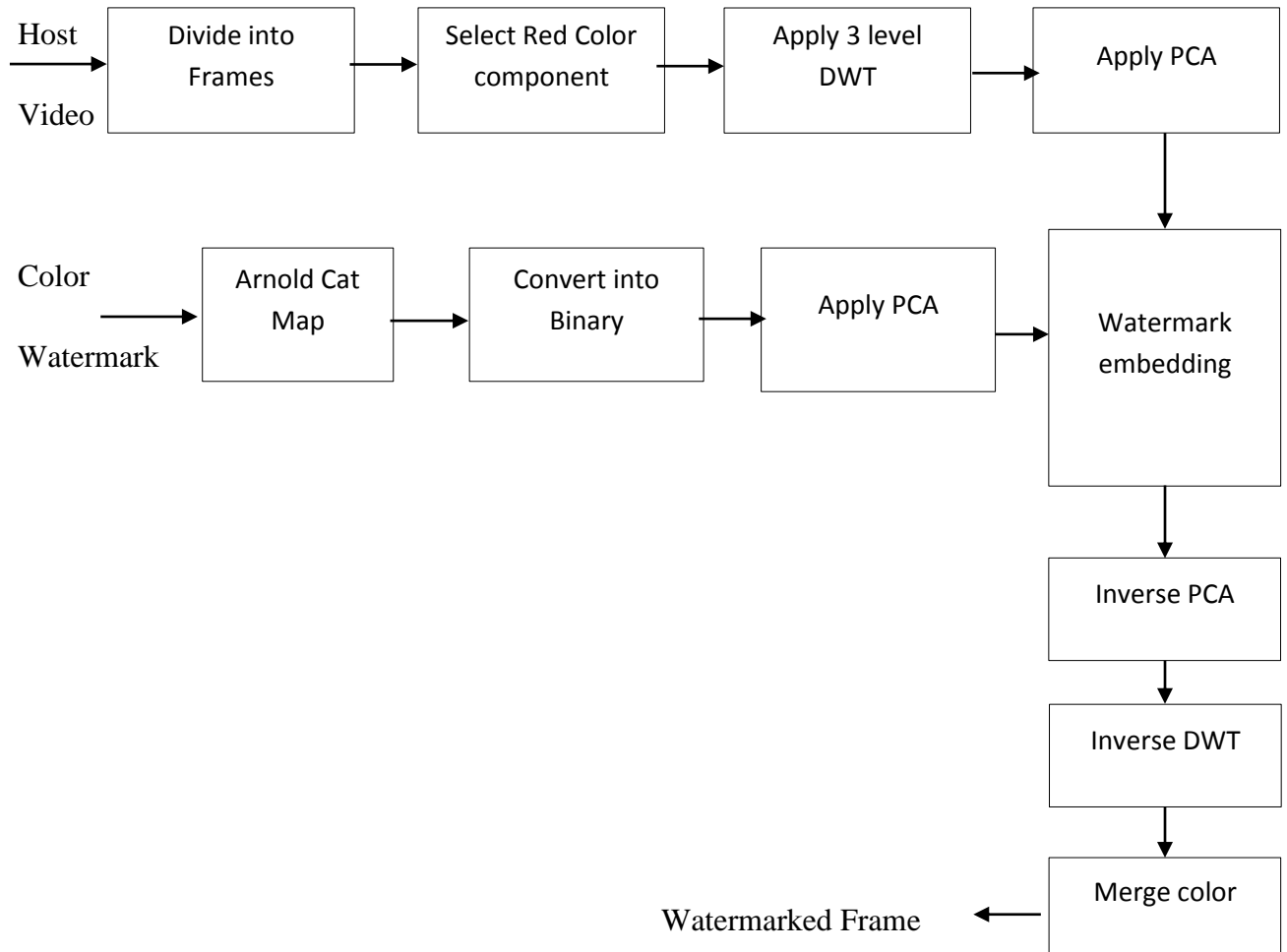


Figure.3.27. Embedding Flowchart for watermarking using both PCA and DWT in Host video image and only PCA for RGB watermark.

Embedding Procedure

Step1. Read the video frame and select the red color component for insertion of watermark .

Step2. Apply 3 level DWT on red color component and select the HH₃₄ sub band for insertion of watermark.

Step3. Apply PCA on the HH₃₄ sub band to obtain the principal components.

Step4. Read the color Watermark image

Step5. Apply Arnold Cat Map to the watermark image

Step6. Extract the blue color component and apply PCA .

Step7. The principal components of the watermark image is embedded into the principal components of the original video frame using the equation

$$PCA' = PCA + \alpha \cdot W_{Pca}.$$

Where PCA is the principal components of the original video frame and PCA' is the modified Principal components and W_{Pca} is the principal components of the watermark image. α is the embedding strength.

Step8. Apply inverse PCA on the modified principal components.

Step9. Apply inverse DWT on the modified CH' sub band.

Step10. Merge color component to obtain the watermarked video frame.

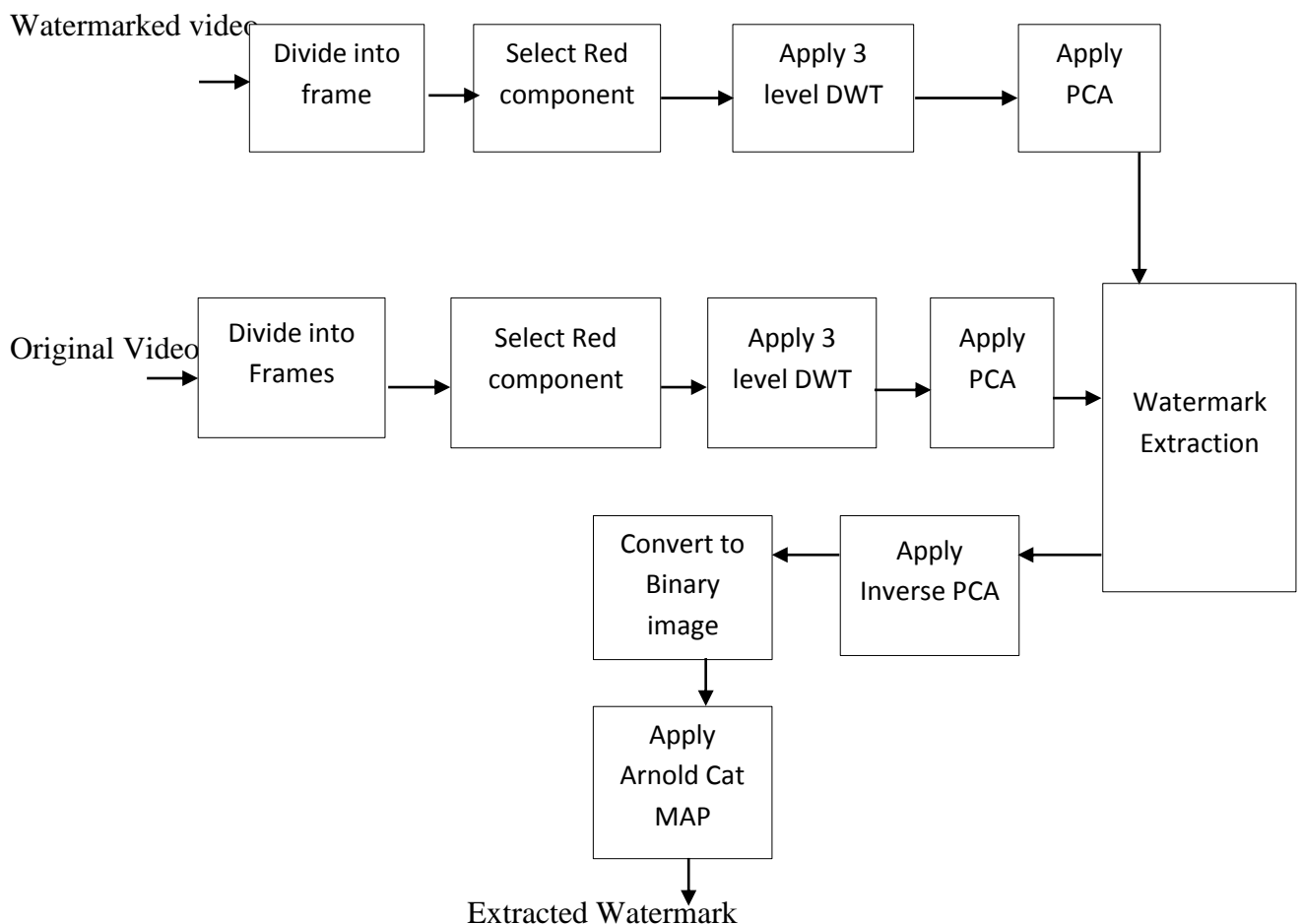


Figure.3.28. Extraction Flowchart for watermarking using Both DWT and PCA in Host video frame and only PCA for RGB watermark.

Extraction procedure

Step1. Read the watermarked video frame and select the red color component for watermark extraction.

Step2. Apply 3 level DWT on the red color component and select the HH_{34} sub band for extraction of watermark.

Step3. Apply PCA on the HH_{34} sub band to obtain the principal components.

Step4. The watermark is extracted using the following equation

$$W'_{Pca} = (PCA_w - PCA)/\alpha.$$

Where PCA_w is the principal components of the watermarked frame and PCA is the principal components of the host video frame, α is the embedding strength.

Step5. Apply inverse PCA on the extracted Principal components.

Step6. Merge the color component and apply Arnold cat map to obtain the watermark image.

For the color watermark algorithm same video sequence 'Xylophone.avi' and color watermark 'color_watermark.jpg' is used which is of dimension 32×32 . the video frame and the color watermark is as shown in figure.



Figure.3.29. Video Frame



Figure.3.30. Color Watermark

Comparison between the algorithms

Attacks	Bit error			
	Proposed	Algorithm 1	Algorithm 2	Algorithm 3
Salt & Pepper noise(0.001)	0.0079	0.0107	0.0225	0.0098
Salt & Pepper Noise(0.01)	0.0615	0.1250	0.2063	0.1025
Poisson Noise	0.0225	0.2432	0.2280	0.0586
Speckle Noise(0.001)	0.0137	0.7627	0.0371	0.0291
Speckle Noise(0.01)	0.0332	0.2539	0.2329	0.0732
Gaussian Noise(0.001)	0.0049	0.2510	0.1672	0.0273
Gaussian Noise(0.01)	0.1877	0.3145	0.3936	0.2471
Gaussian Filter [2 2]	0.0303	0.1094	0.1028	0.0488
Gaussian Filter [3 3]	0.0078	0.0527	0.0090	0.0081
Gaussian Filter [5 5]	0.0079	0.0547	0.0100	0.0090
Median Filter [2 2]	0.0771	0.1063	0.1040	0.1387
Median Filter [3 3]	0.2309	0.3398	0.1484	0.0557
Median Filter [5 5]	0.3964	0.4287	0.3457	0.2832
Mean Filter [2 2]	0.0303	0.1094	0.1028	0.0488
Mean Filter [3 3]	0.4275	0.4600	0.4277	0.4092
Mean Filter [5 5]	0.4575	0.5706	0.4707	0.4756
Gamma-Correction	0.0020	0.2070	0.0052	0.0003
Histo-Equalisation	0.0527	0.2285	0.0420	0.0334
Cropping(10%)	0.0020	0.1709	0.2161	0.0031
Cropping(20%)	0.0743	0.1094	0.0859	0.8083

Cropping (30%)	0.1495	0.3359	0.3291	0.9801
----------------	--------	--------	--------	--------

Table.3.3. Bit error for binary watermark

Attacks	Proposed Method	Algorithm 1	Algorithm 2	Algorithm 3
Salt & Pepper Noise(0.001)	0.9927	0.9893	0.9783	0.9901
Salt & Pepper Noise(0.01)	0.9440	0.7345	0.8192	0.8900
Poisson Noise	0.9754	0.8915	0.8011	0.9494
Gaussian Noise(0.001)	0.9898	0.8021	0.8373	0.9711
Gaussian Noise(0.01)	0.8373	0.6855	0.5895	0.7251
Speckle Noise(0.001)	0.9934	0.7627	0.9602	0.9168
Speckle Noise (0.01)	0.9601	0.6503	0.7396	0.9582
Gaussian Filter[2 2]	0.9788	0.9500	0.9024	0.9450
Gaussian Filter [3 3]	0.9927	0.9473	0.9901	0.9921
Gaussian Filtering [5 5]	0.9934	0.9453	0.9845	0.9910
Mean Filtering [2 2]	0.9788	0.7890	0.9024	0.9458
Mean Filtering [3 3]	0.6136	0.5908	0.5696	0.5823
Mean Filing [5 5]	0.5600	0.4600	0.4919	0.5081
Median filtering [2 2]	0.9125	0.7634	0.8499	0.8300
Median Filtering [3 3]	0.7621	0.6602	0.7089	0.7589
Median Filtering [5 5]	0.3964	0.5713	0.6438	0.6949
Histogram equalisation	0.9024	0.7715	0.9446	0.9538
Gamma Correction	0.9982	0.7930	0.9821	0.9993
Cropping(10%)	0.9643	0.8402	0.8205	0.9403
Cropping(20%)	0.9287	0.8906	0.8879	0.9012
Cropping(30%)	0.8503	0.6641	0.6420	0.8083

Table.3.4. Normalised correlation for binary watermark

Attacks	RGB watermark with PCA on watermark and only DWT on Host Video frames	RGB watermark with PCA on watermark and Both PCA and DWT on Host Video
Salt and Pepper Noise(0.01)	.9588	.9634
Salt and Pepper noise(0.001)	.9597	.9660
Poisson	.9599	.9621
Gaussian noise(0.01)	.9724	.9845
Gaussian noise(0.001)	.9585	.9839
Speckle noise(0.001)	.9595	.9636
Speckle noise(0.01)	.9598	.9636
Gaussian filtering [2 2]	.9439	.9589
Gaussian Filtering [3 3]	.9505	.9590
Gaussian Filtering [5 5]	.9505	.9591
Mean Filtering [2 2]	.9439	.9589
Mean Filtering [3 3]	.9424	.9589
Mean Filtering [5 5]	.9428	.9590
Median Filtering[2 2]	.9440	.9589
Median Filtering [3 3]	.9426	.9590
Median Filtering [5 5]	.9420	.9589
Histogram equalisation	.9594	.9681
Gamma Correction	.9589	.9614
Cropping(10%)	.9590	.9606
Cropping(20%)	.9591	.9602
Cropping(30%)	.9592	.9631
Rotation (10°)	.9501	.9590
Rotation (20°)	.9492	.9590
Rotation (30°)	.9483	.9633

Table.3.5. Normalised correlation for color watermark

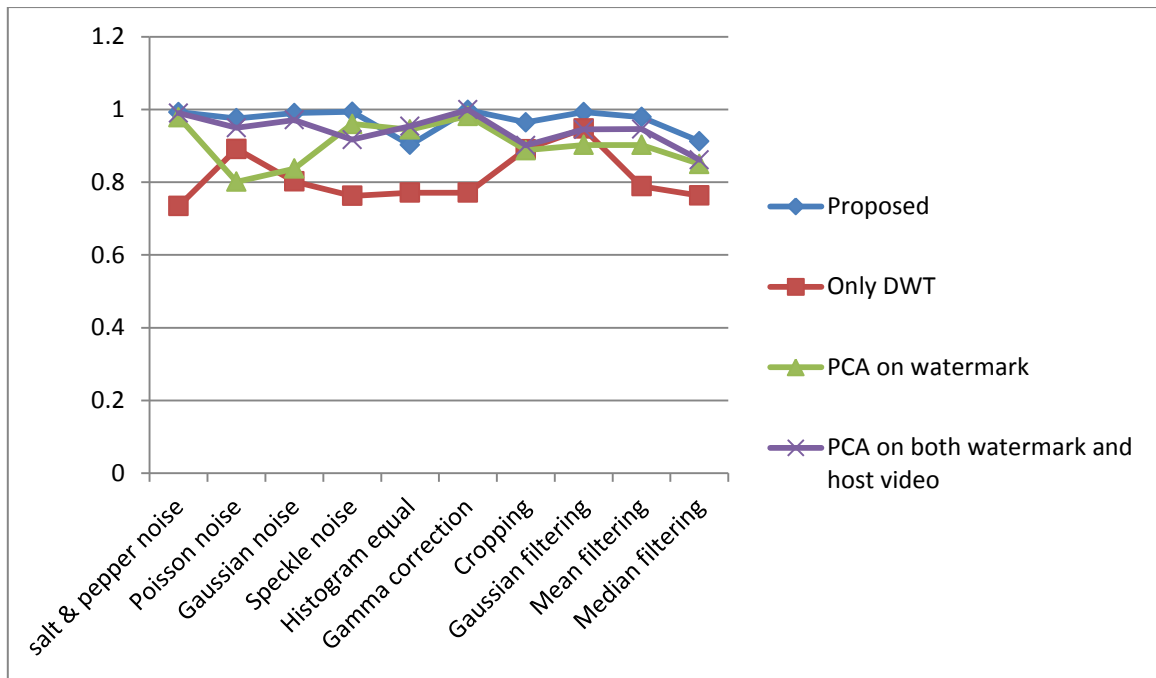


Figure.3.31. Analysis between the proposed technique in terms of NC with other techniques for binary watermark.

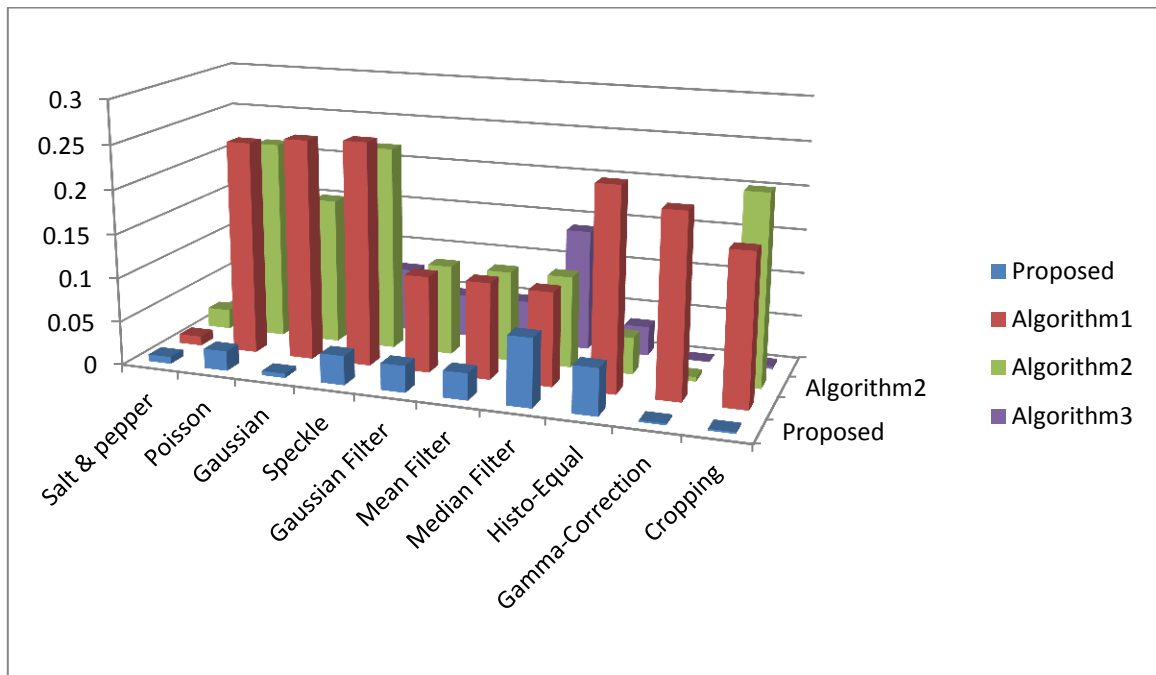


Figure.3.32. Analysis between the proposed technique in terms of bit error with other techniques for binary watermark.

CHAPTER 4

CONCLUSION

Conclusion

Future Work

Chapter-4

4.1 Conclusion

The proposed algorithm shows great robustness over some common signal processing attacks such as the Poisson noise attack, Gaussian Noise attack, Speckle noise attack, Salt and Pepper noise attack, Gaussian filtering attack, Median filtering attack, Mean filtering attack, Gamma-correction attack, Histogram Equalisation attack, Cropping attack. It is also observed that the algorithm produce a higher visual quality than that of earlier two level DWT.

It was observed that the proposed scheme provides a higher level of robustness against noisy attacks as compared to that where watermark bits are embedded on the discrete wavelet coefficients. It is also observed that a greater level of similarity measure is achieved after filtering operations like Gaussian, mean and median by using a transform (PCA) in the watermark before embedding than those without transform. The proposed scheme can also be used for color watermark by inserting a transform in the watermark before embedding, its performance measure has been compared to that scheme where the color watermark is embedded directly on the discrete wavelet coefficient. For signal processing operation like gamma correction and histogram equalisation and geometric attack like cropping using a transform (PCA) before watermark insertion and applying both DWT and PCA in the host video frame gives a much better similarity measure than the other algorithms.

The proposed method for color watermark has a higher robustness than that of the algorithm where the watermark is embedded on the wavelet coefficients. It was found that for color watermarking, we can obtain recognizable watermark even after rotation attack.

The algorithm is also robust from the attacker who aims remove watermark by exploiting the knowledge of the watermarking algorithm because of the non-blind algorithm and by using Arnold Cat Map scrambling technique. Since, even if the attackers manage to extract the watermark bits it will be difficult for them to get a readable form of the watermark image without the knowledge of the scrambling key. The computation of the algorithm is simple and compact. And the proposed watermarking scheme is simple for extraction of watermark as there is no need for transform of original watermark in the extraction process. Hence we conclude that the proposed watermarking scheme is a simple and better watermarking system both in terms of imperceptibility and robustness.

4.2 FUTURE WORK

The discussed watermarking algorithm for the binary watermark is not robust to rotation attack. We can extend this work by developing new watermarking algorithms which are robust to rotation attack for binary watermark. For rotation attack shift invariant wavelet can be used to provide robustness against rotation attack. Also we can exploit the knowledge of 3-D PCA for getting more efficient results. Future work can also concentrate on making hybrid watermarking methods i.e. for both video and audio, using some complex wavelet transform and which should be robust to all attacks both geometric and non-geometric attacks. The Daubechies wavelet can be used to increase the level of imperceptibility.

REFERENCES

- [1] M. Barni and F. Bartolini. *Watermarking Systems Engineering*. Marcel Dekker, 2004.
- [2] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker. *Digital Watermarking and Steganography*. Morgan Kaufmann, 2007.
- [3] H. H. Yu, D. Kundur, and C.-Y. Li. Spies, thieves, and lies: The battle for multimedia in the digital era. *IEEE Multimedia*, 8(3):8–12, 2001.
- [4] J. Dittmann, M. Steinebach, P. Wohlmacher, and R. Ackermann. Digital watermarks enabling E-commerce strategies: conditional and user specific access to services and resources. *EURASIP Journal on Applied Signal Processing*, 2002(2):174–184, Feb. 2002.
- [5] I.J.Cox, M.L.Miller, and J.A.Bloom. *Digital watermarking*. Morgan Kaufmann Publisher, October 2001.
- [6] U. Kohl, J. Lotspiech, and M. A. Kaplan. Safeguarding digital library content and users: Protecting documents rather than channel. <http://www.dlib.org/dlib/september97/ibm/09lotspiech.html>, 1997.
- [7] J.Lacy, S. Quackenbush, A.Reibman, and J.Snyder. Intellectual property protection and digital watermarking. In *information Hiding, Second International workshop Proceedings*, volume 1525, pages 158–168, April 1998.
- [8] J. Linnartz, T. Kalker, and J.Haitsma. Detecting electronic watermarks in digital video. In *Proc.IEEE ICASSP*, pages 2071–2074, March 1999.
- [9] J.A. Bloom, I.J.Cox, T.Kalker, J.Linnartz, and M.L. Miller. Copy protection for dvd video. *Proceeding of the IEEE*, 87(7):1267–1276, July 1999.
- [10] R.B. Wolfgang and E.J.Delp. Fragile watermarking using the vw2d watermark. In *Proc. Electronic Imaging'99*, pages 204–213, January 1999.
- [11] C–Y.Lin and S.F.Chang. A robust image authentication algorithm surviving jpeg compression. In *SPIE: Storage and Retrieval Image/ Video Databases*, January 1998.
- [12] C–Y.Lin and S.F.Chang. A robust image authentication algorithm surviving jpeg compression. In *SPIE: Storage and Retrieval Image/ Video Databases*, January 1999.
- [13] D.L Robie and R.M. Marsereau. Video error correction using stenography. In *Proc. IEEE ICIP*, pages 207–226, October 2001.
- [14] C. I. Podilchuk and W.Zeng. Image-adaptive watermarking using visual models. *IEEE Journal on selected Areas in Communication*, 16(4):525–539, May 1998.

- [15] C. De Vleeschouwer, J.F.Delaigle, and B.Macq. Invisibility and application functionalities in perceptual watermarking- an overview. Proceedings of the IEEE, 90(1):64-77, January 2002.
- [16] S. Voloshynovskiy and S.Pereira and I.T.Pun. Attack modelling: Towards a second generation watermarking benchmark. Signal Processing, 81:1177-1212,2001.
- [17] I.J.Cox, J. Killian, F.T. Leighton, and T.Shannon. Secure Spread Spectrum Watermarking for Multimedia. IEEE Transaction on Image processing, 6(12): 16273-1687, December 1997.
- [18] A.Z.Tirkel, G.A. Rankin, R.van Schyndel, W.J.Ho, N.R.A.Mee, and C.F.Osborne. Electronic watermark. In Proc. Digital Image Computing, Technology and Applications. Pages 666-672, December 1993.
- [19] C.I.Podilchuk and Zeng. Image-adaptive watermarking using visual models. IEEE Journal on selected Areas in communication, 16(4):525-539, May 1998.
- [20] C.Honsinger and Rabbani. Data embedding using phase dispersion. International conference on information Technology: Coding and Computing(Invited paper), April 2000.
- [21] J.R.Hernandez, F.P.Gonzales, J.M. Rodriquez, and G. Nieto. Performance Analysis of a 2D- Multispace Amplitude modulation scheme for data hiding and watermarking n still images. IEEE journal on selected areas in communication, 16(4): 510-524, May 1998.
- [22] J. R. Smith and B.O. Cosmiskey. Modulation and information hiding in images. In information Hiding, First International Workshop Proceeding , pages 207-226. June 1996.
- [23] W. Bender, D.Gruhl, N. Morimoto and A.Lu. Techniques for data hiding. In IBM Systems Journal, Volume 35, pages 313-336,1996.
- [24] J.R. Hernandez, M. Amado, and F.P. Gonzalez. Dct- Domain watermarking techniques for still images: Detector performance analysis and a new structure. IEEE Transaction on Image Processing, 9(1):55-68, January 2000.
- [25] G.C. Langelaar, I.Setyawan, and R.L.Lagendijk. Watermarking digital image and video data: A State of art overview. IEEE Signal Processing Magazine,17(5):20-46, September 2000.
- [26] C.I. Podilchuk and E.J.Delp. Digital Watermarking: Algorithms and Applications. IEEE Signal Processing Magazine,18(4):33-46, July 2001.
- [27] I.J. Cox, M.L.Miller, and A.L.Mckellips. Watermarking as Communications with side information. Proceeding of the IEEE, 87(7):1127-1141, July 1999.

- [28] B.Chen and G.Wornell. Dither modulation: a new approach to digital watermarking and information embedding. In Proc.SPIE: Security and Watermarking of multimedia Contents, pages 342-353, January 1999.
- [29] B.Chen and G. Wornell. Quantization Index Modulation: a class of probably good methods for digital watermarking and information embedding. IEEE Transactions on Information theory, IT-47(4):1423-1443, May 2001.
- [30] Brian Chen. Design and analysis of digital watermarking: information embedding and data hiding systems. PhD dissertation, MIT, Cambridge, June 2000.
- [31] M.H.Costa. Writing on dirty paper. IEEE Transactions and Information Theory, IT-29(3):439-441, May 1983.
- [32] B. Chen and G. Wornell. An information-theoretic approach to the design of robust digital watermarking systems. In Proc. IEEE ICASSP, pages 823-827, April 1999.
- [33] B. Chen and G. Wornell. Preprocessed and post processed quantization index modulation for digital watermarking. In Proc.SPIE: Security and watermarking of multimedia Contents, pages 48-59, January 2000.
- [34] J. Eggers and B. Girod. Quantization effects in digital watermarking. Signal Processing, 81(2):239-263, February 2001.
- [35] J. Eggers and B. Girod. Informed watermarking. Kluwer Academic Publishers, 2002.
- [36] M.L Miller, G.Doerr, and I.J. Cox. Dirty –paper trellis codes. In Proc. IEEE ICIP, pages 129-132, September 2002.
- [37] P.Moulin and J.A. O’sullivan. Information-theoretic analysis of information hiding. Preprint, 1999.
- [38] J. Eggers and B. Girod. Informed watermarking. Kluwer Academic Publishers, 2002
- [39] P. Moulin, M.K. Mihcak, and G.I.A.Lin. An information theoretic model for image watermarking and data hiding. In Proc. IEEE ICIP, September 2000.
- [40] Van Schyndel, R.G., Tirkel, A.Z., and Osborne, C.F., “A digital Watermark.” Proc. of the IEEE Int. Conference on Image Processing. Vol. 2, (1994): pp. 86-90.
- [41] Craver, S., Memon, N., Yeo, B.-L., and Yeung, M.M., “Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications.” IEEE Journal On Selected Areas in Communications. Vol. 16, No. 4, (May 1998): pp. 573-586.
- [42] A. C. Popescu and H. Farid. Exposing digital forgeries in color filter array interpolated images. IEEE Transactions on Signal Processing, 53(10):3948–3959, Oct. 2005.
- [43] M. Chen, J. Fridrich, M. Goljan, and J. Lukas. Determining image origin and integrity

using sensor noise. *IEEE Transactions on Information Security and Forensics*, 3(1):74–90, Mar.2008.

[44] J. Fridrich. *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge University Press, Nov. 2009.

[45] T. Kalker, J. Haitzma, and J. Oostveen. Issues with digital watermarking and perceptual hashing. In *Proceedings of SPIE, MediaWatermarking Technology I*, volume 4518, pages 189–197, Denver, CO, USA, Aug. 2001. SPIE.

[46] Haar A. Zur theorie der orthogonalen Funktionssysteme. *Math Annal* 1910;69:331–71.

[47] Castleman KR. *Digital image processing*. Englewood Cliffs: Prentice-Hall; 1996.

[48] Moharir PS. *Pattern recognition transforms*. New York: Wiley; 1992.

[49] Falkowski BJ, Chang CH. Calculation of paired Haar spectra for systems of incompletely specified Boolean functions. *Proc IEEE Int Symp Circ Syst (31st ISCAS)*, vol. VI. Monterey, CA, USA, June 1998. p. 171–4.

[50] Falkowski BJ, Chang CH. Paired Haar spectra computation through operations on disjoint cubes. *IEE Proc Circ Dev Syst* 1999;146(3):117–23.

[51] Falkowski BJ, Chang CH. Efficient algorithm for forward and inverse transformations between Haar spectrum and binary decision diagrams. *Proc 13th Int Phoenix Conf Comput Commun*, Phoenix, AZ, USA, April 1994. p.497– 503.

[52] Falkowski BJ, Chang CH. Forward and inverse transformations between Haar spectra and ordered binary decision diagrams of Boolean functions. *IEEE Trans Comput* 1997;46(11):1272–9.

[53] Hansen JP, Sekine M. Decision diagrams based techniques for the Haar wavelet transform. *Proc IEEE Int Conf Inform, Commun Signal Process (1st ICICS)*, vol. 1. Singapore, September 1997. p. 59–63.

[54] Stankovi_c M, Jankovi_c D, Stankovi_c RS. Efficient algorithm for Haar spectrum calculation. *Proc IEEE Int Conf Inform, Commun Signal Process (1st ICICS)*, vol. 4. Singapore, September 1997. p. 6–10.

[55] Uljanov PL. On series for Haar system. *Math Sb* 1964;3:356–91.