

ROBUST AND IMPERCEPTIBLE COPYRIGHT PROTECTION FOR DIGITAL VIDEOS IN TRANSFORM DOMAIN

A thesis submitted in fulfillment for the requirement for the Degree of

DOCTOR OF PHILOSOPHY

IN

COMPUTER SCIENCE & ENGINEERING

BY

JABIR ALI

(Enrollment No 126206)



Department of Computer Science & Engineering and Information Technology,
Jaypee University of Information Technology, Wahnaghat, Solan–173234,
Himachal Pradesh, INDIA

May 2019

ROBUST AND IMPERCEPTIBLE COPYRIGHT PROTECTION FOR DIGITAL VIDEOS IN TRANSFORM DOMAIN

A thesis submitted in fulfillment for the requirement for the Degree of

DOCTOR OF PHILOSOPHY

IN

COMPUTER SCIENCE & ENGINEERING

BY

JABIR ALI

(Enrollment No 126206)



Department of Computer Science & Engineering and Information Technology,
Jaypee University of Information Technology, Wahnaghat, Solan–173234,
Himachal Pradesh, INDIA

May 2019

TABLE OF CONTENTS

TITLE	PAGE NO
INNER FIRST PAGE	
TABLE OF CONTENTS	I-III
DECLARATION BY SCHOLAR	IV
SUPERVISOR'S CERTIFICATE	V
ACKNOWLEDGEMENT	VI-VIII
ABSTRACT	X-XII
LIST OF ABBRIVIATIONS	XIII-XIV
LIST OF SYMBOLS	XV
LIST OF FIGURES	XVI-XVIII
LIST OF TABLES	XIX

CHAPTER 1

INTRODUCTION 1-9

1.1 Introduction	1
1.2 Video Watermarking	1
1.2.1 Properties of Video Watermarking	2
1.3 Watermarking Process	2
1.3.1 Application of Watermarking	5
1.4 Video Process	5
1.4.1 Color Video	6
1.5 Problem Identification	7
1.6 Objectives of Thesis	8
1.7 Organization of Thesis	9

CHAPTER 2

REVIEW AND BACKGROUND 10-31

2.1 Introduction	10
2.1.1 Robustness	11

2.1.2 Data Capacity	11
2.1.3 Security	11
2.1.4 Low Error Probability	12
2.2 Natural Video Scene	14
2.3 Capture	16
2.4 Video Watermarking	16
2.5 Frame and field	16
2.6 Spatial Domain	17
2.7 Temporal Domain	18
2.7.1 Discrete cosine transform	20
2.7.2 Discrete wavelet Transform	22
2.7.2.1 Haar Wavelet	23
2.7.2.2 Daubechie Wavelet	25
2.8 Watermark Based on MPEG Structure	25
2.9 Paper Reviewed	27
2.9.1 Compression Domain	27
2.9.2 Spatial Domain	30
2.9.3 Transform Domain	30
2.10 Conclusion	31

CHAPTER 3

A METHOD OF DIGITAL COPYRIGHT PROTECTION BY IMPLEMENTATION OF SWEA FOR DIGITAL VIDEOS **32-48**

3.1 Introduction	32
3.2 Background	37
3.3 Proposed Method	37
3.3.1 SCD (Scene Changed Algorithm)	38
3.3.1.1 Working Process For SCD	38
3.3.2 Watermark Pre-process	38
3.3.3 Embedding Algorithm	39
3.3.4 Detection Algorithm	41
3.4 Experimental Results	41
3.5 Conclusion	48

CHAPTER 4

A DIGITAL VIDEO COPYRIGHT PROTECTION TECHNIQUE ZPA ALONG WITH SWEA **49-61**

4.1 Introduction	49
------------------	----

4.2 Background	49
4.3 Proposed Method	51
4.3.1 SWEA	51
4.3.2 ZPA	53
4.3.3 Embedding Algorithm	54
4.3.4 Detection Algorithm	56
4.4 Experimental Results	56
4.4.1 Combine small Pieces of watermark	58
4.5 Comparative Analysis	60
4.6 Conclusion	60

CHAPTER 5
CWEA: A DIGITAL VIDEO COPYRIGHT PROTECTION
SCHEME **62-80**

5.1 Introduction	62
5.2 Related Work	62
5.2.1 RGB	64
5.2.2 YCbCr	65
5.2.3 YCbCr Color Format	68
5.3 Background	70
5.3.1 Video Watermarking	70
5.3.2 Types of Video watermarking	71
5.4 Proposed Algorithm	72
5.5 Experimental Results	75
5.6 Conclusion	80

CHAPTER 6
CONCLUSION AND FUTURE WORK **81-82**

8.1 Conclusion	81
8.2 Future Work	82

REFERENCES **83-92**

LIST OF PUBLICATIONS **93-94**



JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY

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

Date: 29, May, 2019

DECLARATION

I hereby declare that the work reported in the Ph.D. thesis entitled **“Robust and Imperceptible Copyright Protection for Digital Videos in Transform Domain”** submitted at **Jaypee University of Information Technology, Waknaghat India**, is an authentic record of my work carried out under the supervision of Professor Brig. (Retd.) Satya Prakash Ghrera. I have not submitted this work elsewhere for any other degree or diploma.

(Signature of the Scholar)

Jabir Ali

Department Of Computer Science & Engineering and Information Technology

Jaypee University of Information Technology, Waknaghat, India

Date (29, May, 2019)



JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY

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

Date: 29, May, 2019

CERTIFICATE

This is to certify that the work reported in the Ph.D. thesis entitled “**Robust and Imperceptible Copyright Protection for Digital Videos in Transform Domain**”, submitted by **Jabir Ali** at **Jaypee University of Information Technology, Waknaghat, India**, is a bonafide record of his original work carried out under my supervision. This work has not been submitted elsewhere for any other degree or diploma.

(Signature of Supervisor)

Brig. (Retd.) Satya Prakash Ghrera

Professor

Department Of Computer Science & Engineering and Information Technology

Date (29, May, 2019)

ACKNOWLEDGEMENTS

First of all I thank to Allah, the most beneficent, gracious and merciful who gave me the patience, ability, intelligence and power to accomplish my PhD thesis. This thesis constitutes a fulfillment of the requirements for the Doctor of Philosophy degree at Jaypee University of Information Technology (JUIT), Himachal Pradesh. This thesis is comprised of introduction, methodologies, results analysis, discussion, conclusion and perspective along with my published papers those are belongs to my PhD work. Many people have directly or indirectly involved in my PhD work. So, I would like to especially thank to the following persons.

I would like to express my heart-felt gratitude to my supervisors, **(Professor) Brig. (Retd.) Satya Prakash Ghrrera**, Head of the Department, Computer Science and Engineering and Information Technology, for his inspiring supervision. He has been a constant source of motivation, ideas and guidance. I am highly grateful to him for his rich experience and expertise in various research areas. His positive attitude and zest for quality research always encouraged me and bought the best out of me. Without his persistence I would never have considered doing PhD on such an amazing topic.

I also express my loyal as well as admirable gratitude to JUIT administration, **Prof. Dr. Vinod Kumar** (Vice Chancellor), **Prof. (Dr.) Samir Dev Gupta** (Director & Dean, Academics & Research), **Prof. (Dr) Y. Medury** (Ex-COO Jaypee Education System) Maj. Gen (Retd.) Rakesh Bassi (Registrar) for providing the opportunity to pursue a Doctorate Program, infrastructural facilities as well as advance lab to complete this scientific endeavor of my life.

I would like to thank the authorities of Jaypee University of Information Technology, Wagnaghat for providing the financial support during my research work. I also like to thank Mr. Ashok Kistwal and Mr. Hardeep Rana, Lab. Technicians of all computer labs in JUIT, for their help and cooperation.

I would also like to thanks **Dr. Vivek Sehgal**, Ph.D Coordinator and **Dr Pradeep Singh, Dr. Hemraj Saini, Prof. Karanjeet Singh (HoD Mathematics)**, Members of my DPMC for their evaluation and valuable suggestions during my presentations. I take this

opportunity to thank Dr. P.K. Gupta, Dr. Pardeep Kumar, Dr. Tanuj Kuthail, (Late) Dr. C. Rout, Dr. Sunil Kumar Khah, Dr. Saini and Dr. R.S Chauhan for their constant advice, suggestions throughout my research work. I am also thankful to all faculty members and Staff of the Computer Science and Engineering Department, JUIT, Wagnaghat for their guidance and support. On a lighter note all the faculty members of Jaypee University of Information & Technology and other DPMC (Doctoral Program Monitoring Committee) members for provide me assistance, moral support, valuable suggestions and necessary facilities during the course of my research work. Thanks are due for my dear friends Kapil Kumar, Dr. Ashwani Kumar, Dr. Dilshad Ansari for their support and encouragement during my research work. I also want to acknowledge my seniors Ved Prakash Bhardwaj, Piyush Chauhan, Rashmi Sharma who shared their valuable support. I am always blessed and lucky to have friends who have stood alongside me and my heartfelt gratitude to all my friends for their continuous support and assistance.

It was not possible without the significance amount of assistance from my family. I would like to start by thanking my father **Janab Sabir Ali** and mother **Mrs. Shahjahan Begum** who always encouraged me to do hard work. They teach me that there is no substitute of hard work. I am very much thankful to my dear parents and family members for their affectionate encouragement and blessings to complete this research work. I am very thankful to my brothers Mr. Shabbir Ahmed, Mr. Hashim Rana and Mohd Asif Ali who always stood beside me to support me mentally as well as financially. I truly appreciate their support, thoughts and considerations for everything I seek their assistance on.

At the last stage of my PhD, I was not only anxious but also depressed about when will I submit my Ph.D. At that moment, Dr Aftab motivates me in a very decent way. He told me that how impossible becomes possible. I would like to express my gratitude towards him for his support and motivation.

I never would have made it to this point in my life without a significance amount of assistance from my wife Sonia Parveen. After the three years of my PhD enrollment, she came into my life and that was the most beautiful moment of my life. Since then she is constantly a pillar of support for me. I started my PhD journey with the support of my parents but the completion was not possible without her. Even she also proves that this idiom is true “Behind Every successful man there is a woman”.

Here on the title page I written that the thesis is submitted by me but I would like to say that whole credit goes to my wife. I am extremely grateful to her unconditional love, help and support.

Last but not the least a very special thanks to my son (MERA SHER) Hammad Jabir Ali for his endless wait and endurance while I was too much busy in my academics as well as in my research work. Every time when I came back to home you always gave me positive vibes through your cute smile. Hammad beta, Daddy loves you a lot.

(Jabir Ali)

For my loving family,.....

ABSTRACT

From the beginning of 2015, the exchanging of the digital data through the internet has increased at the rapid. We also know that the exchanging the data on the internet is not secured, so the digital copyright protection becomes the basic need of the time as it needs to be protected from various unauthorized owners claiming on the video. In the last few years lot of research has been carried out in the field of digital watermarking. It also provides an opportunity to protect the videos from unauthorized users. To protect the data we have many different approaches e.g. Copy prohibited bit method, password protection, warning disclaimer and digital watermarking. Here we have considered the digital watermarking method for the protection of the digital data from unauthorized users. In the digital watermarking method the biggest challenge is to protect the digital watermark which remains unaltered by various types of attack or we can say the watermark should be robust.

The concept of watermarking is more demanding and it is not only limited to the identification of the copyright owner, we also used it as an actual proof of ownership. A main problem occur when an intruder or unauthorized user uses some kinds of editing tools to crack or modified or replace the actual and then claims to have possession of the copyright himself or herself. In the initial stage of the watermarking techniques, there are many tools available to detect the watermark. Therefore, the intruder replaces the owner's watermark with his own watermark in order to claim the ownership of the video. But in the absence of the detector, the removal of a watermark by an adversary is the extremely difficult job. In some cases if an intruder was not able to remove then intruder try to damage or destroy the host signals by embedding some special codes.

This problem can be resolve by using an algorithm which can prove that the intruder's image is derived from the original watermark image in place of directly embedding the watermark signal in the host image. In this thesis, we proposed some novel and robust video watermarking techniques to embed the watermark in the frames of digital video. The first method we proposed split watermark embedding algorithm, where we are splitting the watermark into non-overlapping blocks and embedding the individual block in the different frames of the video. For the extraction process we have applied the watermark detection method

on the watermarked video and also performed the process of merging the extracted blocks of watermark to make it as original one. This method is resists many attacks like frame averaging, Gaussian noise, and compression. This method is strongly recommended for the compression attack where no one can remove the embedded watermark by using compression. In the second method, we proposed (SWEA) “split watermark embedding algorithm” along with “zero padding algorithm” (ZPA), where we are embedding the scaled watermark. In this method, we can resize the watermark block according to the video frame and the quality of watermark block will remain same. This method is also recommended for the compression attack. Here in this method, we also achieved the highest robustness for the extracted watermark. In the third method, we proposed a colored watermark embedding algorithm where we are embedding a color watermark in the video and we are getting much better PSNR of extracted watermark in respect of previous methods. In this method we are taking the luminance part (Y) of the watermark image and embedding into the chrominance of the video frame. This method can absorb any type of impurity (noise) and the quality of original media will remain same. The primary focuses of authors are to improve the robustness of the watermark and imperceptibility of digital content. So, we have presented our major donation to the watermark embedding and extracting scheme into the digital videos.

LIST OF ABBREVIATIONS

BER	Bit Error Rate
B-FRAME	Bi-directional Frame
CHROMA	Chrominance
CRT	Cathode Ray Tubes
CWEA	Color Watermark Embedding Algorithm
dB	Decibel
DC	Direct Current
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DT CWT	Dual-Tree complex wavelet transforms
DWT	Discrete Wavelet Transform
FDCT	Forward Discrete Wavelet Transform
GOP	Group of Pictures
HDTV	High Definition Television
HVS	Human Visual System
IDCT	Inverse Discrete Cosine Transform
IDFT	Inverse Discrete Fourier Transform
IDWT	Inverse Discrete Wavelet Transform
IFDCT	Inverse Forward Discrete Cosine Transform
I-FRAME	Identical Frame

LCD	Liquid Crystal Display
Lf ₂	2 nd Level Low frequency
LUMA	Luminance
MPEG-1	Moving Picture Expert Group-1
MPEG-2	Moving Picture Expert Group-2
MSE	Mean Squared Error
O _{video}	Original Video
PCA	Principle Component Analysis
P-FRAME	Predictive Frame
PSNR	Peak Signal to Noise Ratio
QCIF	Quarter Common Intermediate Format
RGB	Red Green Blue
SVD	Singular Value de-composition
SWEA	Split Watermark Embedding Algorithm
TDWIA	Time Division Watermark Insertion Algorithm
ZPA	Zero Padding Algorithm

LIST OF SYMBOLS

W	Watermark
K	Key
X	Luminance Pixel
O	Chrominance Pixels
ϵ	Elements of
k & q	Scaling Factors
WmI_i	Watermarked I Frame
Lf_2	2 nd Level Low Frequency

LIST OF FIGURES

Figure Number	Caption	Page Number
Figure 1.1	Functioning modules of watermark embedding process	4
Figure 1.2	Functioning modules of watermark detection process	4
Figure 1.3	Chrominance sub-sampling showing positions of chrominance pixels relative to luminance pixels (\times =Luminance pixel, \square =Chrominance pixel)	6 & 7
Figure 2.1	Different domains for video watermarking	12
Figure 2.2	Classification of existing watermarking technique	13
Figure 2.3	Frame captured from Natural Video Scene	14
Figure 2.4	Sampling of a video sequence (Spatial and transform domain)	15
Figure 2.5	Still Image with 2 sampling grids	15
Figure 2.6	Vector quantization	17
Figure 2.7	Image sampled at difference of two consecutive frames (black sampling grid)	18
Figure 2.8	Image sampled at difference of two consecutive frames at slightly finer resolution (Gray sampling grid)	19
Figure 2.9	Interlaced Video Sequence	20
Figure 2.10	8x8 DCT Coefficient distribution (Frame)	22
Figure 2.11	2 nd Level DWT by Haar Wavelet	24
Figure 2.12	2 nd Level DWT by Daubechie Wavlet	25
Figure 3.1	General watermarking System	33

Figure 3.2	Watermark decryption process	34
Figure 3.3	Block diagram of watermark embedding process	35
Figure 3.4	Watermark Image (b) Split as per proposed algorithm (c) Watermark Blocks	39
Figure 3.5	Calculating the target frames before embedding the watermark	40
Figure 3.6	Original Frames of Foreman Video after SWEA Algorithm.	42
Figure 3.7	Watermark blocks of JUIT logo after SWEA algorithm	42
Figure 3.8	Watermarked frames of Foreman Video	43
Figure 3.9	Extracted Watermark Blocks	43
Figure 3.10	Watermark extracted blocks in matrix form	44
Figure 3.11	Extracted watermark blocks with merging process	44
Figure 3.12	Extracted watermark for foreman video after applying merging technique.	44
Figure 3.13	Original car race frames (b) Watermarked car race frames.	45
Figure 3.14	Extracted Watermark for car race video after applying merging technique.	45
Figure 3.15	PSNR of watermarked frame and extracted watermark after Gamma Correction.	47
Figure 3.16	BER (Log Scale) under temporal Attack for foreman Video (Frame Repetition)	47
Figure 4.1	Original foreman video frame and their decomposition (a) Original gray foreman video frame (b) 2-Level decomposition of Foreman Video	57

Figure 4.2	Original car race video frame and their decomposition (a) Original gray car race video frame (b) 2-Level decomposition of car race Video	57
Figure 4.3	Watermarked frames (after embedding the first block of watermark. (a) Watermarked Foreman video. (b) Watermarked car race video frame.	58
Figure 4.4	Extracted Watermark blocks for foreman video.	59
Figure 4.5	Extracted complete watermark from foreman video.	59
Figure 4.6	BER (log scale) under spatial attack (Uniform Noise)	60
Figure 5.1	Top Field in color space model	63
Figure 5.2	Bottom Field in color space model	63
Figure 5.3	Red, Green and Blue components of JUIT logo	64
Figure 5.4	YCbCr color components of JUIT logo	66
Figure 5.5	4:2:0, 4:2:2 and 4:4:4 sampling patterns (progressive).	69
Figure 5.6	Allocation of 4:2:0 samples to top and bottom fields	70
Figure 5.7	Complete process of watermark embedding in color domain.	76
Figure 5.8	YCbCr color components of Car race video.	77
Figure 5.9	YCbCr color components of Foreman Video	77
Figure 5.10	YCbCr Color components of Original watermark (JUIT log).	78

Figure 5.11	Watermark extraction process Original Car race frame (B) Original luminance of colored watermark (C) Watermarked Car race frame (D) Extracted Watermark (E) Noisy watermarked car race frame (F) Extracted watermark from the noisy frame (G) Added (Cb & Cr) of the original watermark with extracted watermark.	78
Figure 5.12	Bit Error Rate (log scale) under spatial attack (Uniform noise)	79
Figure 5.13	Bit Error Rate (log scale) under spatial attack (Uniform noise)	79

LIST OF TABLES

Table Number	Caption	Page Number
Table 2.1	Classification of watermarking System	26
Table 3.1	PSNR and MSE for wakna road watermarked video at different size of watermark.	46
Table 3.2	PSNR and MSE for foreman watermarked video at different size of watermark	46
Table 4.1	Video PSNR (in dB) after watermarking	59

CHAPTER 1

INTRODUCTION

1.1. INTRODUCTION

The quick broaden of the digital videos over internet strain the robust techniques for securing the data. The demand is increasing for the discouragement of unauthorized duplication. Copyright protection [1-7] of the digital videos has become a basic need just because of the huge demand and sharing on the internet. There are various techniques like embedding and hiding of the data and digital watermarking which provide the invisible environment for embedding the information in host data that has secret information. The most effective approach of the watermarking is in which the implnted information is uidentified to the unauthorized parties who are not allowed to access the data as well as attempt any kind of attacks.

1.2. VIDEO WATERMARKING

In the last decade, the digital watermarking becomes the most popular area for the research. Many researchers are working in the field of video applications such as internet multimedia, set-top box, personal video recorder etc. has extensively increased the demand for securing the videos. Digital video watermarking [8-11] is an extension of digital image watermarking but in case of video watermarking it has to face many challenges. The video characteristics which effects watermarking are as follows.

1. The high connection between successive video frames. An attacker could remove significant portions of the embedded watermark from each frame carrying an independent watermark in each frame
2. Attacks Like frame averaging, statistical analysis, frame swapping, digital-analog conversions and lossy compressions can be easily performed on watermarked video sequences. [8], [9], [10]
3. The unbalance between the motion and motionless region

1.2.1 PROPERTIES OF VIDEO WATERMARK

The few characteristics required for the process of watermarking as well as the watermark are as follows:

1. **Invisibility:** The code or a digital watermark that we are embedding in the host signal it should not be visible to the human or a spectator.
2. **Robustness:** The operations such as calculation of signals, lossy compression, and collusion perform intentionally or unintentional on the compressed or uncompressed video should not manipulate the watermark and degrade the quality of the digital video. [9]
3. **Fidelity:** The watermark should have high fidelity, so that viewer could not perceive the degradation.
4. **Interoperability:** In the literature survey, we have many applications for watermarking in the compressed domain but without encoded the host signal like compression, it would be more attractive. It is required that the watermark should remain unaffected if compression and decompression operations performed on it.
5. **Constant bit rate:** Watermarking should not increase the bit rate in the bit-stream sphere of influence preferable for the constant bit rate application where transmission channel bandwidth has to follow.
6. **Computational cost:** Every application of watermark embedding and detecting, works at a different speed. So in case of broadcasting monitoring, the speed of embedding as well as detecting should be fast and the computational complexity should be low. As we know, a detector is considered to be fast if it takes just a couple of days to detect whether the watermark is available or not.

1.3. WATERMARKING PROCESS

For the copyright security of the digital media, watermarking is the best technique in which the watermark in the form of digital code is embedded to the original video and later can be recover if the correct pair of keys is used [11-13]. To ensure the robustness also known as

toughness which means that the watermark can easily be obtained from the small portion of watermarked data, which is embedded over many pixels of the original data. There are some issues in the designing of a watermarking system.

One of the best ways of protecting the copyrights of digital media is watermarking where a digital code (watermark) is embedded in the original media and can be extracted by the authorized user whenever he wants to extract it. An authorized user must ensure that the robustness of the watermarked media should not be degraded at the time of watermark insertion as well as detection.

There are some key points we have to remember at the time of designing the watermark system.

1. In the equation 1.1, we have a typical structure of a watermarking process, where W is the watermark signal that has to be supplementary with the original signal. Generally, the watermark depends on the watermark information I and respective key K .

$$W = f_0(I, K) \tag{1.1}$$

It might also be possible that it depends on the host data X that has shown in equation 1.2

$$W = f_0(I, K, X) \tag{1.2}$$

In the equation 1.1, we have the host data X and watermarked signal W that will become watermarked data Y .

$$W = f_1(I, K) \tag{1.3}$$

In the equation 1.4 watermark extraction process has shown where the watermarked signal is having the key K and original data X .

$$I'' = g(X, Y, K) \tag{1.4}$$

In the Figure 1.1, we have shown the block diagram for watermark generation where we have watermark bits W and host data X as the input file along with a public key K . With the help of watermark embedding algorithm (explained in the proposed chapter) we get watermarked data. In the Figure 1.2, we have an uncertain watermark data and test data as an input along with same public key K [12] and applied the detection algorithm that gives the watermark or confidence measure.

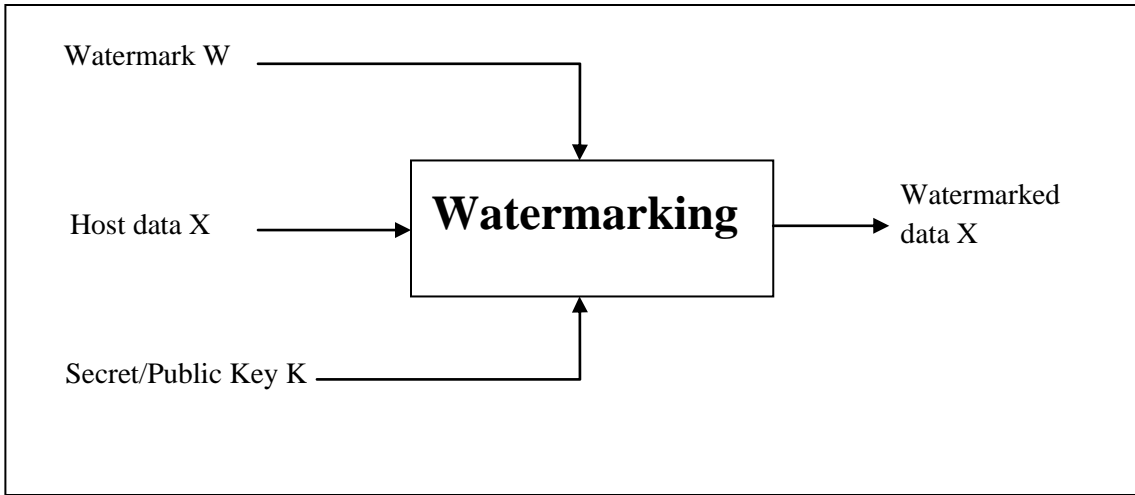


Figure 1.1. Functioning module of watermark embedding process.

And without original

$$I'' = g(Y, K) \tag{1.5}$$

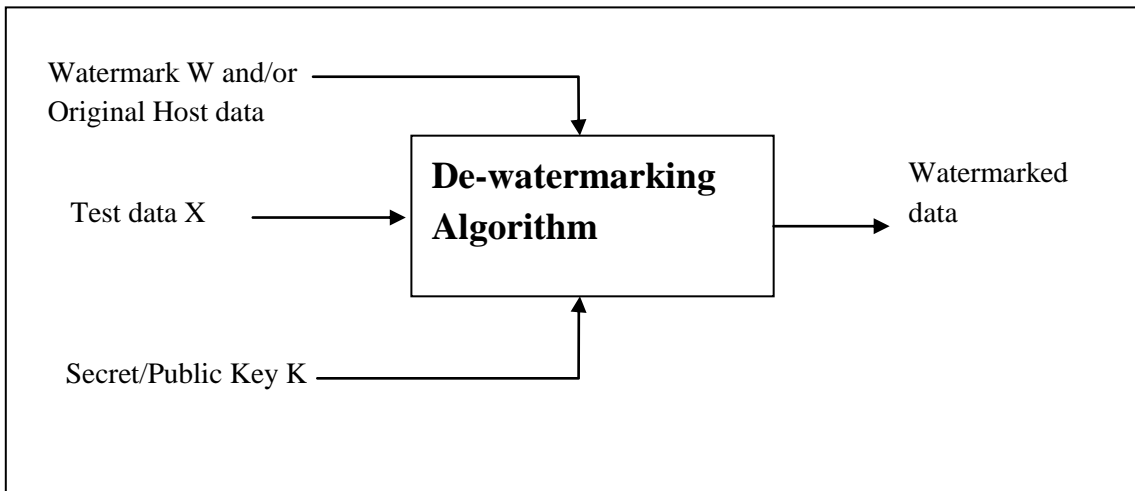


Figure 1.2. Functioning modules for watermark detection process

1.3.1 APPLICATION OF WATERMARKING

Watermarking techniques are evaluated on the basis of some common properties such as robustness, tamper resistance, and fidelity.

The most important applications of the watermarking include copy control, video authentication, copyright protection, broadcast monitoring, fingerprinting and enhance video coding.

1. Broadcast monitoring: The wide range of product is distributed over the television network. So the broadcasted channels should be checked by building a broadcast surveillance system. We can embed the distinctive watermark in each video before its broadcasting so that it can be identified when and where each clip appears by the automated monitoring stations.
2. Video authentication: It is necessary to protect the data from tempering, therefore, validation can be conceded. The result of this difficulty is to insert the watermark straight into the image.
3. Copyright protection: The approach behind embedding a watermark is to identify the rightful owner so that owner can claim the ownership by extracting the watermark.
4. Copy control: The soundtrack of a signal might stop if it detects a watermark which prohibitive the recording, here watermarking technique secure the information in the header and prevent the data from copying.
5. Fingerprinting: It means the ownership belongs to the one who has the authorized user id for the same. It also helps to track the illegal or misused copy of the data that has been distributed by a company. One of the issues is the illegal copying of a newly released movie by a handheld camera and this issue can be solved by embedding the watermark during the show time.

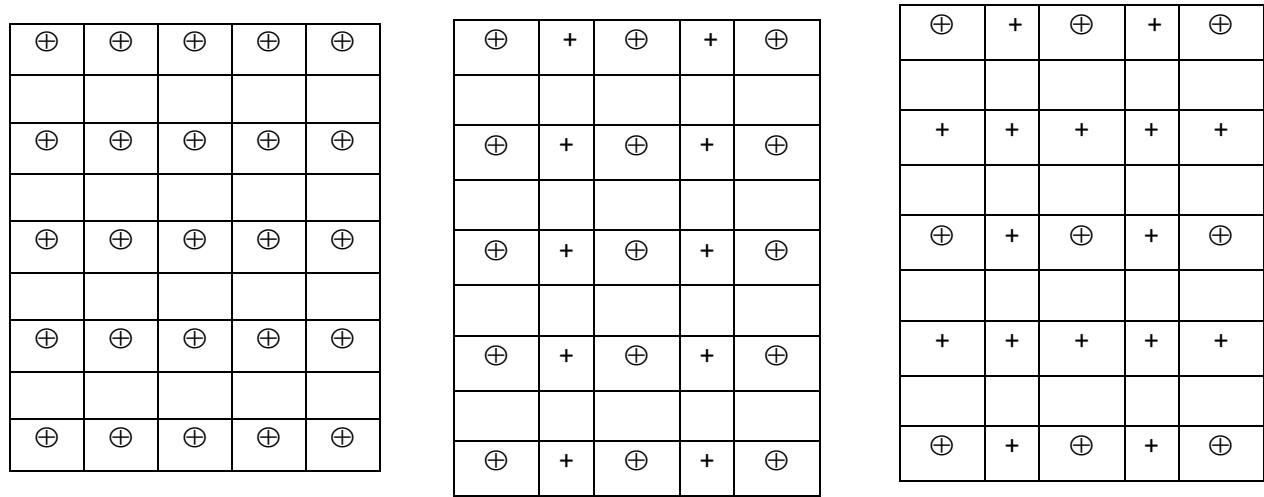
1.4. VIDEO PROCESS

A video is a collection of frames those are moving in respect of time. It is also an ordered sequence of digital images along with audio signals. A video is a collection of images and each image is known as video frame. Every frame is moving in respect of time that is known as the

frame rate. Generally the videos are representing through two different fields that can be represents in a furnish manner.

1.4.1 COLOR VIDEO

A color video is having one luminance and two chrominance components. Luminance represents the brightness and chrominance represents the color information of the video. For the basic knowledge every color video is a combination of RED, GREEN & BLUE pixels.

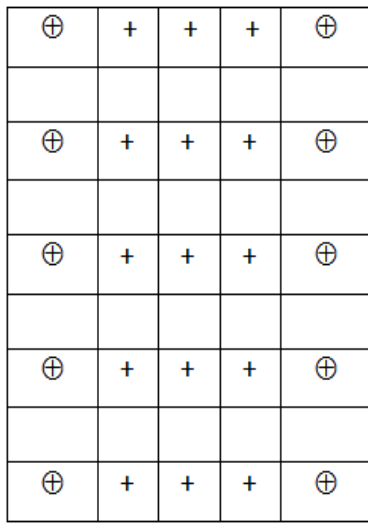


(a) No sub-sampling

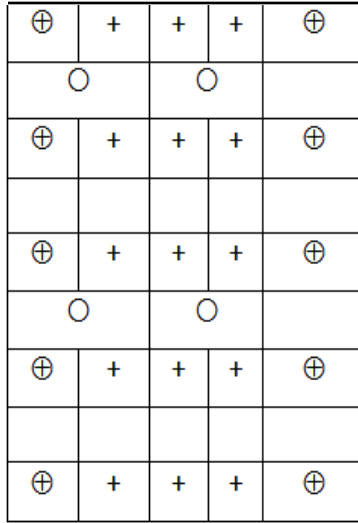
(b) 4:2:2

(c) 4:1:1

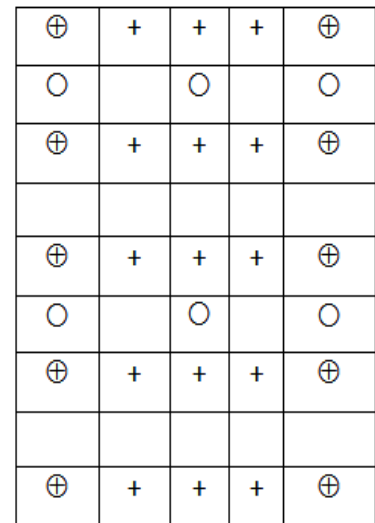
Generally a colored image that has “luminance and chrominance” part is sampled at the same rate, where the pixels coordinates (x,y) are composed. Even chrominance may be sampled at lower rate and also at the different position from the luminance part of the image. As we know that the human visual system (HVS) has less sensitivity for the color information in compare of brightness. So it is easy to modify the color information in place of the brightness of the image. It means we can embed the watermark information in blue chrominance or red chrominance. In the figure 1.3 we have shown chrominance pixels (O) with respect to luminance pixels (+). To calculate the size of an image or a video frame we depend on the displayed size or we can say the pixel size. The display size can be explained by the physical dimensions of an image when it displayed where a display size is belongs to the independent of pixels representations and also distinct for both analog and digital images as well.



(d) 4:1:1 (alternate)



(e) 4:2:0 (MPEG-1, H.263)



(f) 4:2:0 (MPEG-2,H.264)

Figure 1.3 Chrominance sub-sampling showing positions of chrominance pixels relative to luminance pixels (⊕=Luminance pixel, ○ =Chrominance pixel)

. The aspect ratio can be explained as the ratio of display width to display heights. In the conventional analog television the aspect ratio is 4:3 while in the high definition television (HDTV) is 16:9. In the motion picture the aspect ratio is 1.85:1 to 2.35:1. The pixel size is referred as the horizontal and vertical dimensions of an image but in case of analog image it does not contains the pixels because the pixel size is undefined. It is also noted that the pixels shape may not be square when the video is displayed.

1.5. PROBLEM IDENTIFICATION

We are sharing a huge number of videos on the internet and that particular video belongs to whom, is the biggest challenge in the current scenario. So to protect the copyright of these digital videos we have developed different kinds of algorithms. In this thesis, the author has focused on the design of robust and secure watermarking techniques for authorization and authentication that also provide the piracy tracing and copyright protection of multimedia content. In this research work, the author has focused on the following problems.

1. In the literature survey of digital video copyright protection [8-10], the author has found that the existing systems are still not fulfilling the requirement of the user. For example, the methods are used for authorization and authentication of the videos needs to improve in many ways.
2. In the literature survey, most of the authors are still not able to provide an exact solution to compression attack [14] where this attack is degrading the quality of extracted watermark.
3. The pattern, we are inserted as a watermark is not secure.
4. If an intruder is not able to understand the pattern of inserted watermark then he may be erased or corrupt that watermark.
5. In the literature survey of digital video copyright protection, the author has found that most of the researchers used gray level image or logo as a watermark.
6. Scalability of inserted watermark still needs to improve.
7. The concept of deep learning can also be used at the time of watermark extraction as well as watermark insertion.

1.6. OBJECTIVE OF THE THESIS

The core objective of this thesis is to offer an appropriate solution to the problem statement that author already explained in the problem identification section. In the world of entertainment and knowledge sharing, digital videos are the best medium. In this thesis, we have designed some algorithms those are providing the best solution for the above problem identification.

So the objective of this thesis is:

1. To propose the robustness and security, where an unauthorized user or an intruder could not understand the pattern of the inserted watermark, as well as the quality of original media, should not be degraded.
2. To propose the scalability, robustness, and security, we designed the zero padding watermark embedding algorithms (ZPA) along with Split watermark embedding algorithm. It is also able to attain the excellent stability among high compression and

channel error toughness. It takes the benefit of the arithmetical performance of the video in spatial as well as temporal domains also.

3. To propose a colored watermark embedding method, where an owner can embed the colored watermark. The time complexity of embedding and extraction of the colored watermark should be very low in comparison with literature survey.
4. To propose a dual watermark embedding environment that improves the security, robustness, imperceptibility and adding of multiple watermarks by an unauthorized user.
5. To propose a digital watermarking scheme that has the ability to overcome the problems which were existing in previously published digital videos copyright protection technique and also increase the efficiency as well as security.

1.7. ORGANIZATION OF THESIS

The thesis has been organized as follows. In chapter 1, the author has given the introductory part of the thesis. In the 2nd chapter, the author has explained review and background, related to the existing system. The author has divided his research work into three major problems. The solutions to these problems are represented by three objectives in three chapters. So in chapter 3, the author has presented a robust and imperceptible digital video copyright protection scheme (SWEA) where watermarking embedding and extraction scheme is based on discrete wavelet transform. In chapter 4, the author has presented an approach of copyright protection for digital videos using zero padding algorithms along with split watermark embedding algorithm. In chapter 5, the author has explained a colored watermark embedding approach (CWEA) that improved the quality of extracted watermark and also reducing the execution time. In chapter 6, we have proposed a dual watermark embedding process in audio and video domain. Here in this approach, we get the improved results in all aspects like security, robustness, imperceptibility and multiple watermark insertion. Finally, the conclusion has been explained in Chapter 7. Since many problems are unsolved or unaddressed so there is a future scope for addressing the problems which were not resolved by the previous methods. References and list of publications are given at the last of this thesis.

CHAPTER 2

REVIEW AND BACKGROUND

2.1 INTRODUCTION

In the literature survey, we have been studied various algorithms for digital video copyright protection [2-5]. For many years researchers are working in the field of digital copyright protection but nowadays researchers are putting their efforts to protect the videos from unauthorized users. A video is a collection of frames which are continuously moving with respect of time and may also have an inbuilt audio file. Every frame has two types of redundancy one is spatial and another one is temporal [15, 16, 17]. So after the study of digital video, we have analyzed that we can embed the copyright information file (watermark) in the frames as well as in the audio file. For embedding a watermark file, we have spatial and transform domain, in the spatial domain we just manipulate the pixels values of the frames or audio for embedding the watermark while in case of transform domain we extract the lower and higher frequency of the frame and embed the watermark in any of frequency. The procedure of embedding the any sort of multimedia data within another multimedia data is called steganography whose main aim is transmission of secret information or code in a hidden manner, far from being noticed. Initially the concept of steganography is used in military services where they used to encode the secret messages inside the other media. For an example an image contains the text data as a secret code. It can be further defined and explained in the given manner.

Here in our system, we are using the same technique for completely different purpose. Here, our goal is not transmission of secret information but to protect the copyright of owner of multimedia video from being threatened. Embedding of information within the video is a helpful process of proving his/her rightful claim on the particular video. The main objective of this thesis is to embed the watermark in video data, where the watermark can be a text, an audio, file or an image. But it has to be ensured that embedded watermark cannot be detected by any unauthorized user, if detected anyhow then it should not be altered or meddled with. The embedded watermark

has to be final in every way which cannot be tampered thus protecting the copyright of the video. But to implement these ideas several concepts and issues have to be dealt with utmost care. These are some basic terminology that we have to consider during the watermark insertion or extraction process.

2.1.1 ROBUSTNESS

The meaning of robustness is toughness of the data. Here we used the term robustness for the watermark image that state the quality of the watermark should not be degraded after applying any kind of attack and the attack whether it was the intentional or unintentionally applied on the data. For an example, unintentional attacks means when we are sending our data on the network then to reduce the network load it will automatically compressed by the network and here in our algorithm we have consider that compression is an attack so the watermark we are embedding it should be robust.

2.1.2 DATA CAPACITY

Data capacity belongs to the size of data that we are embedding in the original media as a watermark. Basically it defined the size of watermark bits that how many bits can be inserted inside a video without any degradation failure. Most of the algorithms state that you are not allowed to embed a bigger size watermark because the capacity of original media for accepting the bits as a watermark is very low.

2.1.3 SECURITY

Security is the major concern of these days and to protect the digital data from unauthorized users or from an intruder is a big challenge. The watermarking technique also provides the security and copyright to an authorized person. In our algorithm mainly we have focused on the security, robustness and imperceptibility of the watermark as well as original video file.

2.1.4 LOW ERROR PROBABILITY

This is also considered on a high priority. The term “low error probability” is defined as the minimum loss of information from the extracted watermark and the original video. In order to obtain low error probability, it is required to apply such algorithm which provide the minimum loss of information from the extracted watermark and original video of the obtained by extracting the watermark extracted watermark should have a very low bit error rate and also maintain the originality of the video file means where we are inserting the watermark bits.

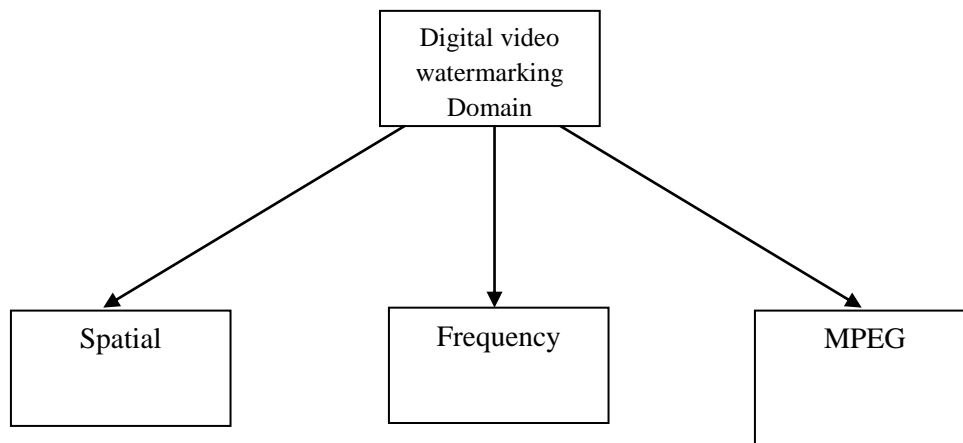


Figure 2.1 Different domains for video watermarking

Watermark insertion and extraction in the spatial domain is a very simple process but the security of watermark is very poor while in case of transform domain watermark insertion and extraction are quite complex but the security, robustness, and imperceptibility are very high. So in the current scenario most of the time we are using transform domain for insertion and extraction of the watermark.

In figure 2.1 we have shown the different domains for invisible video watermarking where in figure 2.1 we have shown the classification of all existing watermarking techniques. When we captured a video it is known as raw video but at the time of visualization we need to compress and decompress these video signals this is called the video coding. Here, we scrutinize the review and background of digital images and digital video also. We have also introduced concept of digital video such as sampling of a video and quality matrices those are very helpful to understand the digital videos.

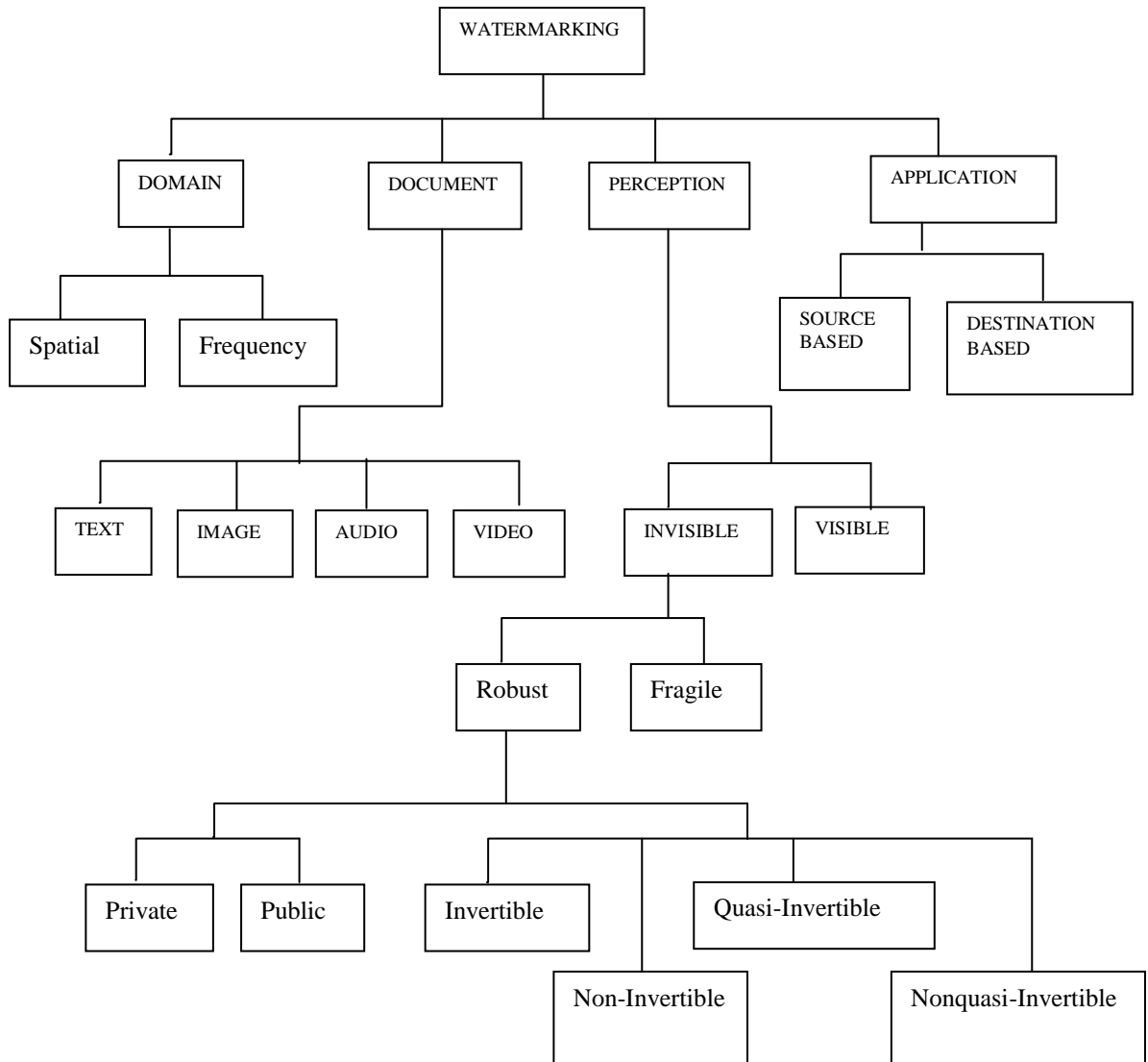


Figure 2.2 Classification of existing watermarking technique

A raw video is the representation of the real world (as we can see through our eyes) that is sampled spatially and temporally. After applying these transformations on a scene it becomes complete visual scene. Every scene is sampled at a fixed point of time to produce a frame or a field. After a fixed interval (1/25 or 1/30 seconds) repetition of the sampling is necessary to produce a moving video. As per the RGB color system three primary colors are required to represent a video in colored domains. As per the color information we required only three colors

Red, Green and Blue for generating any color. YCbCr colored video format we required luminance and chrominance components to produce a video in colored domain. Here in YCbCr Y is representing the brightness and CbCr representing the color information.

2.2 NATURAL VIDEO SCENE

When we captured a natural scene it comprised many objects and each object is having their own characteristics shape, depth, texture etc. In figure 2.3 we can see a typical natural video scene in which every object is reflecting their characteristics. While watching a movie at that time the color and brightness of the scene continuously varying their degree of smoothness. In the figure 2.3 can identify each object like green trees, a white t-shirt, gray trouser and water with stones. We are able to detect all the objects because every object is reflecting their degree of smoothness.



Figure 2.3 Frame captured from natural video scene

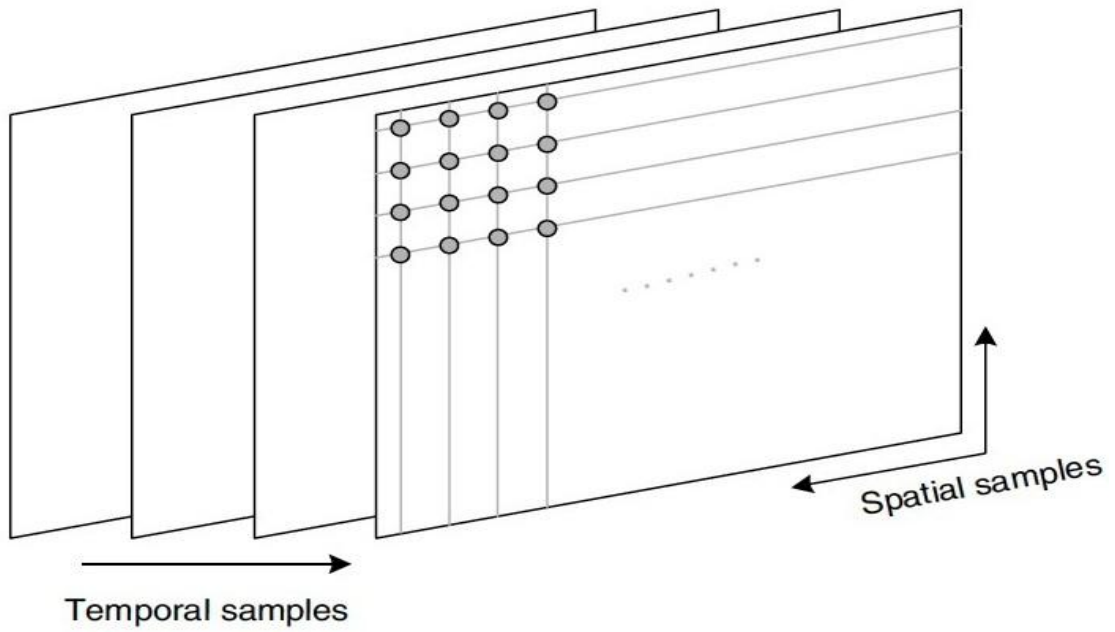


Figure 2.4 Sampling of a video sequence (Spatial and transform domain)



Figure 2.5 Still frame with 2 sampling grids

2.3 CAPTURE

In order to represent a natural visual scene in a digital format, it is required to sample the real scene spatially and temporally. A digital video is basically the representation of sample frames those are moving in respect of time e.g. 25 fps or 30 fps video. With the help of spatial-temporal samples we can represent the pixels of the image that can describe the actual brightness of the image of a video frame. A pixel represents the smallest unit of an image, where a pixel is represented by a number. An 8-bit gray image is having the values 0-255.

2.4 VIDEO WATERMARKING

Initially the trend was to re use the still image watermarking in which the video is considered to be the sequence of still images and image watermark is embedded to each frame which results in increasing the payload and decreasing the visual impact. After comparing both video watermarking and image watermarking, we came to the conclusion that the former one imposes real-time constraints on the watermarking system.

2.5 FRAME AND FIELDS

A video gesture is considered as a succession of continuous frames (those are moving in respect of time) or an interlaced field in which half of the data is sampled at each TEMPORAL sampling interval. A field is a collection line, where total number of lines in a complete video may be odd-numbered or even-numbered. An interlaced video sequence can be describes as a series of fields. Each field is representing maximum information of a video frame. The best part of sampling is that it is possible to send more than one fields per second as it is required by the number of frames. For an example if we take a PAL video sequence that consists of 50 fields per second and when we played back, the motion can be seem very smooth in compare of an equivalent video sequence that containing 25 frames per second. We have shown the classification of existing technique in figure 2.2.

There are three domains in which we can embed the watermark which is as follows:

1. Spatial domain
2. Frequency domain
3. MPEG coding structure domain

2.6 SPATIAL DOMAIN

In this method, the process of embedding the watermark is a very simple process and on the other hand the computational cost of watermark extraction is very low. The watermark is inserted in the pixel domain and can be extracted by spread spectrum modulation. Since its method of extraction is also a simple process so it can be detected very easily from the host signal and in that case, its uniqueness can't be claimed [18]. In the spatial domain we have direct pixels values and all the values are stored as an output of CCD array. An image after the sampling is having the fixed values at a position of defined sampling points. An ordinary format is used for a sampled image, that is four-sided figure blocks and these blocks are positioned on a rectangular grid.

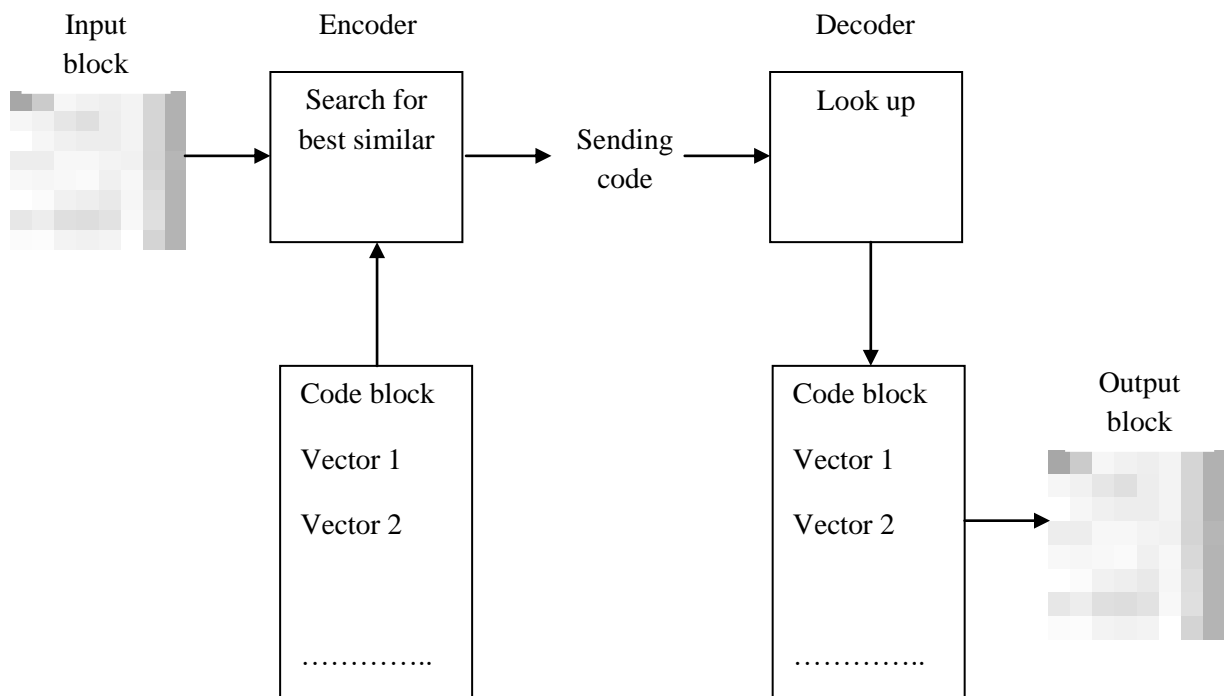


Figure 2.6 Vector Quantization

In figure 2.4 there are two dissimilar sampling grids those are superimposed on it in a continuous-tone frame. Here sampling is occurring at each of the junction points on the grid and the sampled image can be reproduced by on behalf of each sample as a square picture element also known as pixel.

2.7 TEMPORAL DOMAIN

A moving video frame is captured by taking a rectangular ‘snapshot’ of the signal at periodic time intervals. In the transform domain it is also noticed that it’s a frame difference of two consecutive frames. A video consists of three types of frames I, P and B where “I is IDENTICAL-frame”, “P is PREDICTIVE-frame” and B is BI-DIRECTIONAL. In figure 2.7 an image sampled at coarse resolution is shown. It is the difference of two consecutive frames. In the temporal domain if the temporal sampling is at higher rate than it gives relatively smoother motion in the video scene.



Figure 2.7 Image sampled at difference of two consecutive frames (black sampling grid)

If we take a video of 10 fps that means 10 frames are moving in one second, the quality of these videos becomes very poor but it is easy to transmit at the time of communication over the internet. But if we choose the frame rate between 10 to 20 frames per second it becomes clearer. But if we play these video in fast forward mode then the quality of these videos becomes jerky. The frame rate 25 or 30 is basically used for standard video quality. The frame rate 25 or 30 is always providing a good quality of video and the size of the bits transferring is also not too much high. For the high quality video we used 50 or 60 frames per seconds but on the cost of a very high data rate. In this case we can get a high quality video but we also have to compromise with the data rate that is too much high. Generally, the frequency domain is used DFT, DCT, and DWT as the method of data transformation.



Figure 2.8 Image sampled difference of two consecutive frames at slightly finer resolution (gray sampling grid)

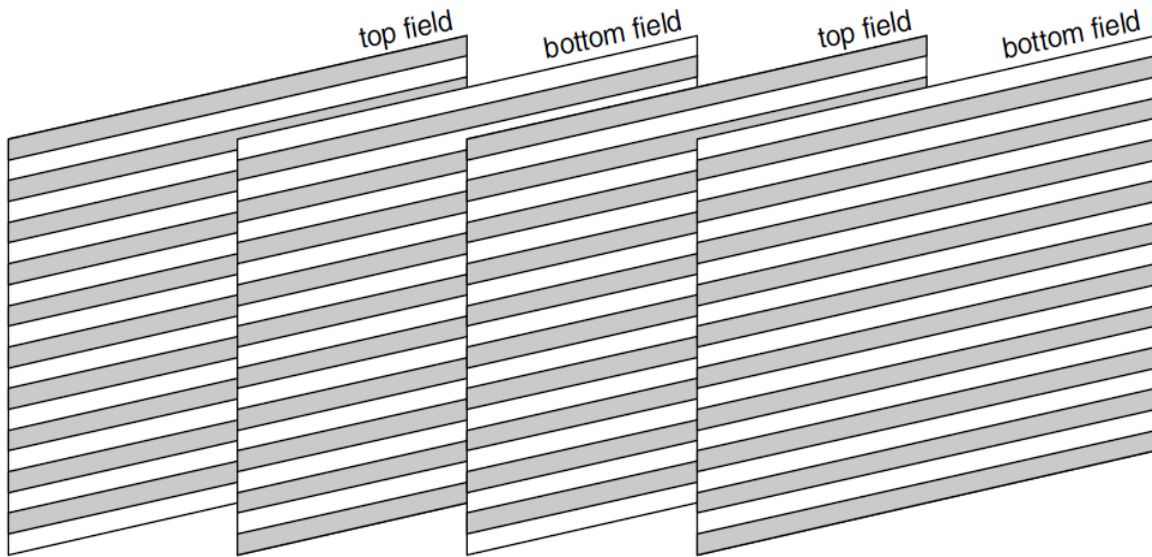


Figure 2.9 Interlaced Video sequence

In the frequency domain, the watermarking algorithms are more secure and robust. With the help of these algorithms imperceptibility and scalability also improved but the execution time complexities of these algorithms still an issue. After comparison of spatial and frequency domain, we came to the conclusion that frequency domain is the best technique for embedding the watermark [19-24].

2.7.1 DISCRETE COSINE TRANSFORM

The Discrete Cosine Transform (DCT) [7], [17], [25-27] operates on \mathbf{P} , a block of $N \times N$ samples, where an image is predicted with the help of image samples or image residual and creates \mathbf{Q} , an $N \times N$ block of coefficients. The action of the DCT (and its inverse, the IDCT) can be described in terms of a transform matrix \mathbf{A} . The forward DCT (FDCT) of an $N \times N$ sample block is given in the current scenario; for the image processing the most accepted domain is discrete cosine transform (DCT). The discrete cosine transform (DCT) divides the image into different frequency bands that making it easier to embed the watermark in middle frequency band of an image. The middle-frequency bands are chosen on the basis of low frequency that also avoids the most visual parts of the image. So when we embed the watermark information in this

kind of frequency of an image, it does not affect its originality. Compression and noise attack also does not affect this technique of watermarking.

$$\mathbf{Q} = \mathbf{A}\mathbf{P}\mathbf{A}^T \quad (3.1)$$

Inverse of DCT (IDCT) by:

$$\mathbf{P} = \mathbf{A}^T\mathbf{Q}\mathbf{A} \quad (3.2)$$

Here \mathbf{P} is representing the samples of a matrix and \mathbf{Q} is representing the coefficients of the matrix and \mathbf{A} is an $(N \times N)$ transform matrix.

The elements of \mathbf{A} can be represented in this way:

$$A_{ij} = C_i \cos \frac{(2j+1)i\pi}{2N} \quad \text{Where} \quad C_i = \sqrt{\frac{1}{N}} (i=0), \quad C_i = \sqrt{\frac{2}{N}} (i > 0)$$

The above equations (3.1 & 3.2) can be written in another form:

$$Q_{xy} = C_x C_y \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} P_{ij} \cos \frac{(2j+1)y\pi}{2N} \cos \frac{(2i+1)x\pi}{2N}$$

$$P_{ij} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} C_x C_y Q_{xy} \cos \frac{(2j+1)y\pi}{2N} \cos \frac{(2i+1)x\pi}{2N}$$

Here given below in the figure 2.10 we have shown the considerable discrete Cosine Transform coefficients of a block of an image or also known as the residual samples. Basically the ‘low frequency’ positions those are near at the DC (0, 0) coefficient. In the Figure 2.10 also explains the plots for likelihood of nonzero DCT coefficients. In the given Figure 2.10, the position of each 8x8 block in a QCIF residual frame is showing in a manner that all the nonzero DCT coefficients are clustered around the top-left (DC) coefficient.

Here, all the coefficients are clustered in the region of the DC position but all these are in the form of ‘skewed’ that means many more nonzero coefficients are occurring along the opposite of right side of the plot. The main reason behind it the field picture. A field picture has the stronger high-frequency components on the vertical axis.

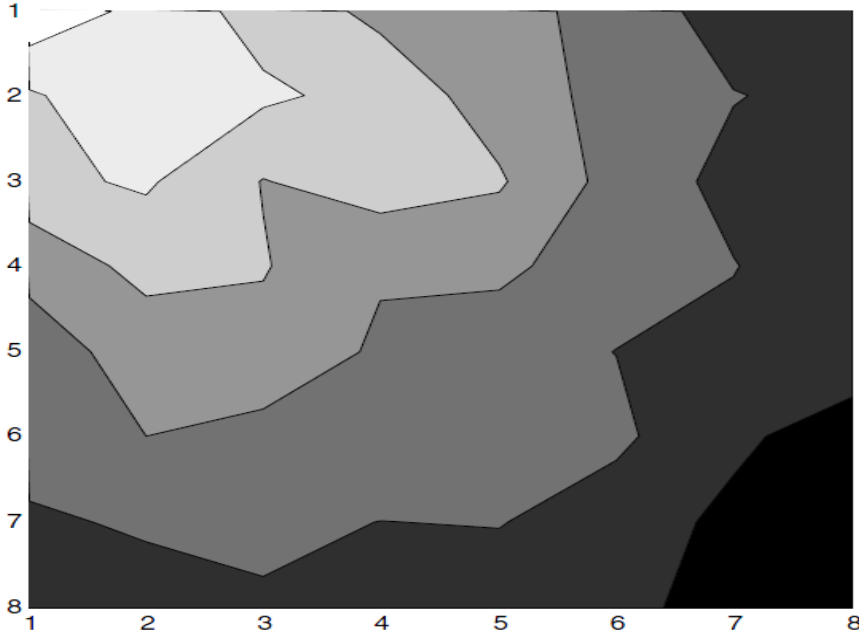


Figure 2.10 8 × 8 DCT coefficient distribution (frame)

The mathematical explanation of the DCT, Suppose we have a 2D watermark W that has to be entrenched in the middle band frequency of 8x8 block. The 8x8 block coefficients $F(u,v)$ will be modulated as per the given equation.

$$I_{W_{x,y}} = \left\{ \begin{array}{ll} I_{x,y}(u,v) + g * W_{x,y}(u,v) & \text{if } u,v \in F_M \\ I_{x,y}(u,v) & \text{if else} \end{array} \right\} \quad (3.3)$$

Here in the equation, 2.1 F_M is the middle frequency, g is the gain factor, x,y are the spatial domain location of 8x8 block and u,v are the DCT coefficients of the image I , in the correspondence of 8x8 DCT block.

2.7.2 DISCRETE WAVELET TRANSFORM

This is also a very popular method of embedding the watermark. The wavelet transforms to convert the original image in four parts “LL, LH, HL and HH” where LL is having the approximate coefficients and HH is having detailed coefficients of the image. In the LL part image also look like as original and in the LH & HL, it shows the boundary region of the image

and finally HH part contains the maximum redundancy of the image. In this domain, we can further divide the image that is also known as 2nd level DWT, 3rd level DWT and so on.

Here in the given figure 2.11 and 2.12, we are showing 2nd level DWT.

Generally, it is the most popular transform for image compression that is based on sets of filters. The discrete wavelet transform (DWT) is used two filters; one is low pass filter and second is high pass filter. DWT [19-22] convert an image signal into two frequencies (low level and high level). In the low level we have the detailed coefficients of the image and in the high level we have approximate coefficients of the image. This process is reversible with the loss of minor bits. In our research work DWT plays a vital role because to get the best and required results, we used this transform only. In this transform an image signal is converts in two frequencies (low frequency and high frequency)

Where low frequency is having maximum information of the image even it looks like the same as original but in case of high frequency we have redundant information or we can say the edge information of the image. For our proposed method it is very obvious that the information we are hiding in the image, it should be robust. So if we embed the information inside high frequency band then it may lose during the compression because at the time of compression it compresses the redundant information.

2.7.2.1 HAAR WAVELET

It was the first time when it was used as a concept of DWT. This method was proposed by the Hungarian mathematician in which, he took the input in the form of 2ⁿ and stored the difference and pass the sum. This method was repeated over and over again in order to pair up the sum to get the 2ⁿ-1 differences and a final sum.

$$\psi(t) = \left\{ \begin{array}{ll} \mathbf{1} & \mathbf{0} \leq t \leq \frac{\mathbf{1}}{\mathbf{2}}, \\ -\mathbf{1} & \frac{\mathbf{1}}{\mathbf{2}} \leq t \leq \mathbf{1}, \\ \mathbf{0} & \textit{otherwise} \end{array} \right\}$$

Its scaling function $\varphi(t)$ can be described as

$$\varphi(t) = \begin{cases} 1 & 0 \leq t \leq 1 \\ 0 & \textit{otherwise} \end{cases}$$

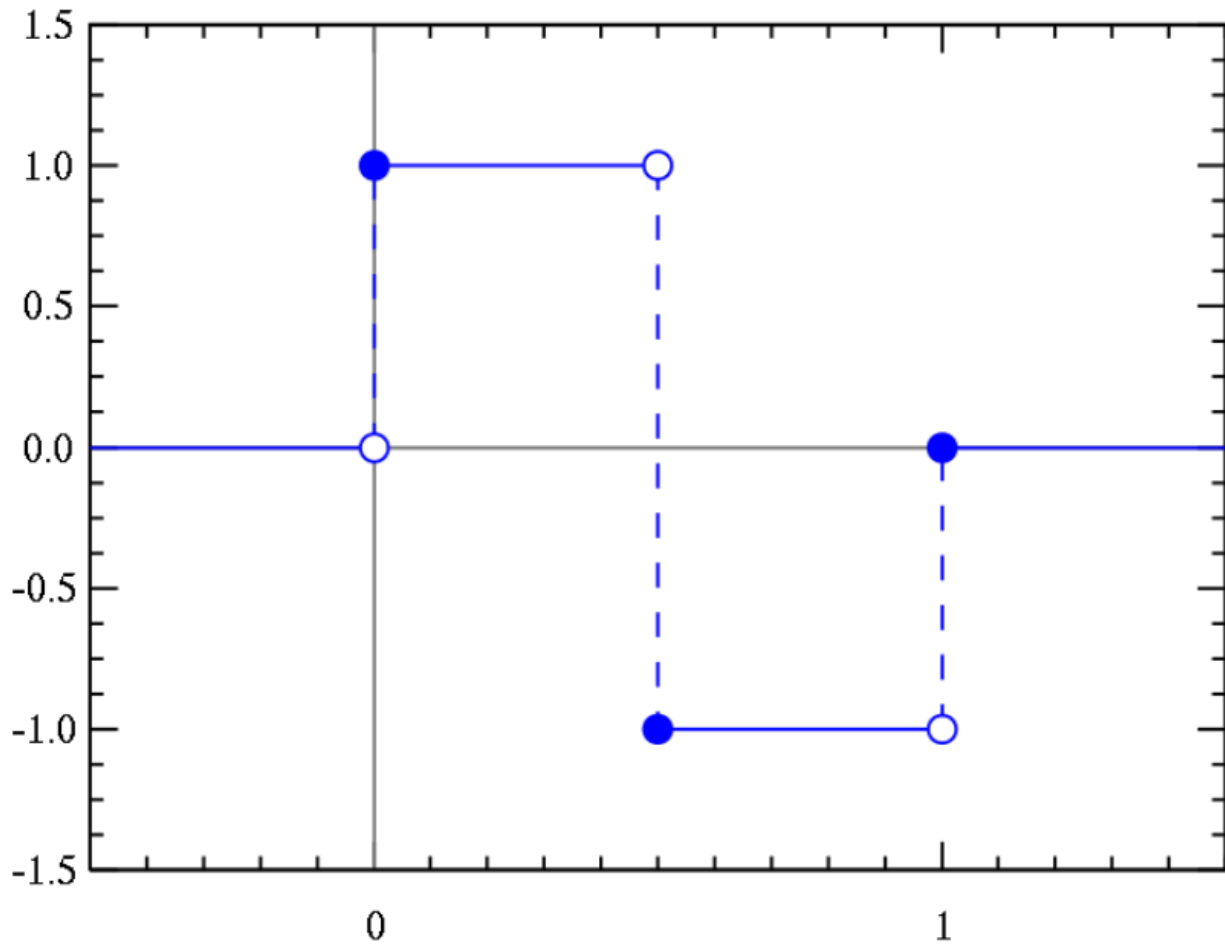


Figure 2.11: 2nd Level DWT by Haar Wavelet

Low-Low -2	Low-High -2	Low-High -1
High-Low -2	High-High -2	
High-Low -1		High-High -1

Figure 2.12 2nd Level DWT by Daubechie Wavelet

2.7.2.2 DAUBECHIE WAVELET

This wavelet is used most commonly and it was formulated by the Belgian mathematician in 1988. This wavelet function was named of that mathematician whose name was Ingrid Daubechies [21], [22]. The method is based on the use of recurrence relations to produce more and more better discrete samplings of wavelet function; each resolution is twice that of the previous scale. Daubechies generate a family of wavelets, where the first is the Haar wavelet..

2.8 WATERMARK-BASED ON MPEG CODING STRUCTURE

In the MPEG [28], [29] coding structure video watermarking technique the main goal is to reduce the overall time complexity in the real-time video and for achieving this goal should concentrate on integrating watermarking and compression also. For the compression, as we know that in MPEG-2, we remove the temporal redundancy by using P-frames (Predictive) and B frames (Bi-directional) and also used the statistical method to remove the spatial redundancy. In the case of re-compression or conversion to any other format, this method is not highly secured and the embedded watermark information may detect or crack by the unauthorized users.

A Digital watermarking scheme for the MPEG-2 coded video is proposed by the Choi, Dooseop et al. [28] in the bit-stream domain. Here in this scheme they proposed, an I-frame will split into

the blocks of 8 x 8 Pixels and will be compressed by using the DCT. The P and B frames are predictive and bi-directional frames respectively. The P frames are depended on the behavior of the previous frames and B frames are depended on the previous and next motion frames. In the place of embedding the watermark indication in the pixel domain, here the algorithm extract, programmed 8×8 block of the video and the analogous block from the watermark signal.

Table 2.1 Classification of watermarking System

Criterion	Class	Description
Domain Type	Pixel	Direct modification in the Pixel values.
	Transform	Customized the coefficients of Transform Domain There are the list of admired Transform:- “(DCT) DISCRETE COSINE TRANSFORM” “(DWT) DISCRETE WAVELET TRANSFORM” “(DFT) DISCRETE FOURIER TRANSFORM” “(PCA) PRINCIPLE COMPONENT ANALYSIS”
Watermark Type	PRNS	“Detect the presence or absence of a watermark”.
	Visual	“Quality of the embedded watermark is calculated”
Information Type	Non-blind	“Both the original image and Secret key required”
	Semi-blind	“The watermark and the Secret key required”
	Blind	“Only the secret key required”.

Here in the Table 2.1 we have shown the classification of watermark system. In this table categorized the watermark on the basis of criterion and the possible classes of the watermarking. Here in the blind watermarking we required only the secret key to extract the information from the watermarked frame.

2.9 PAPER REVIEWED

In the last few years, those applications were present in grayscale for image or video now extended to the colors, where color is a combination of three components R (Red), G (Green) and B (Blue). To get the alternative of RGB, YUV comes into the picture where Y is having the maximum information of the frame or we can say the information of brightness and UV contains the information about colors.

In the early stage of the video or image watermarking most of the researchers used the grayscale image for their experiments but in the present scenario colored image or video is widely used. To embed the watermark inside the video frame is not a big challenge. So a watermark insertion method should have a good robustness, imperceptibility and capacity. Here we have explained the literature survey that categorizes the watermark insertion domain used by an author.

2.9.1 COMPRESSION DOMAIN

Huang, Hui-Yu, Cheng-Han and wen-Hsing, explained the compressed domain watermarking techniques [25], they embedded the watermark by using the technique called discrete cosine transform (DCT) which generates the encoders namely “MPEG-2,MPEG-4,H.264/AVC,H.265/HEVC”. C. S. Lu et al. also explained that we can embed the watermark in compression domain by using specific components. In the below section, we discussed the format of moving picture expert group (MPEG-2 and MPEG-4) and also explained the high definition “H.264/AVC and H.265/HEVC” video format video watermarking techniques.

1) MPEG-2 Video Watermarking: MPEG-2 is a compression standard which is widely used in TV signals and also used to accumulate the movies and other videos on DVD disc at the speed of 10Mbps.

In the MPEG-2 [28] video compression method, the frames of the video are compacted in three ways, the first one is intra-coded (I-frame), this frame is having its own information and it is identical also. The next frame is predictive coded (P-frame), this frame is depends on the just previous frame and contain the maximum information of the previous frame. Last but not the least frame is bi-directional coded (B-frame), this frame is depends on the just previous one and also depends on the just next frame. Bi-directional frame is containing the information of both

the frames previous one and next one. Hartung et al. also proposed an algorithm for the uncompressed domain based on the spread spectrum watermarking that is also well-matched expansion of this method. In this method an encrypted pseudo-random indication by using the discrete cosine transform embed in the “MPEG-2” bit stream. For the decoding process of the watermark they used blind watermark extraction technique. Chung *et al.* also proposed a watermarking method for MPEG-2 video. In this method the author exploiting the direct progression of spread spectrum that mainly focus on the watermark embedding power and the area where watermark is going to be inserted to maintain the quality of watermarked video remain same. This method was able to extract the watermark information without the original video.

1) MPEG-2 Video watermarking: Here in this method the author comprises an encrypted, pseudo-random signal using the discrete cosine transform function and then embed into the MPEG-2 video signal. These kinds of algorithms are valuable in terms of watermark extraction because it is easy to extract the watermark in the blind fashion. The Author Chung et al. also proposed a watermarking algorithm for the MPEG-2, in this method author is just putting direct sequence through the spread spectrum technique. In this method, author mainly focused to retain the quality of watermarked media. It can also extract the watermark from the watermarked video without depending on the watermarked video. In this method author used the spread spectrum watermark by modifying the DCT coefficients. The result section of this paper is also demonstrated that this method is robust against many attacks. One more algorithm is explained in [89] that can be designed in the VLC domain of the MPEG-2 video.

2) MPEG-4 video watermarking: In the [29] the authors explained latest compression standards for MPEG-4 video specifically for the low bandwidth audio and video. This technique is also based on the MPEG-1 and MPEG-2 but it also carried out some more features and functionality. The main feature of this technique is object based coding. Here in this method it can be individually defined the objects (audio and video) for embedding the watermark and finally rendered together to make it watermarked video. One more author Boulgouris et al. proposed a method for digital video watermarking. In this method the author is able to embed the watermark in the low-bit rate MPEG-4 videos. This scheme is also provide the protection against geometric attacks. Here they also introduce a new feature that is gain control to improve the

visual excellence of watermarked video. Here they also proposed a secured method that after compression attack the quality of embedded watermark will not degrade. This scheme is also suitable for the low bit rate videos. In this paper author also improved the quality of extracted watermark after performing some common attacks. The best way of quality measuring of extracted watermark is PSNR (peak signal to noise ratio). This is highly recommended for quality measuring. Here the author gets the good PSNR of extracted watermark as he compared his method with his literature.

In the literature survey, we have been studied that some of the watermarking algorithms are purely designed on the basis of “MPEG-4 video”. In an article Barni et al. proposed an algorithm of watermarking for MPEG-4 video. In this paper he embeds the watermark in every purpose of a “MPEG-4” video. The embedding process is defined as associations linking with a number of predefined pairs of quantized DCT coefficients. Here we also studied that the watermark embedding can be done in the Y channel blocks of selected intra and inter-macro blocks with the help of pseudo-random algorithms.

Here they used the blind watermarking system and occurrence masking. The algorithm is providing the good results in case of visual quality and robustness. This algorithm is having the limitations in case of robustness that can be done only in the case of bit-rate moving back and frame dropping. Here in [29], the Boulgouris proposed a method of digital watermarking for MPEG-4 natural video objects, where the watermark signals are embedded into the MPEG-4 video to enable the fast harmonization improvement in the case of any modification with the original media. Lu et al. also proposed a watermarking algorithm that is based on the concept of communications with side information for a “MPEG-4 video” object. Here in the proposed method they calculated the value of eigenvectors of a video object to conclude it’s most important and negligible orientation is used to deal with arithmetical transformations. This method also claimed that it resists several attacks; e.g. histogram equalization, flipping and blurring.

3) “*H.264/AVC Video Watermarking*”: H.264/AVC video compression [30-35] is most commonly used in these days. It is also known as the part of MPEG-4. This compression technique is much better the previous standards in video quality at lower bit rate. This technique is also includes the various new features and these features are strongly recommended. In [33] Xu, Dawen et al. used a method of encryption for the “H.264 AVC/SVC” in compressed domain.

After making some required improvements in the “H.264 AVC/SVC” it becomes more popular as H.265/HEVC. Tew et al. in [36] also projected an algorithm for watermark embedding in the HEVC domain. In this algorithm he used coding block size pronouncement on every coding tree. In this method he embedded the watermark in the non-zero DCT coefficients. In [27] the watermark is embedded in the least significant bits of the non-zero quantized transform coefficients those are selected at the time of indoctrination phase.

2.9.2 SPATIAL DOMAIN

In this method, the embedding and extraction of the watermark is a simple process. The watermark is inserted in the pixel domain and can be extracted by spread spectrum modulation. Since its method of extraction is also a simple process so it can be detected very easily from the host signal and in that case, its uniqueness can't be claimed [18]. In the spatial domain we have direct pixels values and all the values are stored as an output of CCD array. An image after the sampling is having the defined values. The most ordinary format is used for a sampled image is rectangle blocks and these blocks are positioned on a rectangular grid.

Block-based: This method is used to embed the watermark in the spatial domain only. Here they divide the target image into some fixed number of blocks and then embed the watermark into each block of the image. The embedding process is done by after checking the intensity level of the target image. These kinds of algorithms are simple and computationally efficient.

2.9.3 TRANSFORM DOMAIN

The meaning of transform is ‘convert’ or ‘make-over’. So a transform domain is just converting the normal pixels values of a frame into the frequency (High level and Low level). For the conversion of a frame into the frequency domain most commonly used methods are “singular value decomposition” (SVD) [37], “discrete wavelet transform” (DWT) [21, 21], “Discrete Fourier transform” (DFT) [38, 39], discrete cosine transform (DCT) [[25, 26] and dual-tree complex wavelet transform (DT CWT) [40]. Every transform domain is having its own distinctiveness for representing the video frame at a different level of frequency. For the watermark embedding process firstly convert the video frames into the frequency domain and adding the watermark bits into that frequency to generate the watermarked frame. The transform domain is highly recommended for achieving the better imperceptibility and robustness.

For the next analysis we considered an approach that was proposed by Mr. Zhang et al. [41]. In this method he has taken the surveillance videos. In this method, a privacy information known as a watermark has been embedded in the video and it will become invisible to everyone. In this method the author used the concept identity sensor that will detect to authorize person and also extracted the matching object in every frame and the resultant frame is compressed and encrypted as well.

In December 2013 Hanieh Khalilian [42] proposed an algorithm for video watermarking. The encoding of watermark was in the wavelet domain, but he decoded the watermark with the help of PCA. He also used a scene changed detection algorithm so that he can select the target frame where the watermark is to be embedded. But this algorithm also was not suitable for the protection of watermark pattern and quality of extracted watermark.

In 2018 Zoran S. et al. also proposed a digital watermarking algorithm. They embed the watermark inside the blue chrominance channel of original video frame. They also increased the security of embedded watermark by scrambling before insertion of it. For the scrambling process they used chaotic GMSAT map.

In 2018 Houria Kelkoul et al. also proposed an algorithm to protect the cinema piracy that also the part of digital video copyright protection. Here in this method they processed a video sequence in the form of audio and video and they also extract an audio fingerprinting pattern which was embedded in video frame as a watermark. To find out the low and high energy of the original frame they used discrete wavelet transform for watermark insertion.

2.10 CONCLUSION

After analyzing all the previous results on the above topic, We came to the conclusion that almost every author used transform domain to embed the watermark but the results obtained from the process was not satisfactory in terms of robustness of the extracted watermark which means we can have some scope for the improvement in the quality (robustness and imperceptibility) of the extracted watermark.

CHAPTER 3

A METHOD OF DIGITAL COPYRIGHT PROTECTION BY IMPLEMENTING OF SWEA FOR DIGITAL VIDEOS

3.1. INTRODUCTION

Digital video watermarking is an emerging field and significant technique of caring the analytical belongings and exclusive rights of the digital videos. Here in this method, we have proposed a new “digital video watermarking algorithm” that is (SWEA) [28]. This method has three important parts, the first one has split the watermark into small pieces with the help of this algorithm, for the second one embed the diminutive pieces of the watermark into the LL-2 frequency coefficients of I-frames of digital video and the last one is recover these small pieces of the watermark and combine them in a resourceful manner. The watermark data has to be embedded into the low frequency coefficients on the basis of the energy of high frequency. In this method we also achieved the highest robustness of the watermark. This method is also resists many attacks i.e. compression, frame averaging and Gaussian noise. Till this date, a lot of work has already been done in the field of protecting the copyright’s of the videos by making use of various legal processes and procedures. Though all these methods are good enough but still we witness so many cases where the original owner finds it difficult to prove his/her legal ownership due to lack of evidences. In order to tackle this major problem of the internet world, some way has to be designed. The project of “A robust and encrypted approach for digital video copyright protection” has been designed with the intention of dealing this puzzling situation.

The system will embed a secret information/secret code into the video file which will serve as a strong evidence at time of claiming the ownership of whoever it originally belongs to, thus successfully protecting the his/her copyright. Usually the practice of embedding a file, message, image or a video into another file, message, image or a video is termed as “Steganography”. It is widely used to share secret and sensitive information without getting noticed in field of multimedia .It’s main agenda is to share or transmit secret information to the intended person without leaving any room for it to be detected. The advantage of steganography over encryption is

alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal.

The proposed system will make use of technique similar to steganography but is different in many ways. Most importantly, in Steganography the main purpose is to transmit the secret information whereas this system includes embedding secret information which could be an image into a video file for the sole purpose of protecting the copyright of the owner. Here, our concern is that the video file with encrypted code should be as good as the original video file rather than focusing on the quality of the embedded information. The general working of the system can be depicted as:

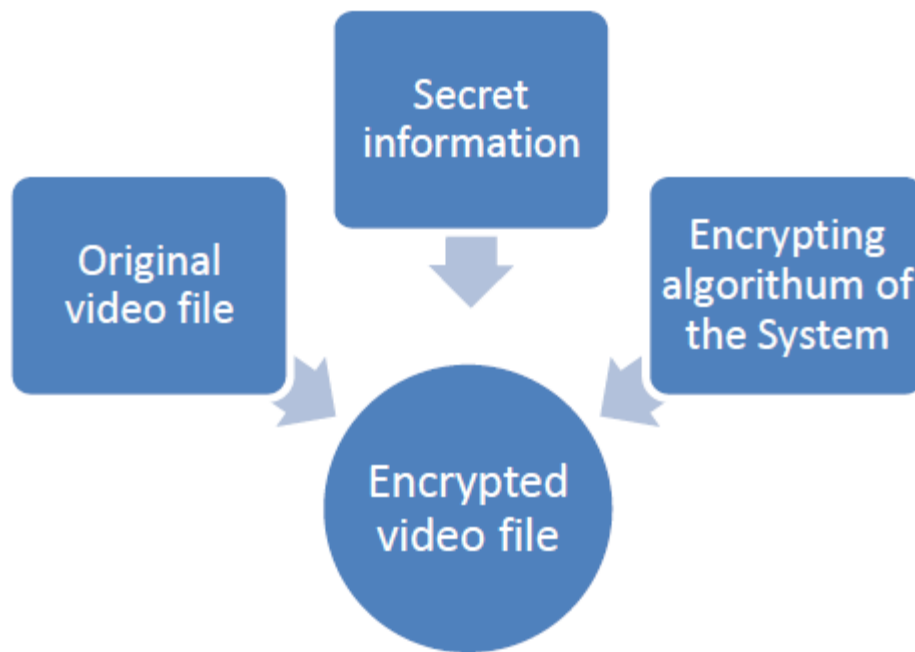


Figure 3.1: General watermarking systems.

In case, the user faces a situation where he has to claim for his ownership this secret information can be extracted back from the encrypted video by making use of decrypting algorithm. This again can be done in similar manner.

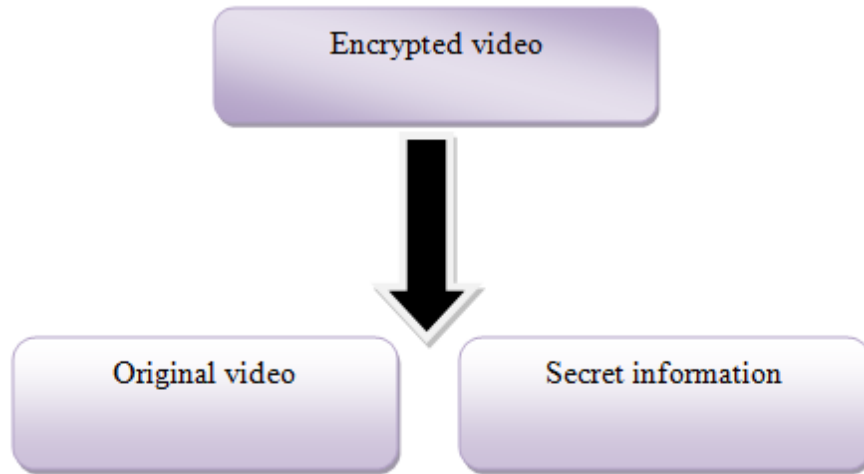


Figure 3.2: Watermark decryption process

Further, this process can be explained and simplified to through light upon its working and to give a better idea of how this proposed system actually manages the entire process of encrypting and decrypting the video file. The detailed process is little lengthy and can be explained through a series of steps.

1. Take the copyright information and perform the encryption operation upon the information using Encryption algorithm. The generated encrypted code is in unreadable format.
2. The above encrypted code is generated using secret key for the security purposes and could not be decoded unless the user knows the secret code.
3. This encrypted code is taken up to be embedded in the video file using embedding algorithm. This operation gives the desired output that is watermarked video.
4. The Watermarked video is taken as input and the de-embedding operation is carried out using de-embedding algorithm to retrieve the copyright information.
5. The above steps gives us encrypted code which could only be decoded using secret key which was earlier used in the encryption process.
6. Using the secret key, the encrypted code is decoded to obtain the original copyright information.

And we have also acquired the secret code from the video file which is used to calculate **PSNR (peak signal to noise ratio)**. It serves the purpose of finding out the difference between the embedded and extracted secret code image.

The above detailed process can be very well explained and depicted using a block diagram in which each and every step can be very easily showcased. So the Block diagram of the proposed system is:

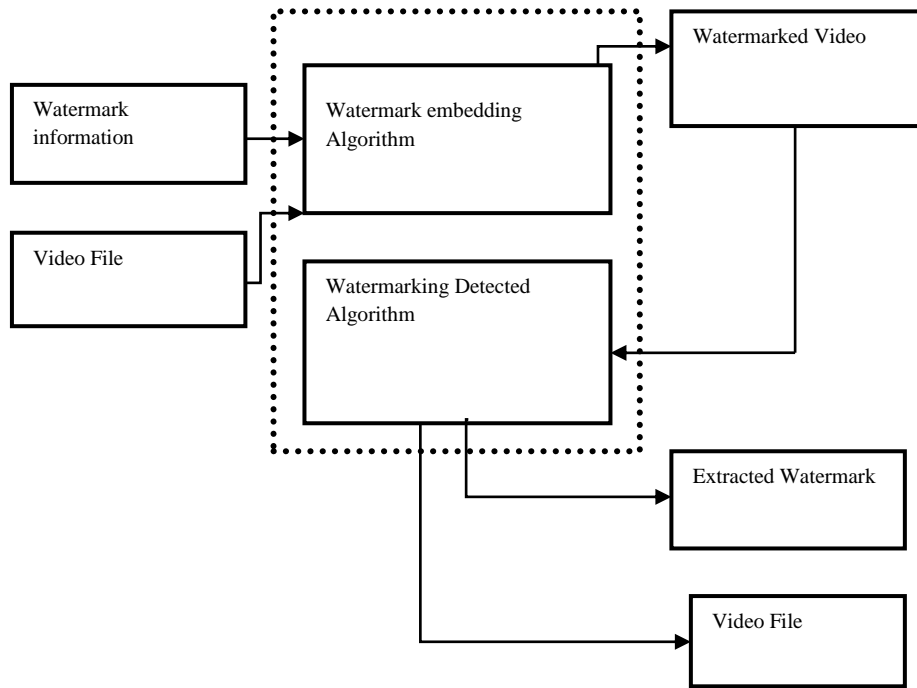


Figure 3.3: Block diagram of watermark embedding process

In this given diagram the video file is taken and the copyright information is taken and both are given as input to the encryption algorithm which produces the desired watermarked video which contains the copyright information in the encrypted format. In order to prove the ownership over a video file the user gives the watermarked video as input to the decrypting algorithm and which gives the original video and encrypted copyright information as output.

The detailed version of this embedding process can be shown with the help of another block diagram.

Watermark Embedding Process:

In this block all the actions constitute towards the achievement of the watermarked video file. There are several steps which are being carried out in-order to obtain the water marked video. The various steps involved are as follows:

- i.) Take the copyright information and perform the encryption operation upon the information using Encryption algorithm. The generated encrypted code is in unreadable format.
- ii.) The above encrypted code is generated using secret key for the security purposes and could not be decoded unless the user knows the secret code.
- iii.) This encrypted code is taken up to be embedded in the video file using embedding algorithm. This operation gives the desired output that is watermarked video.

Watermark Detection Process: [29]

It is the inverse of the embedding block. In other words the action carried out in the block of proposed system is totally opposite of that carried out in the embedding block. The various steps involved are as follows:

- i.) The Watermarked video is taken as input and the de-embedding operation is carried out using de-embedding algorithm to retrieve the copyright information.
- ii.) The above steps gives us encrypted code which could only be decoded using secret key which was earlier used in the encryption process.
- iii.) Using the secret key, the encrypted code is decoded to obtain the original copyright information.

The de-embedding block is performed in case the owner needs to claim his/her ownership over a video which indeed belongs to him/her. Otherwise, the embedding process is what is more commonly used.

For the purpose of security reasons and to make this Proposed system robust under attack the system allows only single embedding of code. Once a code is embedded in a video, no user can embed the code second time, thus multiple embedding of code is prohibited.

3.2. BACKGROUND

The prospect expansion of the digital video copyright security products essentially depends on the actual network. In the current scenario, a vast quantity of multimedia data has been shared on the internet but the required security is not enough to stop it. In the literature survey, we also go through a range of proposed algorithms for the data security and copyright protection. The concept of watermarking is more demanding and it is not only limited to the identification of the copyright owner, we also used it as an actual proof of ownership. A main problem occur when an intruder or unauthorized user uses some kinds of editing tools to replace the actual watermark with his own watermark and then claims to have possession of the copyright himself. In the beginning of the watermarking systems, the main problem came into the picture that the watermark detector tools were easily available to the intruder. Therefore, the intruder replaces the owner's watermark with his own watermark in order to claim the ownership of the video. But in the absence of the detector, the removal of a watermark by an adversary is the extremely difficult job. However, in some cases if intruder is not able to remove the watermark, then adversary might try to destroy the host signal by embedding his own watermark with the help of his own watermarking system. This problem can be resolve by using an algorithm which can prove that the intruder's image is derived from the original watermark image instead of directly embedding watermark signal in the host image. Here, we have proposed a novel method of copyright protection technique, SWEA.

3.3. PROPOSED METHOD

For our result experiments, we have taken a gray image of (256 x 256) as a watermark and a video sequence name as a foreman video. To get the total number of the scene changed of foremen video, we have to apply SCD (Scene Changed Detection) algorithm [30] on it and after applying this algorithm we got 77 scene changed frames. For embedding the watermark into the frames, we have to pre-process the watermark as well as target video which we have shown in figure 3.4 and figure 3.5 respectively.

3.3.1. SCD (SCENE CHANGED DETECTION)

Video is the most effective media for capturing the world around us. Video scene change detection is a fundamental operation used in many multimedia applications such as digital libraries, video on demand and digital watermarking. Scene change detection is the procedure for identifying changes in the scene content of a video sequence. Video data can be divided into different shots. A shot is a video sequence that consists of continuous video frames for one action. Scene change detection is an operation that divides video data into physical shots. The most common working process of the SCD is given below.

3.3.1.1. WORKING PROCESS FOR SCD

1. Read the video
2. Select no. of frames from video to detect scene change.
3. The frames which are selected from videos are converted to gray.
4. Applying edge function to the frames which represents 1's and 0's.
5. Divide every image into blocks of 4×4. Take mean of the blocks.
6. Set the threshold on trial and error basis as 0.5 for abrupt scene change and set 0.2 for gradual scene change detection.
7. Take the difference of images and then compare.
8. If the difference is greater or equal to 0.5, then there is a scene change taking place otherwise no scene change.
9. Display frame number and the frame/image where scene change is taking place.

3.3.2. WATERMARK PRE-PROCESS

Before embedding the watermark bits into a video, firstly we have to pre-process the watermark as per the given below equation 3.1. As already we have been explained that our watermark size is (256 x 256).

$$\left(4^n \leq m; n > 0\right) \quad (3.1)$$

In the above equation m is representing total no. of the identical frames and the watermark will be broken up in 4^n numbers. In the figure 3.4, we have shown the procedure of it.

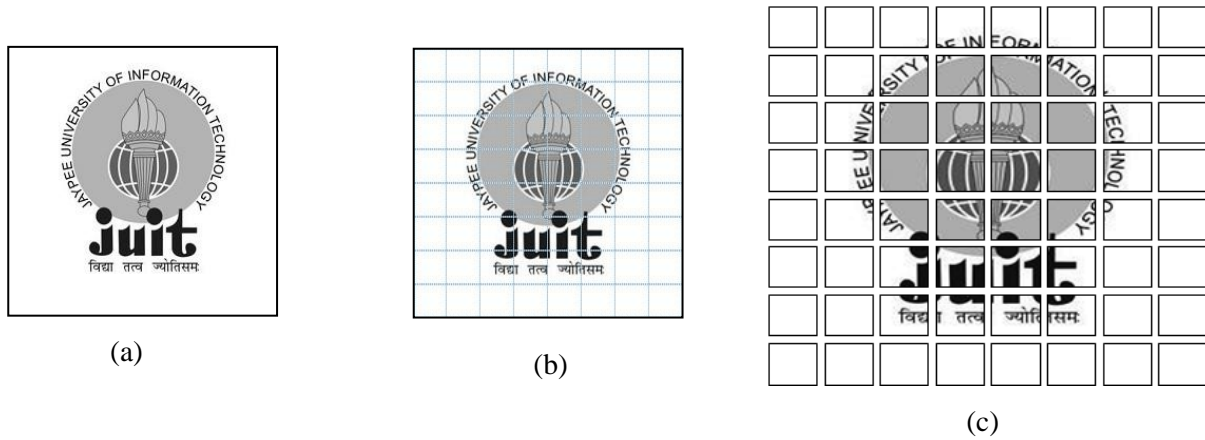


Figure 3.4: (a) Watermark Image. (b) Split as per proposed algorithm. (c) watermark blocks.

3.3.3. EMBEDDING ALGORITHM

1. Firstly apply SCD algorithm on the host video (O_{video}) and also segregate each scene into non-overlapping GOPs. Each GOP has an I-frame. For embedding the watermark find out all the I-frames of the input video.

$$WmI_i = k \times (Lf_2) + q \times (Wm_2)$$

WmI_i is representing watermarked I frame, Lf_2 is representing low-frequency approximation I-frame Wm_2 is representing a watermarked data, where k is the scaling factor for the target frame & q is for the watermark image.

2. Watermark Image W is the size of (256 x 256). Calculate all the small blocks of the watermark as per the proposed algorithm in which $4^n \leq m$.

4^n is representing the entirety number of small blocks of the watermark ($W_1, W_2, W_3, \dots, W(4^n)$) n is the number of rows or columns and m is representing total number of scene changed frames.

3. Where the watermark block (x,y) = $\left[\left(\sqrt{4^n} \right) * \left(\sqrt{4^n} \right) \right]$

4. While $m \geq 4^n$, $I_i = W_4^n I_i$, I_i is representing original I-frame, $W_4^n I_i$ = is representing watermarked I-frames, i is a constant value up to m , 4^n is representing the whole number of watermarked pieces and $n > 0$.
5. Take 2^{nd} level coefficients of DWT of I_i
for $i = 1 : m$
 $[Ca_i, Ch_i, Cv_i, Cd_i] = DWT2(I_i, \text{"haar"})$
 $j=i+1$
 $[Ca_j, Ch_j, Cv_j, Cd_j] = DWT2(Ca_i, \text{"haar"})$
6. The first block of watermark has to be embedded in the low frequency coefficients of step 5 which are Ch_i, Cv_i, Ch_j, Cv_j . After embedding new coefficients will becomes $WCh_i, WCv_i, WCh_j, WCv_j$
7. Apply the inverse of DWT to the watermarked frames. W_f , where $f=1,2,3,\dots,4^n$.

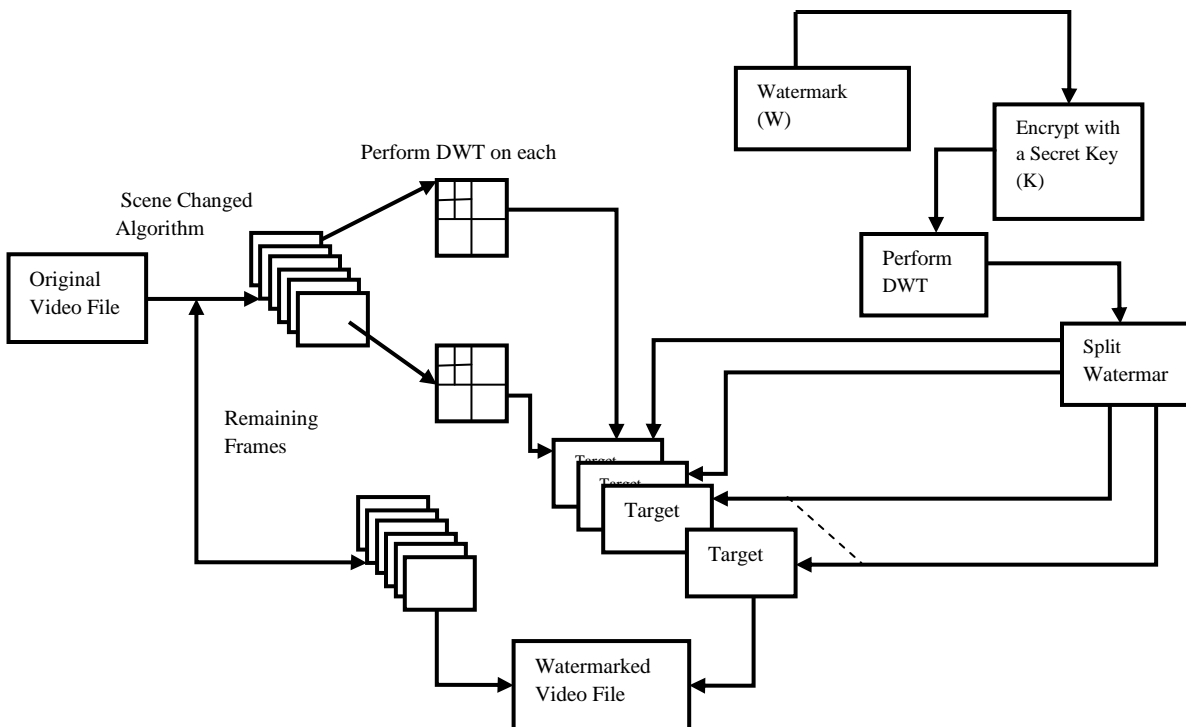


Figure 3.5: Calculating the target frames before embedding the watermark

3.3.4. DETECTION ALGORITHM

1. Firstly apply SCD algorithm [30] on the host video and then apply the SCD algorithm on the imaginative videotape sequence (O_{video}) and also segregate all picture into non-overlapping GOPs. And also apply the DWT on the watermarked frame and original frame.
2. Now calculate the difference of LL-1 low frequency coefficients of the watermarked frame and the LL-1 low frequency coefficients of original I-frame which are WCh_i , WCv_i , Ch_i and Cv_i respectively.

$$\text{Now, } A_x = WCh_i - Ch_i$$

$$B_y = WCv_i - Cv_i$$

3. Calculate cross-correlation of A_x & B_y and the detail coefficients of original watermark.
4. If relationship = = high
Watermark detected.
else
go over from step 3.
else if
Take 2nd-level low frequency coefficients and replicate from step 3 in the anticipation of detected watermark not match
else
Watermark not found.

3.4. EXPERIMENTAL RESULTS

In order to apply SWEA, new video 'Foreman' of the aspect of "352 x 288" and the dimension of "256 x 256" real watermark image is used. In the below Figure 3.6 represents original video frames, Figure 3.7 represents watermark blocks after applying SWEA algorithm, Figure 3.8 represents watermarked frames, Figure 3.9 represents extracted watermark blocks. Finally we applied merging technique and get the actual extracted watermark in figure 3.10 & 3.11.

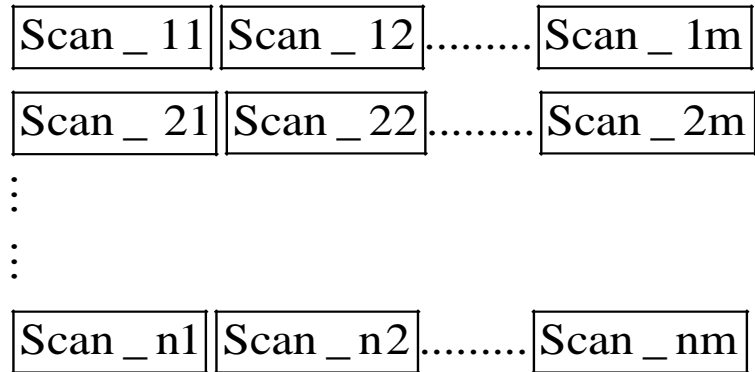


Figure 3.10: Watermark extracted blocks in matrix form

Scan _ 11	Scan _ 12	Scan _ 1m
Scan _ 21	Scan _ 22	Scan _ 2m
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮
Scan _ n1	Scan _ n2	Scan _ nm

Figure 3.11: Extracted watermark blocks with merging process



Figure 3.12: Extracted Watermark for foremen video after applying merging technique.

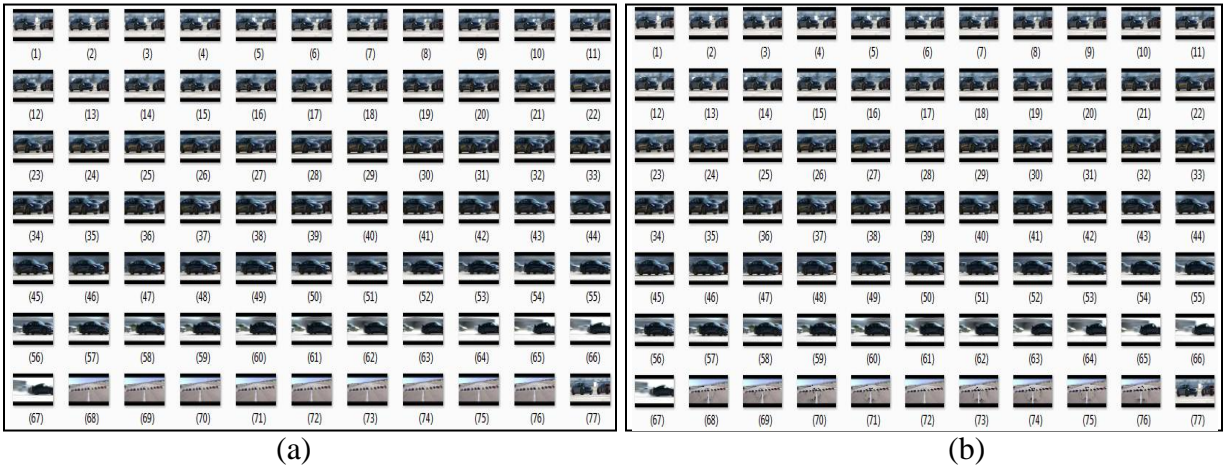


Figure 3.13: (a) Original car race frames (b) Watermarked car race frames



Figure 3.14: Extracted Watermark for car race video after applying merging technique.

Splittance of all the above figures is based on equation 3.1 where number of scene changed frames should be greater than equal to number of watermark Splittance.

In TABLE 3.1 and TABLE 3.2 we have shown the results in terms of PSNR and MSE for different size of watermark for wakna road and foreman video. According to our result analysis we found that if the size of watermark is very small then we get the highest PSNR of watermarked video but we also analyze that in this case the mean squared error will increase gradually.

Table 3.1: PSNR and MSE for wakna road watermarked video at different size of watermark

Size of inserted watermark	Watermarked video (PSNR) in dB	Extracted Watermark (MSE)
“8 x 8”	51.10	5.97
“16 x 16”	49.88	6.26
“32 x 32”	43.13	6.91
“64 x 64”	41.87	7.31
“128 x 128”	41.03	7.69
“256 x 256”	40.91	7.84

Table 3.2: PSNR and MSE for Foremen watermarked video at different size of watermark

Size of inserted watermark	PSNR (dB)	MSE
8 x 8	48.1001	6.3544
16 x 16	47.6682	7.0188
32 x 32	45.8523	7.3765
64 x 64	44.4006	7.4648
128 x 128	43.3987	7.4893
256 x 256	41.3812	7.4982

In the figure 3.16 we evaluate our algorithm with author H. Khalilian et al [27] by performing frame repetition attack on the foreman frame in order to calculate the bit error rate (BER). By this progression, we get the better result in comparison of [27] and [20].







	Gamma correction 0.5	Gamma correction 2	Gamma correction 4
Video frame	 PSNR=25.34 dB	 PSNR = 19.80 dB	 PSNR = 13.54 dB
Extracted watermark	 PSNR=27.29 dB	 PSNR=26.73 dB	 PSNR=21.24 dB

Figure 3.15: PSNR of watermarked frame and extracted watermark after Gamma Correction

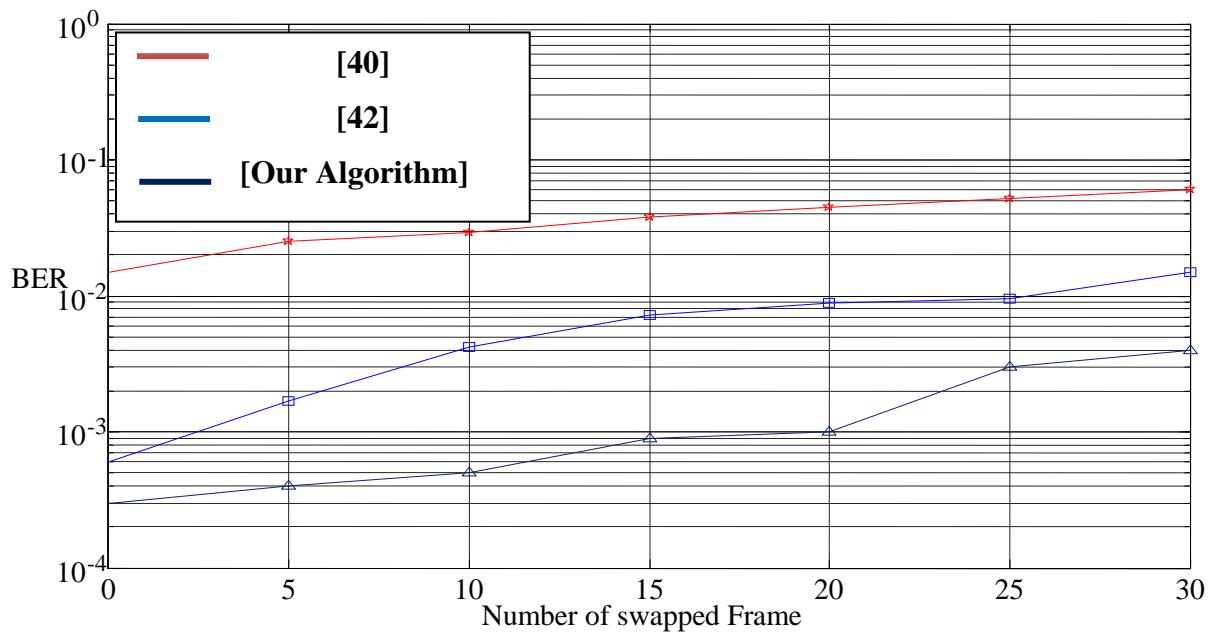


Figure 3.16: BER (Log Scale) under temporal attack for foreman video (Frame Repetition)

3.5. CONCLUSION

Embedding of the watermark in a video in transform domain becomes more challenging because there are lots of algorithms available with the intruders. So we have to embed a watermark that has the maximum robustness and also should not humiliate the eminence of original media. In this chapter we have shown a different process of watermark insertion that is more robust and secured in comparison of previous methods. Here we used SWEA that is providing the great level of satisfaction in terms of security and robustness. But the computational time complexity for watermark embedding as well as watermark extracting is also high because of the watermark has been divided into small pieces. So embedding the each block of watermark inside the video frames (one after another) is maximizing the computational time complexity.

As per the current status of this work, it is developed as well prepared to handle the copyright information in the efficient way. Efforts have been made to make it robust and secure so that it works to meet its purpose.

CHAPTER 4

A DIGITAL VIDEO COPYRIGHT PROTECTION TECHNIQUE ZPA ALONG WITH SWEA

4.1. INTRODUCTION

Digital copyright protection has played a significant role in protecting the multimedia stuffing from illegitimate use and illegal users and also helpful in proving the ownership. In order to claim the ownership of a video, there are definite safety programs which is also called watermark is embedded in the video. In this paper, we have introduced a new technique, “SWEA (Split watermark embedding algorithm)” along with “Zero Padding Algorithm” (ZPA) [5] for the exclusive rights protection of digital videos. By applying “split watermark embedding algorithm” (SWEA), it is not easy to recognize the exact blueprint of watermark and by ZPA, we minimize the perceptual degradation of the watermarked video and also improve the imperceptibility. For the watermark embedding, we are using db1 domain of wavelet transform. Watermark insertion is done in the LL sub-band based on the energy of high frequency. For the watermark insertion, we have taken I-Frame of the video. Here we also used SCD algorithms [43] to find out the I-frames. After getting these frames, we pre-process our watermark image as per our proposed method. The proposed algorithm passed through different kinds of attacks, such as compression attack, uniform noise attack, Gaussian noise attack and frame repetition and frame averaging attacks [14], [16], [44, 45]. It also sustains all the above attacks and provides the improved results in comparison of the literature.

4.2. BACKGROUND

The term of copyright belongs to a branch of law that grants an author, (where he is a writer, artist, musicians or another creator) protection of their work. Under the law of copyright, authors are entitled to protection against illegal or unauthorized use of their original contribution.

Digital watermarking techniques have been studied extensively. In this era, extensive use of video-based applications is growing which include the internet, multimedia, video recorder,

video conferencing, etc. which increases the demand to secure the videos. The video watermark technique is having a different extension and also more complicated than the image watermark technique [46-48].

For the blind watermarking algorithm, it does not required the host data for extracting the watermark from the watermarked video. Only we required the secret key that we used at the time of watermark embedding process. Even without key we also can extract the watermark information if we are not needed the additional security. In the semi-blind method [6] it required some information of the host data for extracting the watermark information. It is not purely depend on the host data but require some information of the original data. In the non-blind watermark extractin process we required the complete information of the original data and then we processed the original data and watermark data to extract the watermark information. The complete classification we have already explained in table 2.1.

In 2007 Jin-Seon Young et al. proposed a TDWIA (Time-Division Watermarking Inserting Algorithm). This algorithm inserts pieces of watermark images into several original video frames during the short time (about 1/20 ~ 1/30 seconds). This algorithm was able to insert the copyright information into original video frames to reduce the distortion. But the PSNR of extracting copyright information was not satisfactory. And the copyright information was not secure as it could be easily detected the pattern of inserting watermarks (copyright information).

In December 2013 Hanieh Khalilian [6] proposed an algorithm for video watermarking. The encoding of watermark was in the wavelet domain, but he decoded the watermark with the help of PCA. He also used a scene changed detection algorithm so that he can select the target frame where the watermark is to be embedded. But this algorithm also was not suitable for the protection of watermark pattern and quality of extracted watermark.

In the literature review [14], [16], [44], [45] we have studied that an attacker may crack or damage or detect watermark after applying the possible combination of algorithms but in the case of SWEA it is very difficult to extract the watermark information. Even in the case of SWEA it is very dificult to understand the blueprint of inserted watermark. In this paper we used the concept of SWEA to make it more secured and used the ZPA to improve the visual quality of the watermarked data.

To demonstrate the rights of a video is a big challenge. If a video becomes popular all of a sudden and people like to watch it over and over again or any video which can be a claim offense or innocence of a person then the price/cost of these videos hikes a lot. In this case, many people claim the ownership of the video.

To find out the authorized/legal owner out of all multiple people claiming the ownership, we perform the Digital Video Copyright Protection and this whole process is named as ownership proof. In the previous chapter we have shown that how we have applied SWEA & ZPA collectively to the input (watermark and video file) and to extract or detect the watermark, applied reverse or inverse.

For many years, researchers have done their work in this field to protect the copyright of any multimedia document [1] and they have succeeded in achieving the same, but on the other hand, many hackers or attackers have also found out the way to crack or break the copyright technique.

4.3. PROPOSED METHOD

In the proposed method, a gray image with the dimension of “256 x 256” is used as a watermark signal. As a gray image has 256 levels so 8 bits can represent each pixel. For the watermark embedding process, we have taken two video sequences first is ‘Foreman’ and the second is ‘Car_race.mp4’ video sequence. In the next process we have performed the SCD method on these video sequences and find “77 and 97 scenes changed frames respectively”. In this algorithm, earlier than embedding the watermark information we have to pre-process the watermark image and original media.

4.3.1 SWEA

Here we used the SWEA to split the watermark into small pieces as per the total number of frames we obtain from the video. In the development of watermark embedding, firstly we have to scaled the watermark with the help of this equation 4.1.

$$\left(4^n \leq m; n > 0\right) \quad (4.1)$$

In Figure 4.1 and 4.4.2, we have used 2-level ‘db1’ wavelet transform on both video sequence and watermark, to obtain the higher (HH, HL) and lower frequency band (LL LH) [11], [12]. After performing 2-DWT on each I-frame (Identical Frame) of video, we get LL-2 (2nd Level low frequency band), which is named as (Lf_2).

We are also applying the 2-DWT technique on each split watermark block and obtain LL-2, which is named as (Wm_2) and multiplied by a scaling factor β . After getting scaled (Wm_2) and (Lf_2) we add them with the help of ZPA (Zero Padding Algorithm) then apply IDWT (Inverse discrete wavelet transform) on video frame (Lf_2) and the result gets stored in WmI_i

$$WmI_i = (Lf_{2_i}) + \beta \times (Wm_{2_i}) \quad (4.2)$$

Wavelets are a more general way to represent and analyze multiresolution images and it can also be applied to 1D signals. Wavelets are very useful for image compression and removing noise.

We don’t need to calculate wavelet coefficients at every possible scale. It can choose scales based on powers of two, and get equivalent accuracy.

$$\psi_{j,k}(x) = 2^{j/2} \psi(2^j x - k) \quad (4.3)$$

We can represent a discrete function $f(n)$ as a weighted summation of wavelets $\psi(n)$, plus a coarse approximation $\varphi(n)$

$$f(n) = \frac{1}{\sqrt{M}} \sum_k W_\varphi(j_0, k) \varphi_{j_0, k}(n) + \frac{1}{\sqrt{M}} \sum_{j=j_0}^{\infty} \sum_k W_\psi(j, k) \psi_{j, k}(n) \quad (4.4)$$

Where j_0 is an arbitrary starting scale, and $n = 0, 1, 2, \dots, M$

Now to find out the approximation coefficients we used equation 4.3. Approximation coefficients can be defined as the coefficients which contains the maximum information of the frame. Here in this part we are embedding the watermark information. But the embedding process should not distort the original approximate coefficients. So we are using the concept of ZPA (Zero Padding Algorithm).

Approximate coefficients

$$W_{\Phi}(j_0, k) = \frac{1}{\sqrt{M}} \sum_x f(x) \varphi_{j_0, k}(x) \quad (4.5)$$

Details coefficients

$$W_{\Psi}(j, k) = \frac{1}{\sqrt{M}} \sum_x f(x) \psi_{j, k}(x) \quad (4.6)$$

As above, we have shown equation 4.2 and that implies the procedure of embedding the watermark for i^{th} frame. So with the help of equation 4.2 we can drive the equation 4.7 and this equation is showing the procedure of embedding the watermark in a video.

$$W_{\text{video}} = \sum_{i=1}^m \left[(Lf_{2_i}) + q \times (Wm_{2_i}) \right] \quad (4.7)$$

4.3.2 ZPA

In the equation 4.2 we are adding, (Lf_{2_i}) and (Wm_{2_i}) and their matrices dimensions are (72×88) and (8×8) respectively. But according to matrices property, we can add two matrices if and only if they are of the same dimensions. So with the help of ZPA we are converting the matrix of (Wm_{2_i}) as the same as of (Lf_{2_i}) . The original matrices are

$$(Lf_{2_i}) = \begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,88} \\ a_{2,1} & a_{2,2} & \dots & a_{2,88} \\ \cdot & \cdot & \cdot & \cdot \\ a_{72,1} & a_{72,2} & \dots & a_{72,88} \end{bmatrix}, (Wm_{2_i}) = \begin{bmatrix} b_{1,1} & \cdot & \cdot & \cdot & b_{1,8} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ b_{8,1} & \cdot & \cdot & \cdot & b_{8,2} \end{bmatrix} \quad (4.8)$$

In equation 4.8, matrix dimensions of (Wm_{2_i}) being 8x8. But after applying ZPA on (Wm_{2_i}) the matrix dimensions will be changed in respect of (Lf_{2_i}) as in equation 4.9.

$$(Lf_{2_i}) = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdot & \cdot & \cdot & \cdot & \cdot & a_{1,87} & a_{1,88} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{36,1} & a_{36,2} & \cdot \cdot & a_{36,44} & a_{36,45} & \cdot \cdot & a_{36,87} & a_{36,88} \\ a_{37,1} & a_{37,2} & \cdot \cdot & a_{37,44} & a_{37,45} & \cdot \cdot & a_{37,87} & a_{37,88} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{72,1} & a_{72,2} & \cdot & \cdot & \cdot & \cdot & a_{72,87} & a_{72,88} \end{bmatrix} \quad (4.9)$$

$$(Wm_{2_i}) = \begin{bmatrix} 0_{1,1} & 0_{1,2} & \cdot & \cdot & \cdot & \cdot & \cdot & 0_{1,87} & 0_{1,88} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0_{33,1} & 0_{33,2} & \cdot & \cdot & \cdot & \cdot & \cdot & 0_{36,87} & 0_{36,88} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0_{40,1} & 0_{40,2} & \cdot & \cdot & \cdot & \cdot & \cdot & 0_{37,87} & 0_{37,88} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0_{72,1} & 0_{72,2} & \cdot & \cdot & \cdot & \cdot & \cdot & 0_{72,87} & 0_{72,88} \end{bmatrix} \quad (4.10)$$

4.3.3 EMBEDDING ALGORITHM

1. **Input** Original video sequence (O_{video}), Watermark (W) [256, 256]
2. Extract scene changed frame (I), Total number of scenes changed frames= m

3. SWEA

while $m \geq 4^n$

$$\text{size of watermark blocks } Wb(x,y) = \left[\frac{256}{\sqrt{4^n}} \times \frac{256}{\sqrt{4^n}} \right]$$

4. Perform 2^{nd} level DWT of I_i

for $i = 1 : m$

$$[Ca_i, Ch_i, Cv_i, Cd_i] = \text{DWT2}(I_i, \text{"db1"})$$

$j=i+1$

$$[Ca_j, Ch_j, Cv_j, Cd_j] = \text{DWT2}(Ca_i, \text{"db1"})$$

Calculate size of Ca_j

$$[p \ q] = \text{size}(Ca_j)$$

1. ZERO PADDING in watermark block

$$Z = \text{zeros}(p,q), \text{ size of } Wb = [x \ y]$$

Insert the values of Wb in Z

$$\text{Row value insertion at } Z\left(\frac{p-x}{2} + 1 : \frac{p-x}{2} + x\right)$$

$$\text{Coulmn value insertion at } Z\left(\frac{q-y}{2} + 1 : \frac{q+y}{2}\right)$$

Now, Zero padded watermark = ZW

2. Insert the zero padded watermark ZW into Ca_j

3. Now new coefficients will be

$$\text{mod } Ca_i, \text{ mod } Ca_j$$

Take IDWT of modified coefficients

4. Finally get the zero padded watermarked frame (EW_f)

and watermarked video (EW_{video})

4.3.4 DETECTION ALGORITHM

1. **Input** watermarked video (EW_{video}), Original Video (O_{video})
2. Take watermarked frame (EW_f) from (EW_{video}) Original frame (I_i) from (O_{video})
3. Subtract 1-level approximate coefficients of watermarked image (EW_f) from the 1-level approximate coefficients of I-frame (I_i) Now, $NewCa_i = \text{mod } Ca_i - Ca_i$
4. Calculate cross-correlation between $NewCa_i$ and original watermark block
If correlation = high
Watermark detected.

else
go over from step 3.

else if

Obtain 2nd-level detailed coefficients and go over from step 3 until the detected watermark not matched.

else

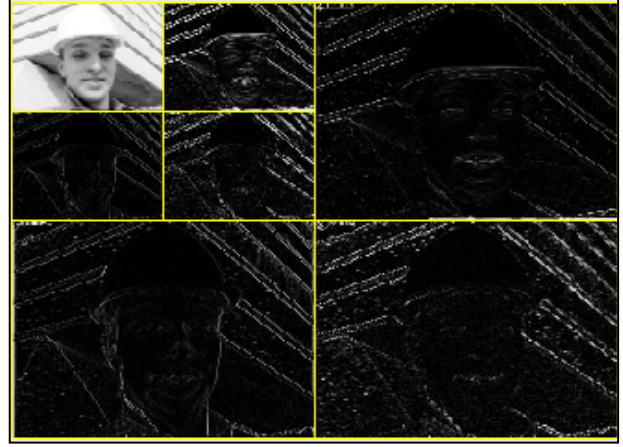
Watermark not found.

4.4. EXPERIMENTAL RESULTS

In this section, we have taken two parameters, imperceptibility, and robustness for the result analysis. For the result examination, we have taken two videos named as 'foreman. yuv' and 'car_race. mp4' with the aspect of "288 x 352" and "640 x 360" respectively. For the watermark image, we have taken juit logo with the dimension of 256 x 256. For comparison and analysis, we have taken two references [4] & [33]. In Figure 4.1 and 4.2, we have shown the original video frames (foreman.yuv and car_race.mp4 respectively) and their 2-Level decompositions.



(a) Original gray foreman video frame.

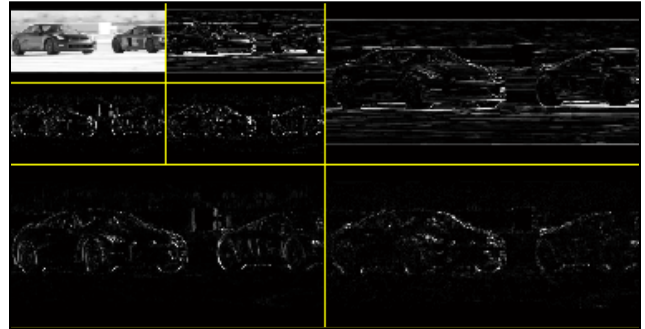


(b) 2-Level De-composition of foreman video

Figure 4.1: Original foreman video frame and their decomposition.



(a) Original car_race video frame.



(b) 2-Level De-composition of the car_race

Figure 4.2: Original car race video frames and their decomposition

In Figure 4.1 (b), we can see there are two types of rectangle blocks, the first one is (144×176) named as [LL-1 LH-1 HL-1 HH-1] and second (72×88) named as [LL-2 LH-2 HL-2 HH-2] starting from the upper left corner. LL-2 is known as the approximate coefficient of the 2nd level de-composition and LH-2, HL-2, & HH-3 are known as detailed coefficients of the 2nd level de-composition. For the watermark embedding we are considering LL-2 part.

After embedding the first block of the watermark from juit logo in LL-2 of figure 4.1(b) and 4.2(b), we have taken IDWT (Inverse discrete wavelet transform) of these two figures that become figure 4.3(a) and 4.3(b). Here in the figure 4.4 we have shown the extracted watermark blocks and in the figure 4.5 shown the final extracted watermark. In the figure 4.6, we are calculating the bit error rate on log scale under the spatial attack for foreman video.



(a).Watermarked Foreman video frame.



(b). Watermarked car race video frame

Figure 4.3: Watermarked frames (after embedding the first block of the watermark).

4.4.1 COMBINED SMALL PIECES OF EXTRACTED WATERMARK

In the merging process firstly detect all the watermark pieces by using of watermark detection algorithm e.g. (explained in previous chapter) and then collect all the blocks of detected watermark. After this process arrange all the blocks of watermark in ascending order as they were detected. In the end, apply the inverse of watermark split algorithm on the small blocks of detected watermark.

Scan x, y

Where x belongs to number of rows and y belongs to number of columns.

In the figure 4.4 we have an image of an object that generated by the proposed watermark split algorithm. Now collect all these pictures in the program folder with their token number and also provide a name to all the pictures. As per the dimensions of the original watermark, we generate

a matrices of zeros and embed all the small blocks of detected watermark image in the zeros matrices. In equation 4.11, we have shown the process of generating the matrices.

$$\begin{pmatrix} \text{image}[1] & \dots & \text{image}[n] \\ \vdots & \ddots & \vdots \\ \text{image}[n] & \dots & \text{image}[n \times n] \end{pmatrix} = \begin{pmatrix} [n[k] \ m[l]] & \dots & n[k]m[l] \\ \vdots & \ddots & \vdots \\ n[k]m[l] & \dots & n[k]m[l] \end{pmatrix} = \left[\sum_{i=1}^n n_i[k] \sum_{i=1}^n m_i[k] \right] \quad (4.11)$$

For the result analysis, we have taken an image of juit logo with the dimensions of 256 x 256, while after applying the SCD algorithm on the original videos we get total number of I-frames “77 and 97” for foreman and car race video correspondingly. Here we have extracted all the watermark blocks from foreman video and car race video after applying the watermark detection algorithm. After getting all the watermark blocks, we have merged them with the help of equation 4.11.

TABLE 4.1: Video PSNR (In dB) After watermarking

Sequence	Average PSNR	Maximum PSNR	Minimum PSNR
Foreman	53.29	59.14	50.31
Car_Race	50.09	56.64	49.85

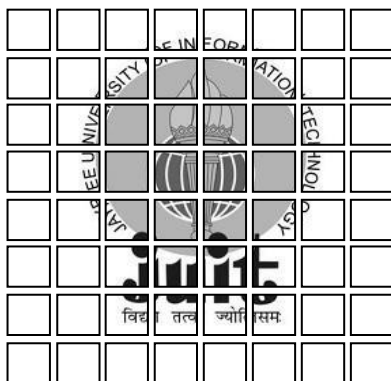


Figure 4.4: Extracted watermark blocks from Foreman video



Figure 4.5: Extracted complete Watermark from Foreman video

4.5. COMPARATIVE ANALYSIS

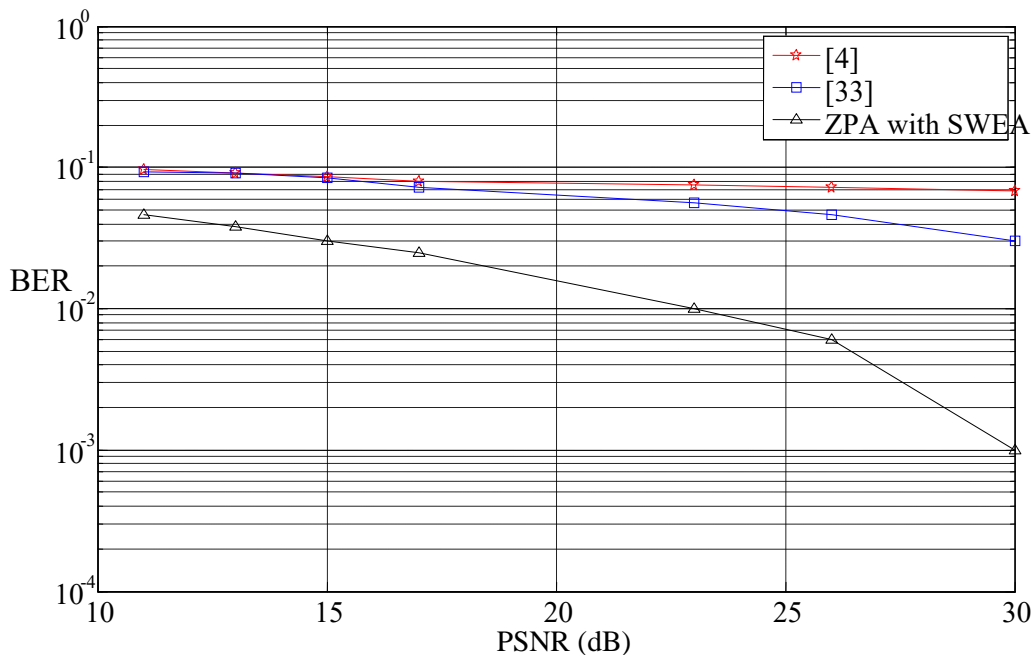


Figure 4.6: BER (log scale) under spatial attack (Uniform Noise)

4.6. CONCLUSION

Embedding the watermark information into the I-frame is much better because the I – frame has its own information, this frame is purely independent. But we found that I frame is very sensitive because it contains the original information and editing may degrade the quality of the frame. So in this case one more thing we analyse that I-frame is not possibly compressed that motivate us to embed the watermark information into the I-frame. After getting the result of our method we can say our method is supplementary adept because the value of extracted watermark is much improved than [4,33] in terms of PSNR and BER.

In the proposed technique we used SWEA and it provides a great security to our watermark, because no one can get the original pattern of inserted watermark and with the help of SWEA we also reduced the inserting bits as in the form of a watermark.

Using ZPA we are resizing the watermark dimensions in increasing order (in respect of original frame dimension) without adding the extra pixels. And that is why the proposed technique ZPA is used and it offers a high level transparency in between original and watermarked video.

So finally we can say that the videotape watermarking is an important necessitate of copyright protection and still many researshers are doing work in this field to make it more secure and robust. In the present time many researchers are working on the image security in transform domain but still we need to improve these domains. The copyright protection of digital videos is more demanding in the next 2-3 years so there is a huge range of improvement and study can be approved to create new methodology for digital video copyright fortification.

CHAPTER 5

CWEA: A DIGITAL VIDEO COPYRIGHT PROTECTION SCHEME

5.1. INTRODUCTION

A method of protecting the copyrights of the digital media is known as digital watermarking. In this chapter, we have proposed an algorithm that is robust and secured, named as “Colored watermark embedding algorithm” (CWEA) [6]. The algorithm is partitioned in two significant parts; primary is YCbCr color system that we used to classify the luminance and chrominance and second one is embedding the 1st level detailed coefficients of Y components of the watermark added to the approximate coefficients (Cb and Cr) of the video frame. Insertion of the watermark is based on the high frequency of detailed coefficients. The process of watermark embedding is shown in fig. 13. For the result analysis we have performed many attacks (compression, Gaussian noise, Frame averaging etc.) on our proposed algorithm and it resists all the attacks in a best way. CWEA resists most of the attacks and provide better results in comparison of literature survey [50, 53]. Here in this thesis, we are using the non-blind watermarking scheme.

5.2. RELATED WORK

The embedding a secret code or a watermark inside the monochrome video was not a big challenge and we have already studied many algorithms for inserting the watermark inside the monochrome image or video. Because we required only single value for representing the pixel value of monochrome image. But in case of colored video or color image we require three values for representing a single pixel. So embedding the watermark inside a color frame is big challenging.



Figure 5.1: Top field in color space model



Figure 5.2: Bottom field in color space model

5.2.1 RGB

In the RGB [48] color domain, a color picture is presented by three values consist of three most important colors namely Red, Green and Blue, the combination of the discussed colors in different proportion can create any desired color. Figure 5.3 shows all the three components of a color image namely red, green and blue: as we can see in the figure the red, green and blue components have all the red samples, green samples and the blue samples respectively. For the more clarity about the RGB we have taken JUIT logo and converted into the RGB color space. As we can see in the Figure 5.3 in the left partitioned the JUIT logo is appears brighter in the red components whereas middle one is representing all the green components and right one is representing the blue components. Basically RGB color space is the most compatible way of representing an image or a video. A display like CRT or LCD represents the color pixels with their intensity that creates a true color object.

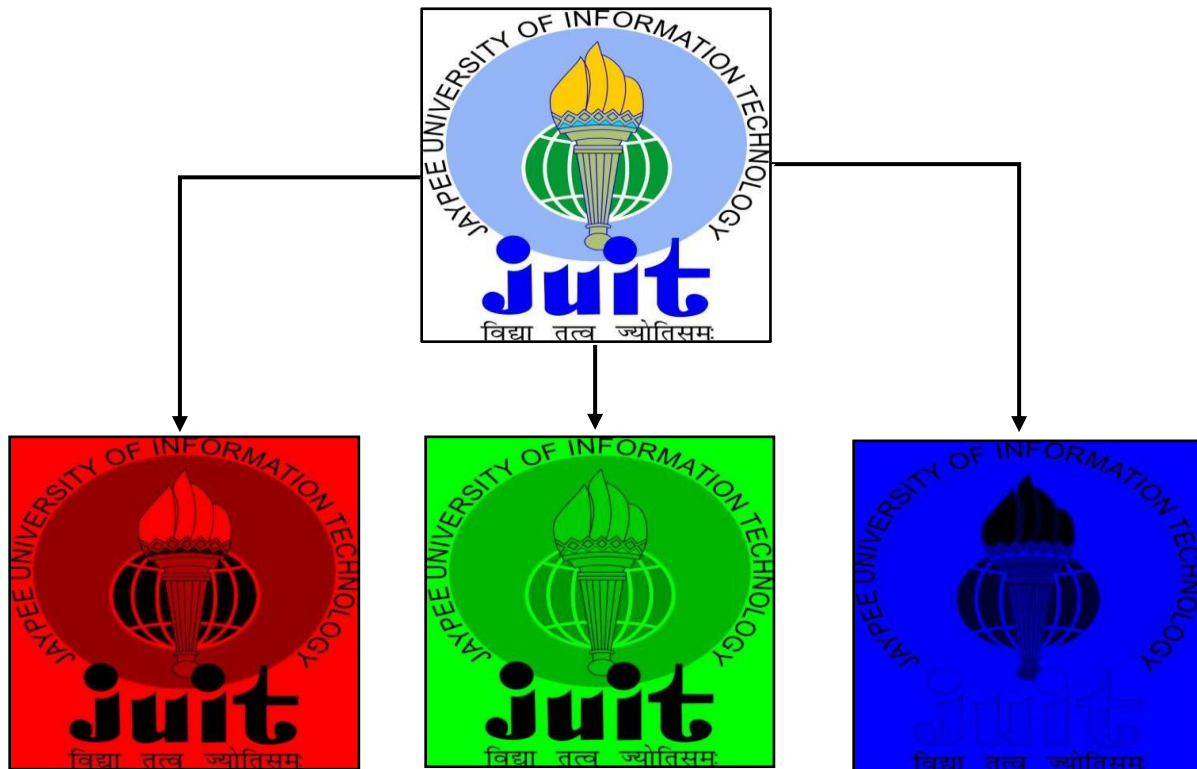


Figure 5.3: Red, Green and Blue components of JUIT logo

5.2.2 YCbCr

Generally, a human visualizes the brightness not the colors of a scene. So according to HVS, a human is less sensitive to color than its brightness. In the last section, we already discussed about the RGB color space. In the RGB color space every color is having the equally importance for projecting a scene. But in case of YCbCr we can represent an image or a frame in a far better way by unscrambling the luminance components from the color. YCbCr is also known as the YUV color format. In the YCbCr color space model Y is representing the brightness of the image whereas Cb and Cr are representing the color information of the image. Y can be considered as a weighted average of RGB.

$$Y = k_r R + k_g G + k_b B \quad (5.1)$$

where k is a weighting factor.

In the YCbCr color format the color information (Cb , Cr and Cg) can be represented as the difference among R , G or B and the luminance Y :

$$Cb = B - Y \quad (5.2)$$

$$Cr = R - Y \quad (5.3)$$

$$Cg = G - Y \quad (5.4)$$

Y (the luminance section) represents the overall details of color image and the differences between the three color namely Cb , Cr and Cg indicates the dissimilarity between every image's color strength and the imply brightness. Figure 5.3 represents the chrominance components (red, green and blue) analogous to the RGB components of Figure 5.4.

The difference is zero when it is mid grey, positive for light grey and negative for dark grey. The color component and the luminance image must have the huge difference then only chrominance components have the major value (Figure 5.3)

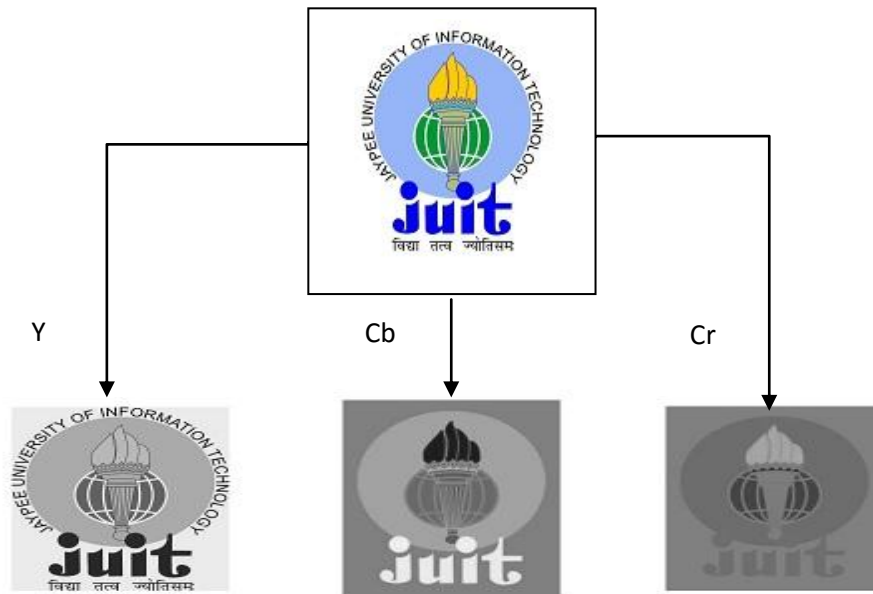


Figure 5.4: YCbCr color components of JUIT logo.

As per the YCbCr color system “ $Cb + Cr + Cg$ ” is a constant. That is why we need to store or transfer only two values out of three because the third value we can calculate from the other two. In the YCbCr color model only Luminance (Y) and blue chrominance (Cb) and red components (Cr) need to be stored for the representation of the YCbCr color space model. The YCbCr color model also has the advantage over the RGB color model. In the RGB color model every component is having the equal importance and weightage but in case of YCbCr, Cb and Cr can be represented by means of a subordinate resolution than Y because the HVS is less sensitive to color than intensity. So the YCbCr color space model is required the fewer amounts of data for the representation, even without affecting the visual quality. Generally, for an informal spectator, there is no difference in the YCbCr and RGB image. An RGB image can be transformed into the YCbCr format just because of it required less data for representation but before displaying the image again we have to convert it into the RGB model.

So finally we can say that there is not necessitate to indicate a split feature ‘kg’ because ($kb + kr + kg = 1$) and that ‘g’ can be extracted from the YCbCr color space representation by subtracting the Cb and Cr from Y .

$$\left\{ \begin{array}{l} Y = k_r R + (1 - k_b - k_r)G + k_b B \\ C_b = \frac{0.5}{1 - k_b} (B - Y) \\ C_r = \frac{0.5}{1 - k_r} (R - Y) \end{array} \right\} \quad (5.5)$$

$$\left\{ \begin{array}{l} R = Y + \frac{1 - k_r}{0.5} C_r \\ G = Y - \frac{2k_b(1 - k_b)}{1 - k_b - k_r} C_b - \frac{2k_r(1 - k_r)}{1 - k_b - k_r} C_r \\ G = Y + \frac{(1 - k_b)}{0.5} C_b \end{array} \right\} \quad (5.6)$$

ITU-R recommendation BT.601 [1] defines $kb = 0.114$ and $kr = 0.299$. Substituting into the above equations (5.5) & (5.6) gives the following widely-used conversion equations (5.7 & 5.8).

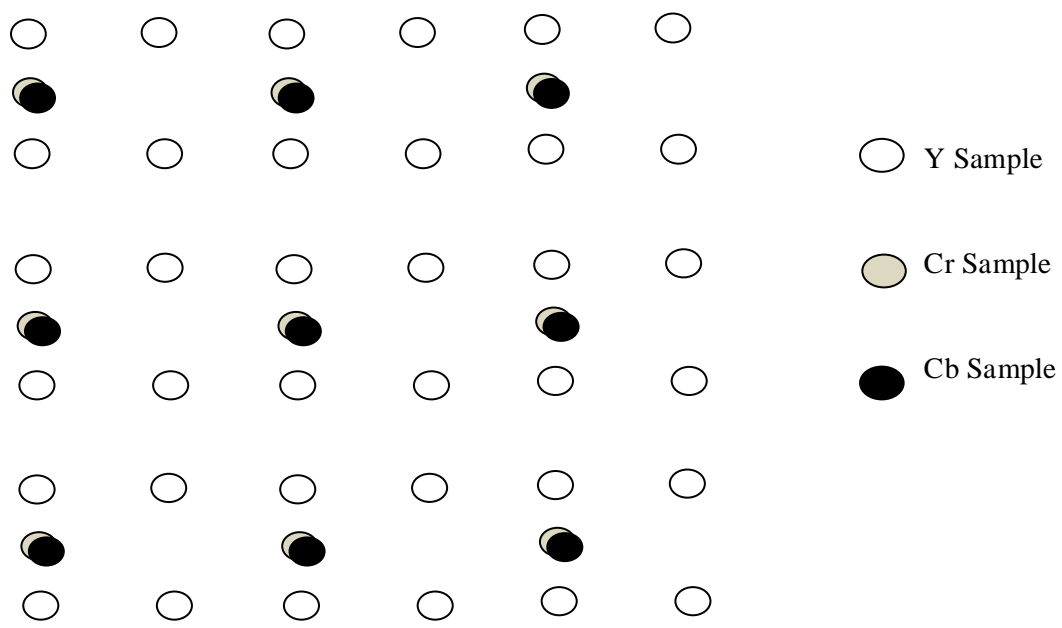
$$\left\{ \begin{array}{l} Y = 0.299R + 0.587G + 0.114B \\ C_b = 0.564 (B - Y) \\ C_r = 0.713 (R - Y) \end{array} \right\} \quad (5.7)$$

$$\left. \begin{aligned} R &= Y + 1.402C_r \\ G &= Y - 0.344C_b - 0.714C_r \\ B &= Y + 1.772C_b \end{aligned} \right\} \quad (5.8)$$

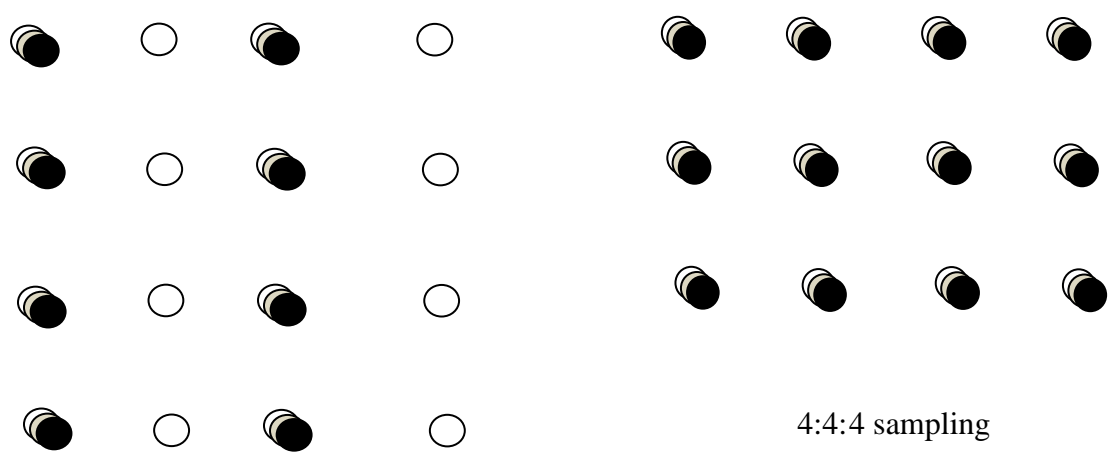
5.2.3 YCbCr COLOR FORMATS

Figure 5.5 shows the three different sampling models for Y, Cb and Cr which are 4:4:4, 4:2:2 and 4:2:0. Every sampling model is used for a different kind of video sequence. Here in the Figure 5.5 we have shown the ‘Y’ components ‘Cb’ components and ‘Cr’ components via white circle, gray circle and black circle respectively. Here in the ‘c’ part of the figure we have shown 4:4:4 sampling that means, every component of (YCbCr) is having the same resolution. In the part ‘b’ of the Figure 5.5, we have also explain the 4:2:2 sampling, it means for every 4 components we are having the 4 ‘Y’ samples, 2 ‘Cb’ and 2 samples of ‘Cr’. In the same way we have shown 4:2:0 sampling in part ‘a’ of the Figure 5.5, that means it contains for every 4 components 4 samples of Y and 2 samples of (Cb & Cr). Here the meaning of ‘0’ is not just like a numerical value it means in this part we are having the 2 samples of color. Here it is also concluded that 4:4:4 sampling is used for the high definition video and 4:2:2, 4:2:0 is used for the MPEG-4 video and low quality video respectively.

Here in the figure ‘c’ we can see 4:4:4 sampling that also means ‘24 bits per pixel’. How it becomes 24 bits per pixels because the 4:4:4 sampling contains total 12 samples and it also required $12 \times 8 = 96$ bits for representing the sample so on an average $96/4=24$ bits per pixel we required. Same in the case of 4:2:0 it contains the bits per pixels, just half of the 4:4:0 samples. For the mathematical calculation we can see it required $4 + 2 = 6$ samples for representing and total number bits require $6 \times 8 = 48$ bits. So in this case we required $48/4=12$ bits per pixel for representing the 4:2:0 sampling that is also the just half of the 4:4:4 sampling.



(a) 4:2:0 sampling



2:2:2 sampling

Figure 5.5: 4:2:0, 4:2:2 and 4:4:4 sampling patterns (progressive)

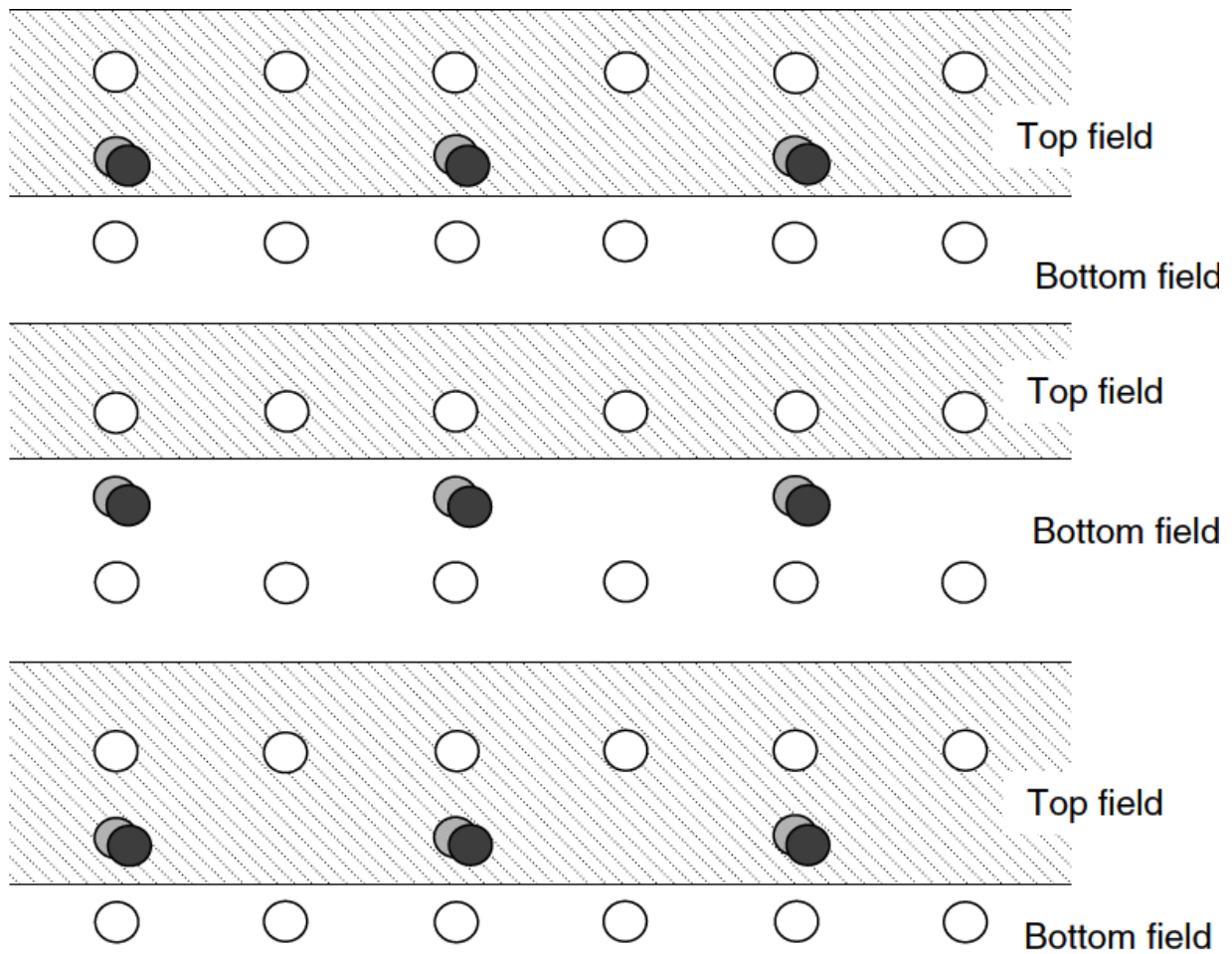


Figure 5.6: Allocation of 4:2:0 samples to top and bottom fields

5.3 BACKGROUND

Despite being protection the copyright of the journals, electronic publications, magazines and static images, there is still enormous scope for protecting the digital videos on a professional front which is based on the real network.

5.3.1 VIDEO WATERMARKING

In this modern era, people are enormously using interne, sharing images, videos and audios. But they are unaware of the fact that whatever they are sharing online is not at all completely protected, so it require certain kind of security to the shared and transferred data. For securing the shared data, many techniques have been proposed [13], [22], [55]. We have discussed about copyright protecting technique in this paper. In this technique, we are using the digital

watermark which is embedded in the digital video frame to increase the robustness (no degradation of the watermark despite being attack numerously), imperceptibility [53] (no visibility to the hidden embedded data), Capacity (the number of bits that can be hidden), Security (controlling illegal use of data) and computational complexity of the embedding and detection process [43-45].

5.3.2 TYPES OF VIDEO WATERMARKING

There are three types of hiding techniques discuss here namely: Blind [56], [58] Semi-blind [57], and non-blind [59] for detecting the watermark. In this chapter, non-blind and semi-blind watermarking systems are used.

In the blind watermarking, we don't require the host data to extract or detect the watermark. But for the security reasons, we have some additional information like a secret key for detecting the watermark. Suppose, we don't require the additional information then security key is not mandatory. This association of the watermarking system has revealed in Table 1. (Discussed in Chapter 1)

In this thesis, we have proposed an algorithm for digital video copyright protection based on discrete wavelet transform. With the help of SCD algorithm [30], we extracted I-frames, and then we pre-process the watermark and target video as well. In this chapter, work is being done towards combining the embedding and pulling out of the watermark with foundation video tracking. In this process watermark is embedded in the video for its protection against the unauthorized user and to claim its authenticity by extracted the embedded watermark from the original source video in order to satisfy the demand of the authentic owner and also comparison between the original and extracted watermark is carried out to prove whether the product is authorized or not.

So far we have analyze in the literature review that the attacks perform on the watermark can crack, damage or detect watermark by using certain algorithms [46-54]. But we have used CWEA to make it difficult for an attacker to detect the modern pattern of the embedded watermark. And that's how it enhanced certain characteristics (robustness and security) of the embedded watermark. TABLE 2.1 has shown the classification of watermark system.

5.4 PROPOSED ALGORITHM

Here we used the YCbCr color space model to make this algorithm better in respect of imperceptibility and robustness. For the embedding process we have taken a colored image with the dimension of 256 x 256 as a watermark image. Firstly we convert the watermark image and target frame into YCbCr color space model. So, for the watermark embedding process we have taken the Y part of the watermark image and CbCr part of the video frame. Now applying the 2 level DWT on it and by using the OR logic operation we added all the coefficients of watermark image and video frame. As per our proposed method, we are considering only the LUMA part of the watermark image that improve the imperceptibility of original video and also considering the CbCr part of the targeted video that increasing the robustness of the watermark

Watermark embedding

1. Applying the SCD algorithm [60] on the original video sequence (O_{video}) and then divide each scene into a non-overlapping group of pictures. Each group of pictures has an Identical frame (I). Select all I frames from input video for embedding the watermark.

$$WmI_i = k \times (Lf_2) + q \times (Wm_2)$$

Where “ Wm_i ” is watermarked identical frame. Lf_2 is representing the low-frequency approximation of original video frame. Wm_2 is representing the low-frequency approximation of watermark image where k & q are the scaling factors.

2. On the every I-frame apply “YCbCr” color format.

Where “ $Y = 0.299R + 0.587G + 0.114B$ ”

$$\text{“Cb} = 0.564 (B - Y)\text{”}$$

$$\text{“Cr} = 0.713 (R - Y)\text{”}$$

$$\text{“Cb} + \text{Cr} + \text{Cg} = 1\text{”}$$

$$\text{“Cg} = 1 - (\text{Cb} + \text{Cr})\text{”}$$

3. Apply the 2nd level discrete wavelet transform on chrominance (Cb & Cr) of each frame and accumulate the LUMINANCE (Y-luminance) for future reference.

$$\text{DWT (Cb)} = [\text{Cai}, \text{Chi}, \text{Cvi}, \text{Cdi}]_o$$

$$\text{DWT (Cr)} = [\text{Cai}, \text{Chi}, \text{Cvi}, \text{Cdi}]_o$$

Where $i=1, 2$.

4. The colored watermark image is 'W' with the dimension of 256 x 256. Apply the YCbCr Color model on W.
5. Apply the 2nd level discrete wavelet transform on Y components and get detail coefficients of LUMINANCE.

$$\text{“DWT (Y)} = [\text{Cai}, \text{Chi}, \text{Cvi}, \text{Cdi}]_w\text{”}$$

Where $i= 1, 2$.

6. For the next process of watermark embedding, add the detailed coefficients of LUMINANCE (Y) watermark with the detail coefficients of CHROMINANCE I-frame of the original video.

Now, for Cb

$$[\text{Mod Chi}]_{\text{Cb}} = [\text{Chi}]_o + [\text{Chi}]_w$$

$$[\text{Mod Cvi}]_{\text{Cb}} = [\text{Cvi}]_o + [\text{Cvi}]_w$$

Now, for Cr

$$[\text{Mod Chi}]_{\text{Cr}} = [\text{Chi}]_o + [\text{Chi}]_w$$

$$[\text{Mod Cvi}]_{\text{Cr}} = [\text{Cvi}]_o + [\text{Cvi}]_w$$

Where $i= 1, 2$.

7. Now, modified Chi and modified Cv_i are the coefficients of (Cb & Cr) of watermark inserted identical frame.

8. Take the Inverse DWT of watermark inserted (Cb & Cr) components of identical frames. At the end we get the modified (mod Cb and mod Cr) of I-frame.
9. Now add the LUMINANCE (Y) from step-2 with the modified CHROMINANCE (mod Cb and mod Cr) and get the final watermark inserted I-frame.
10. Finally combine all the watermark inserted I-frame in a resourceful manner with the remaining frames and get the watermarked video.

Watermark detecting

1. Apply the SCD algorithm [60] on the watermarked video sequence (W_{video}) and then divide each scene into the non-overlapping group of pictures. Each group of pictures has an Identical frame (I). Select all I frames from input watermarked video for detecting the watermark.
2. Take the watermarked video frame (W_f) and original identical frames (I_i) then apply the YCbCr color space model on the both.
3. Apply the DWT on (Cb & Cr) of both watermarked frame and identical frames.
4. Calculate the difference of detail coefficients of (Cb & Cr) of watermarked frame and the detail coefficients of original I-frame which are mod Ch_i , mod Cv_i , Ch_i and Cv_i respectively.

Now, for Luminance

$$[\text{NewCh}_i]_{\text{dw}} = "[\text{mod Ch}_i]_{\text{ew}} - [\text{Ch}_i]_{\text{o}}"$$

$$[\text{NewCv}_i]_{\text{dw}} = "[\text{mod Cv}_i]_{\text{ew}} - [\text{Cv}_i]_{\text{o}}"$$

Where $i= 1, 2$.

5. Take the inverse discrete wavelet of the detail coefficients of detected (Y) and add with the original (Cb & Cr) and get the YCbCr format of the detected watermark.
6. At the end compute the cross relationship of both (Extracted watermark and original watermark).

7. If relationship == high

Then, discontinue the implementation and print a message that watermark has been detected.

Else if

Consider the 2nd level detailed coefficients and go over from step 3.

Else

Watermark is not detected.

5.5 EXPERIMENTAL RESULTS

For the outcome investigation we have taken two videos named as 'wakna road' and 'foramen' with the aspect of 320 x 240 and 352 x 288 respectively. We have also taken an image (JUIT logo) as a watermark with the dimension of 256 x 256 and the size of original watermark image is (256 x 256). In the Figure 5.7 we have shown the complete procedure of video watermarking where we have taken a video and applying the SCD algorithm to find out the identical frames. For every I-frame applied the YCbCr color format. Here we are considering only the Cb component of the frame for watermark embedding and keeping the rest of the components (YCr) for future reference. After the above process, we have taken color watermark and applied YCbCr and only taken Y component and perform 2nd level DWT on the same. Finally the low frequency component of both video and color watermark is merge together and perform the operation of IDWT. Finally include (Y) and (Cr) components of the video to make it watermarked video.

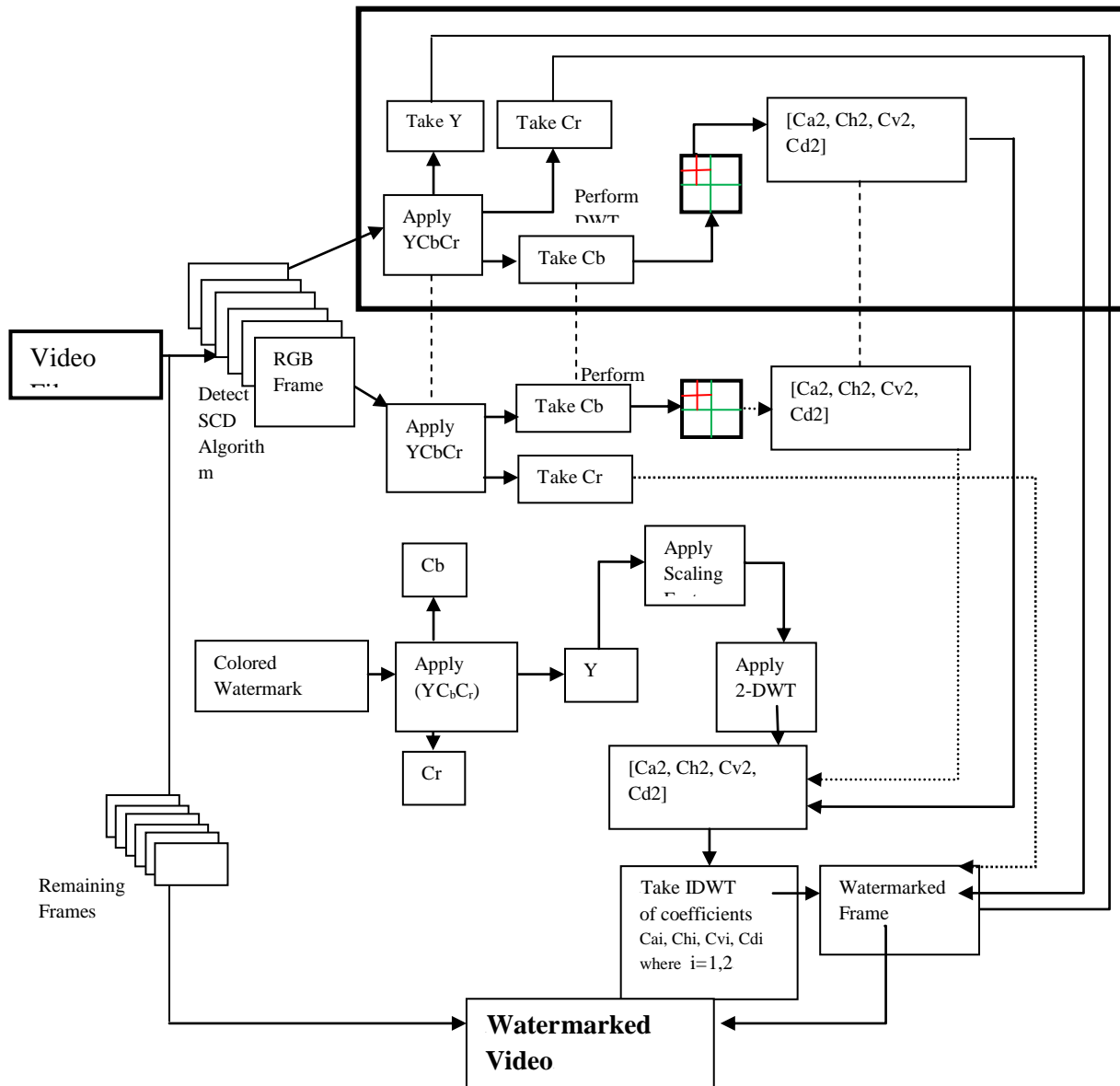


Figure 5.7: Complete process of watermark embedding in color domain

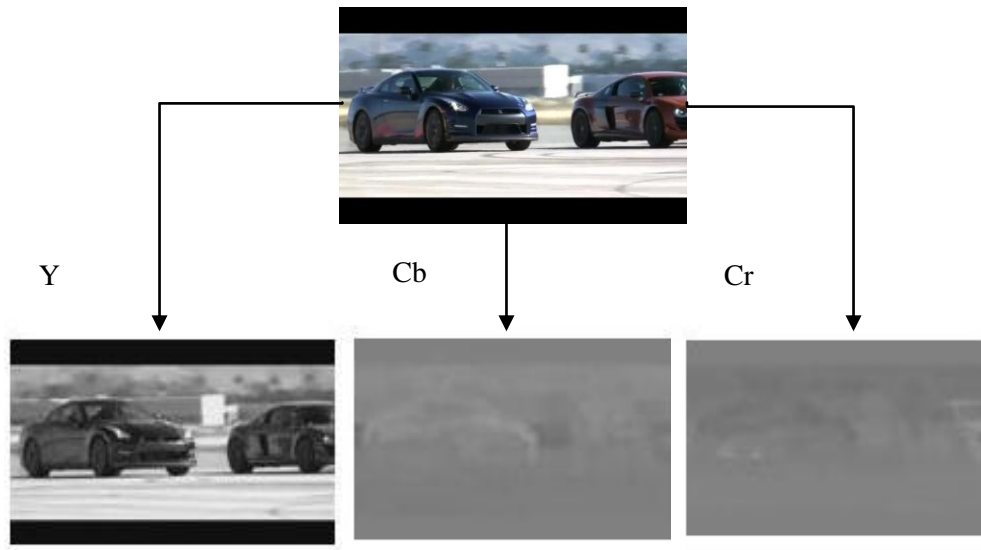


Figure 5.8: YCbCr color components of Car Race video.

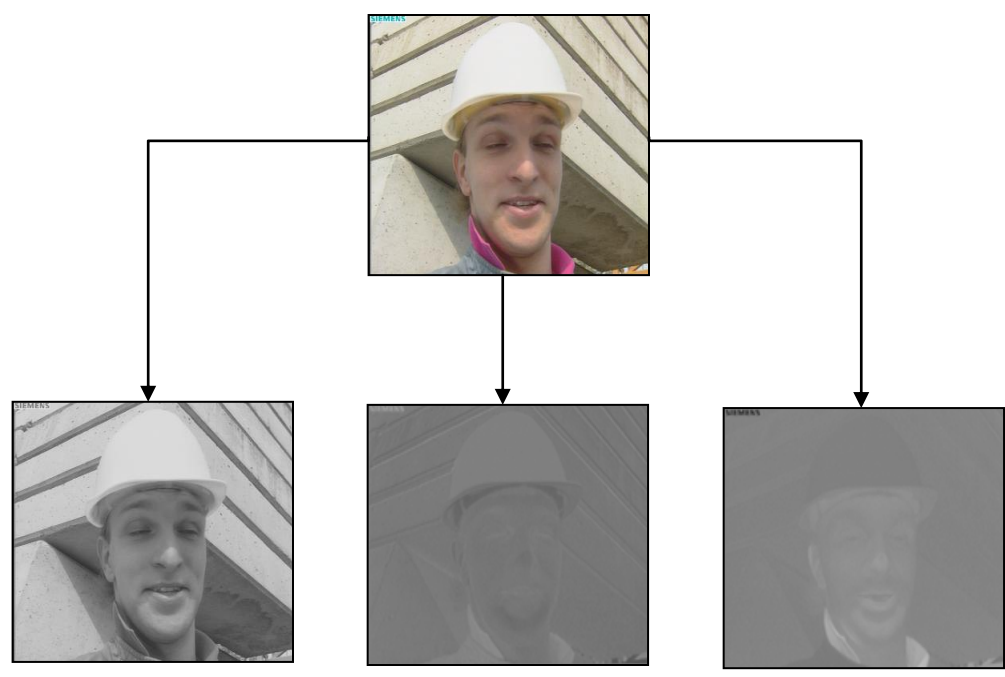


Figure 5.9: YCbCr color components of Foremen Video.

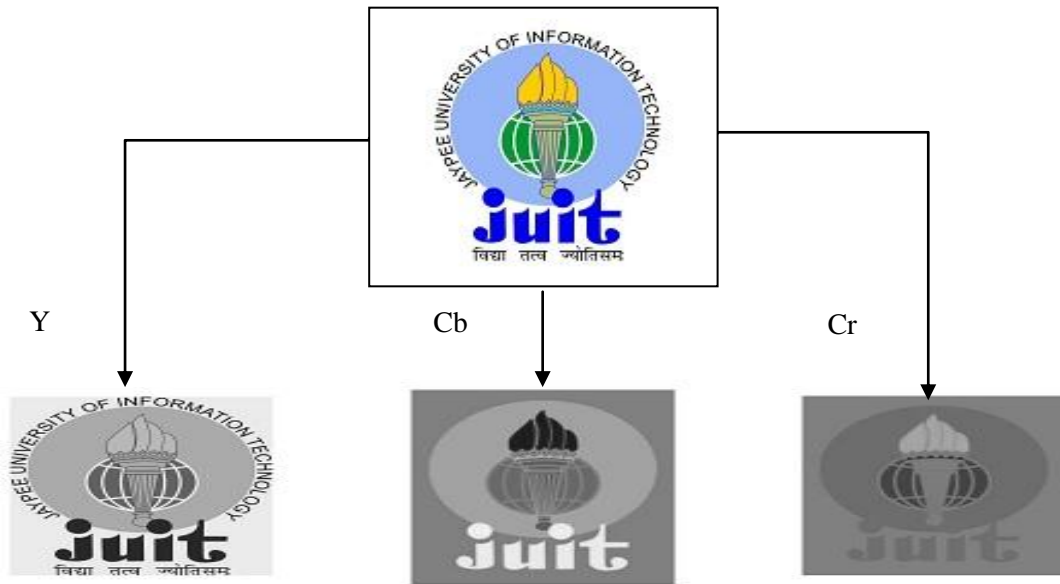


Figure 5.10: YCbCr color components of original watermark (JUIT logo).

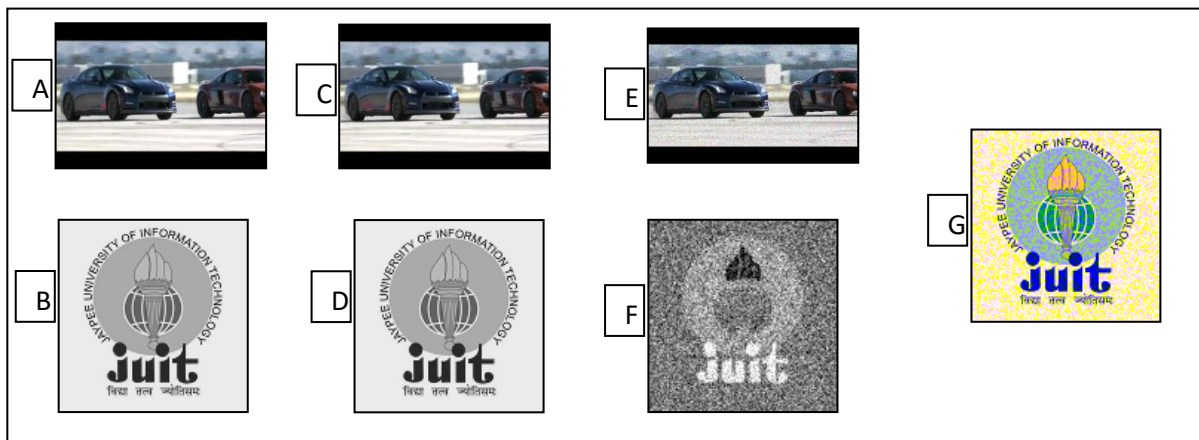


Figure 5.11: Watermark extraction process

- (A) Captured a frame from Car race video (B) 'Y' part of original watermark. (C) Watermarked Car race frame (D) "Extracted Watermark" (E) Bisterous watermarked car race frame (F) Extracted watermark from the noisy frame (G) Combined with the (Cb & Cr) of the new watermark with extracted watermark

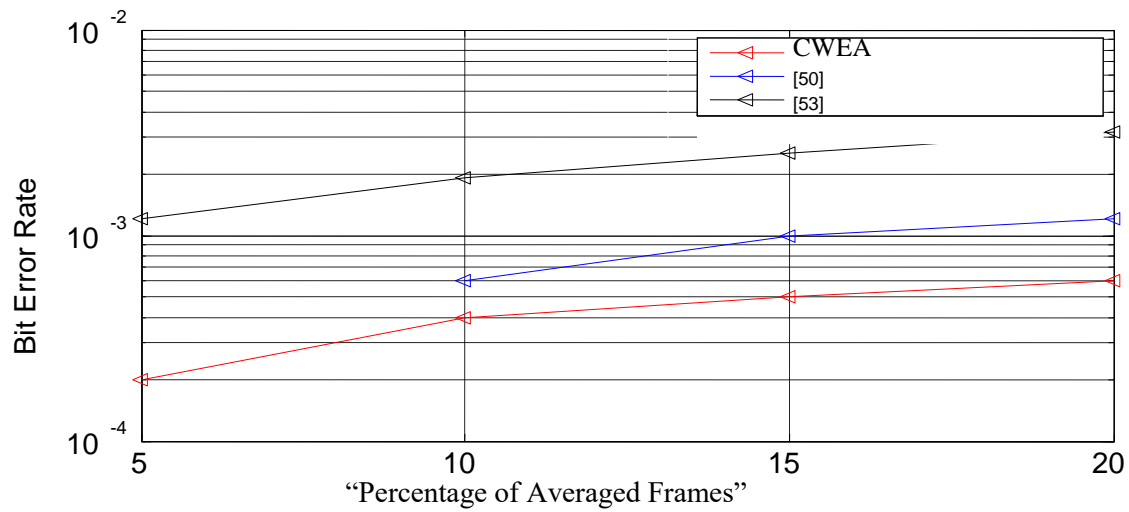


Figure 5.12: Bit Error Rate (log scale) under frame averaging attack

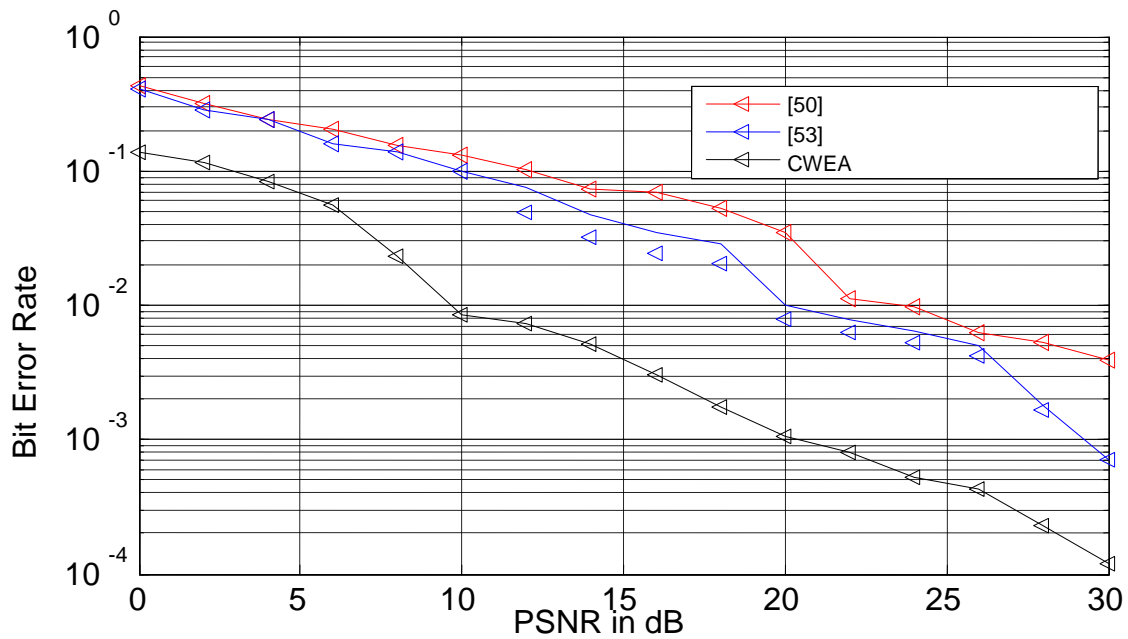


Figure 5.13 : Bit Error Rate (log scale) under spatial attack (Uniform noise)

5.6 CONCLUSION

As per the algorithm we designed it is very obvious that the watermark we have to embed into I-frames. As per our study and literature survey I frames are the independent frames and they have only their own information. So the process of embedding the watermark into I-frame is much better than the other parts of the frame. But as we know that the I-frame is containing the real information and we have to be very careful when we are embedding the watermark information in the I-frame.

To embed the color watermark is more challenging in compare of a gray scale. A color image is having three values for a single pixel while in gray scale image a pixel value is having only one. But the quality of the extracted watermark in color domain is much better than the gray scale. So finally we conclude that at the time of color watermark insertion we have to maintain the quality of original media because of the higher size of watermark the quality of embedded media may degrade.

In the Figure 5.11, we have shown the different images for the result analysis and we found that as per the HVS our results are much better than the references we have taken. After the extraction of the watermark (Y components), we combined it with the Cb & Cr components of the original watermark to make it the original. In the end we have applied the YCbCr to RGB to make it the colored watermark. Here, we obtain a high-quality watermark with the PSNR of 46.22. So here we get the better results in compare of [50], [53] and [54].

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1. CONCLUSION

In this thesis, we have designed a robust and secure technique to protect the ownership of a digital video. At the time of designing the algorithms, we have focused on the robustness and imperceptibility. To get the best experimental results, the process of watermark embedding has been done in the transform domain where we used 1st level and 2nd level discrete wavelet transform (DWT).

In chapter 3, we split a watermark in a fixed square or a rectangular block that depends on the watermark dimensions and a number of blocks will depend on the scene changed detection in the video. By applying this technique, we have got the following benefits

1. No matter how big the size of the watermark, it can be easily inserted in the video without altering the imperceptibility of the same.
2. If an intruder detects the watermark, he can only detect the block but can't detect the whole pattern.
3. Compression attack cannot affect the quality of watermark because the watermark is inserted inside the identical frames.

In chapter 4, we have proposed ZPA (zero padding algorithm) along with SWEA (Split watermark embedding algorithm) which gives us the better result in the following ways:

1. There is no need of re-sampling of the watermark because it is embedded in the frame as it is and the rest of the block of the matrix (frame) is occupied by 0.
2. The extracted watermark is of high quality.

3. Compression, re-sizing, cropping attacks cannot affect the quality of inserted watermark because we are inserting the watermark in identical frame where we do not require the re-sampling of the watermark.

In chapter 5, we have proposed a colored watermark embedding algorithm (CWEA) that provides us with even better results along with some advantages which are as follows:

1. Removal of the watermark is very difficult for the unauthorized user.
2. No one can introduce his own watermark in the frame in which we have already embedded our watermark.
3. Quality of extracted watermark is much better because blue Chroma and red Chroma we used to improve the quality of extracted watermark.

6.2. FUTURE SCOPE

The algorithms used until now are unable to fulfill all the parameters which include: Robustness, security, imperceptibility, and scalability. Real-time watermark embedding algorithms need to improve their execution time complexity. We should also focus on audio watermarking because it may resolve many problems that we are facing regarding the video watermarking.

We worked on the offline videos but these algorithms should also be applied to online videos because online streaming is much needed the copyright protection. To protect the online video we can design some kind of tools those have the application of machine learning also. The concept of machine learning is not introduced in this field till now.

References

- [1] Zeng, Peng, Zhenfu Cao, and Kim-Kwang Raymond Choo. "An ID-based digital watermarking protocol for copyright protection." *Computers & Electrical Engineering* 37, no. 4 (2011): 526-531.
- [2] Ghosh, Poulami, Rilok Ghosh, Souptik Sinha, Ujan Mukhopadhyay, Dipak Kr Kole, and Aruna Chakroborty. "A novel digital watermarking technique for video copyright protection." *Computer Science and Information Technology*(2012): 601-609.
- [3] Masoumi, Majid, and Shervin Amiri. "A blind scene-based watermarking for video copyright protection." *AEU-International Journal of Electronics and Communications* 67, no. 6 (2013): 528-535.
- [4] Ali, Jabir, and S. P. Ghrera. "A secure method of copyright protection for digital videos using split watermark embedding algorithm." In *2017 Fourth International Conference on Image Information Processing (ICIIP)*, pp. 1-5. IEEE, 2017.
- [5] Jabir Ali, Satya Prakash Ghrera "A novel method for copyright protection of digital videos using SWEA and ZPA technique", in *International Journal of Engineering & Technology (UAE)*, ISSN 2227-524X, Volume 7 (2.9) (2018) pp. 90-96.
- [6] Ali, Jabir, and Satya Prakash Ghrera. "CWEA: A Digital Video Copyright Protection Scheme.", In *International Journal of Computer Information Systems and Industrial Management Applications*. ISSN 2150-7988 Volume 10 (2018) pp. 009-017.
- [7] Lin, Shinfeng D., and Chin-Feng Chen. "A robust DCT-based watermarking for copyright protection." *IEEE Transactions on Consumer Electronics* 46, no. 3 (2000): 415-421.
- [8] Doerr, Gwenaël, and Jean-Luc Dugelay. "A guide tour of video watermarking." *Signal processing: Image communication* 18, no. 4 (2003): 263-282.
- [9] Doërr, Gwenaël, and J-L. Dugelay. "Security pitfalls of frame-by-frame approaches to video watermarking." *IEEE Transactions on Signal Processing* 52.10 (2004): 2955-2964.

- [10] Holliman, Matthew J., William W. Macy, and Minerva M. Yeung. "Robust frame-dependent video watermarking." In *Security and Watermarking of Multimedia Contents II*, vol. 3971, pp. 186-198. International Society for Optics and Photonics, 2000.
- [11] Wong, Ping Wah, and Nasir Memon. "Secret and public key image watermarking schemes for image authentication and ownership verification." *IEEE transactions on image processing* 10.10 (2001): 1593-1601.
- [12] Paillier, Pascal. "Public-key cryptosystems based on composite degree residuosity classes." In *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 223-238. Springer, Berlin, Heidelberg, 1999.
- [13] J Zhou, W Sun, L Dong, X Liu, OC Au, YY Tang "Secure reversible image data hiding over encrypted domain via key modulation." *IEEE transactions on circuits and systems for video technology* 26.3 (2016): 441-452.
- [14] Doërr, Gwenaël. "Security issue and collusion attacks in video watermarking." PhD diss., Nice, 2005.
- [15] Koz, Alper, and A. Aydin Alatan. "Oblivious spatio-temporal watermarking of digital video by exploiting the human visual system." *IEEE Transactions on circuits and systems for video technology* 18.3 (2008): 326-337.
- [16] Asikuzzaman, Md, Md Jahangir Alam, Andrew J. Lambert, and Mark R. Pickering. "A blind high definition videowatermarking scheme robust to geometric and temporal synchronization attacks." In *2013 Visual Communications and Image Processing (VCIP)*, pp. 1-6. IEEE, 2013.
- [17] Cedillo-Hernandez, Antonio, Manuel Cedillo-Hernandez, Mireya Garcia-Vazquez, Mariko Nakano-Miyatake, Hector Perez-Meana, and Alejandro Ramirez-Acosta. "Transcoding resilient video watermarking scheme based on spatio-temporal HVS and DCT." *Signal Processing* 97 (2014): 40-54.

- [18] Kimpan, Somchok, Attasit Lasakul, and Sakreya Chitwong. "Variable block size based adaptive watermarking in spatial domain." In *IEEE International Symposium on Communications and Information Technology, 2004. ISCIT 2004.*, vol. 1, pp. 374-377. IEEE, 2004.
- [19] Bhatnagar, Gaurav, and Balasubramanian Raman. "A new robust reference watermarking scheme based on DWT-SVD." *Computer Standards & Interfaces* 31, no. 5 (2009): 1002-1013.
- [20] Lai, Chih-Chin, and Cheng-Chih Tsai. "Digital image watermarking using discrete wavelet transform and singular value decomposition." *IEEE Transactions on instrumentation and measurement* 59, no. 11 (2010): 3060-3063.
- [21] Faragallah, Osama S. "Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain." *AEU-International Journal of Electronics and Communications* 67.3 (2013): 189-196.
- [22] Makbol, Nasrin M., and Bee Ee Khoo. "A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition." *Digital Signal Processing* 33 (2014): 134-147.
- [23] Thompson, A. Ian, Ahmed Bouridane, and Fatih Kurugollu. "Spread transform watermarking for digital multimedia using the complex wavelet domain." In *2007 ECSIS Symposium on Bio-inspired, Learning, and Intelligent Systems for Security (BLISS 2007)*, pp. 123-132. IEEE, 2007.
- [24] Hwang, Dong Choon, Kyung Hoon Bae, and Eun-Soo Kim. "Stereo image watermarking scheme based on discrete wavelet transform and adaptive disparity estimation." *Mathematics of Data/Image Coding, Compression, and Encryption VI, With Applications*. Vol. 5208. International Society for Optics and Photonics, 2004.
- [25] Huang, Hui-Yu, Cheng-Han Yang, and Wen-Hsing Hsu. "A video watermarking technique based on pseudo-3-D DCT and quantization index modulation." *IEEE transactions on information forensics and security* 5.4 (2010): 625-637.

- [26] Barni, Mauro, Franco Bartolini, Vito Cappellini, and Alessandro Piva. "A DCT-domain system for robust image watermarking." *Signal processing* 66, no. 3 (1998): 357-372.
- [27] Wu, Chuan-Fu, and Wen-Shyong Hsieh. "Digital watermarking using zerotree of DCT." *IEEE Transactions on Consumer Electronics* 46.1 (2000): 87-94.
- [28] Jabir Ali, Satya Prakash Ghrera. "A Secure Method of Copyright Protection for Digital videos using Split Watermark Embedding Algorithm" *Fourth International Conference on Image Information Processing (ICIIP) (2017): 569-573.*
- [29] Boulgouris, N. V., F. D. Koravos, and M. G. Strintzis. "Self-synchronizing watermark detection for MPEG-4 objects." *Electronics, Circuits and Systems, 2001. ICECS 2001. The 8th IEEE International Conference on*. Vol. 3. IEEE, 2001.
- [30] Shahraray, Behzad. "Scene change detection and content-based sampling of video sequences." In *Digital Video Compression: Algorithms and Technologies 1995*, vol. 2419, pp. 2-14. International Society for Optics and Photonics, 1995.
- [31] Xu, Dawen, Rangding Wang, and Jicheng Wang. "A novel watermarking scheme for H. 264/AVC video authentication." *Signal Processing: Image Communication* 26.6 (2011): 267-279.
- [32] Guo, Yao, and Feng Pan. "Information hiding for H. 264 in video stream switching application." *Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on*. IEEE, 2010.
- [33] Jiang, Xinghao, Tanfeng Sun, Yue Zhou, Wan Wang, and Yun-Qing Shi. "A robust H. 264/AVC video watermarking scheme with drift compensation." *The Scientific World Journal* 2014 (2014).
- [34] Xu, Dawen, Rangding Wang, and Yun Q. Shi. "Data hiding in encrypted H. 264/AVC video streams by codeword substitution." *IEEE transactions on information forensics and security* 9.4 (2014): 596-606

- [35] Ma, Xiaojing, Zhitang Li, Hao Tu, and Bochao Zhang. "A data hiding algorithm for H. 264/AVC video streams without intra-frame distortion drift." *IEEE transactions on circuits and systems for video technology* 20, no. 10 (2010): 1320-1330.
- [36] Pröfrock, Dima, Henryk Richter, Mathias Schlauweg, and Erika Müller. "H. 264/AVC video authentication using skipped macroblocks for an erasable watermark." In *Visual Communications and Image Processing 2005*, vol. 5960, p. 59604C. International Society for Optics and Photonics, 2005.
- [37] Tew, Yiqi, and KokSheik Wong. "Information hiding in HEVC standard using adaptive coding block size decision." *Image Processing (ICIP), 2014 IEEE International Conference on*. IEEE, 2014.
- [38] Kong, Wenhai, Bian Yang, Di Wu, and Xiamu Niu. "SVD based blind video watermarking algorithm." In *First International Conference on Innovative Computing, Information and Control-Volume I (ICICIC'06)*, vol. 1, pp. 265-268. IEEE, 2006.
- [39] Solachidis, Vassilios, and Ioannis Pitas. "Circularly symmetric watermark embedding in 2-D DFT domain." *IEEE transactions on image processing* 10.11 (2001): 1741-1753.
- [40] Kang, Xiangui, Jiwu Huang, Yun Q. Shi, and Yan Lin. "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression." *IEEE transactions on circuits and systems for video technology* 13, no. 8 (2003): 776-786.
- [41] Asikuzzaman, Md, Md Jahangir Alam, Andrew J. Lambert, and Mark R. Pickering. "A blind watermarking scheme for depth-image-based rendered 3D video using the dual-tree complex wavelet transform." In *2014 IEEE International Conference on Image Processing (ICIP)*, pp. 5497-5501. IEEE, 2014.
- [42] Zhang, Zengnian, Zhongjie Zhu, and Lifeng Xi. "Novel scheme for watermarking stereo video." *International Journal of Nonlinear Science* 3.1 (2007): 74-80.
- [43] Khalilian, Hanieh, and Ivan V. Bajic. "Video watermarking with empirical PCA-based decoding." *IEEE transactions on image processing* 22.12 (2013): 4825-4840.

- [44] I.B Shahraray "Scene Change Detection and Content-Based Sampling of Video Sequences," in SPIE 2419 (Digital Video Compression: Algorithms and Technologies):2-13, 1995.
- [45] Hartung, Frank H., Jonathan K. Su, and Bernd Girod. "Spread spectrum watermarking: Malicious attacks and counterattacks." *Security and Watermarking of Multimedia Contents*. Vol. 3657. International Society for Optics and Photonics, 1999.
- [46] Karmakar, Amlan, Amit Phadikar, and Arindam Mukherjee. "Video Watermarking Scheme Resistant to Rotation and Collusion Attacks." *Emerging Trends in Computing and Communication*. Springer, New Delhi, 2014. 95-101.
- [47] Nasir, Ibrahim Alsonosi, and A. B. Abdurrman. "A robust color image watermarking scheme based on image normalization." *Lecture Notes in Engineering & Computer Science* 2206.1 (2013): 2238-2243.
- [48] Mirza, Hanane, Hien Thai, and Zensho Nakao. "Digital video watermarking based on RGB color channels and principal component analysis." *International Conference on Knowledge-Based and Intelligent Information and Engineering Systems*. Springer, Berlin, Heidelberg, 2008.
- [49] Miyara, Kazuyoshi, Thai Duy Hien, Hanane Harrak, Yasunori Nagata, and Zensho Nakao. "Multichannel color image watermarking using PCA eigenimages." In *Intelligent Information Processing and Web Mining*, pp. 287-296. Springer, Berlin, Heidelberg, 2006.
- [50] Asikuzzaman, Md, Md Jahangir Alam, Andrew J. Lambert, and Mark Richard Pickering. "Imperceptible and robust blind video watermarking using chrominance embedding: a set of approaches in the DT CWT domain." *IEEE transactions on Information Forensics and Security* 9, no. 9 (2014): 1502-1517.
- [51] Dhaliwal, Kiratpreet Singh, and Rajneet Kaur. "Comparative study of single watermarking to multiple watermarking over a color image." *International Journal of Latest Trends in Engineering and Technology (IJLTET)* 2.2 (2013).

- [52] Dogan, Sengul, Turker Tuncer, Engin Avci, and Arif Gulten. "A robust color image watermarking with Singular Value Decomposition method." *Advances in Engineering Software* 42, no. 6 (2011): 336-346.
- [53] Tang, Xianghong, and Liping Chen. "A Color Video Watermarking Algorithm Based on DTCWT and Motion Estimation." *Communications and Mobile Computing, 2009. CMC'09. WRI International Conference on*. Vol. 3. IEEE, 2009.
- [54] Párraga, C. A., Gavin Brelstaff, Tom Troscianko, and I. R. Moorehead. "Color and luminance information in natural scenes." *JOSA A* 15, no. 3 (1998): 563-569.
- [55] . Asikuzzaman, Md, Md Jahangir Alam, and Mark R. Pickering. "A blind and robust video watermarking scheme in the DT CWT and SVD domain." *Picture Coding Symposium (PCS), 2015*. IEEE, 2015.
- [56] Cox, Ingemar J., Joe Kilian, F. Thomson Leighton, and Talal Shamooh. "Secure spread spectrum watermarking for multimedia." *IEEE transactions on image processing* 6, no. 12 (1997): 1673-1687.
- [57] Asikuzzaman, Md, Md Jahangir Alam, Andrew J. Lambert, and Mark R. Pickering. "A blind digital video watermarking scheme with enhanced robustness to geometric distortion." In *2012 International Conference on Digital Image Computing Techniques and Applications (DICTA)*, pp. 1-8. IEEE, 2012.
- [58] Thanh, Ta Minh, Pham Thanh Hiep, Ta Minh Tam, and Keisuke Tanaka. "Robust semi-blind video watermarking based on frame-patch matching." *AEU-International Journal of Electronics and Communications* 68, no. 10 (2014): 1007-1015.
- [59] Burini, César, Séverine Baudry, and Gwenaél Doërr. "Blind detection for disparity-coherent stereo video watermarking." *Media Watermarking, Security, and Forensics 2014*. Vol. 9028. International Society for Optics and Photonics, 2014.

- [60] Nguyen, Philippe, Raphael Balter, Nicolas Montfort, and Severine Baudry. "Registration methods for nonblind watermark detection in digital cinema applications." In *Security and Watermarking of Multimedia Contents V*, vol. 5020, pp. 553-563. International Society for Optics and Photonics, 2003.
- [61] Doerr, Gwenael, and Jean-Luc Dugelay. "A guide tour of video watermarking." *Signal processing: Image communication* 18.4 (2003): 263-282.
- [62] Zheng, Dong, Jiying Zhao, and Abdulmotaleb El Saddik. "RST-invariant digital image watermarking based on log-polar mapping and phase correlation." *IEEE transactions on circuits and systems for video technology* 13.8 (2003): 753-765.
- [63] Hwang, Dong Choon, Kyung Hoon Bae, and Eun-Soo Kim. "Stereo image watermarking scheme based on discrete wavelet transform and adaptive disparity estimation." *Mathematics of Data/Image Coding, Compression, and Encryption VI, With Applications*. Vol. 5208. International Society for Optics and Photonics, 2004.
- [64] Dawei, Zhao, Chen Guanrong, and Liu Wenbo. "A chaos-based robust wavelet-domain watermarking algorithm." *Chaos, Solitons & Fractals* 22.1 (2004): 47-54.
- [65] Wang, Yao, Jorn Ostermann, and Ya-Qin Zhang. "Digital video processing and communications." *New Jersey: Prentice Hall* (2001).
- [66] Hartung, Frank, and Bernd Girod. "Watermarking of uncompressed and compressed video." *Signal processing* 66.3 (1998): 283-301.
- [67] Cayre, Francois, Caroline Fontaine, and Teddy Furon. "Watermarking security part one: theory." *Security, Steganography, and Watermarking of Multimedia Contents VII*. Vol. 5681. International Society for Optics and Photonics, 2005.
- [68] Langelaar, Gerhard C., Iwan Setyawan, and Reginald L. Lagendijk. "Watermarking digital image and video data. A state-of-the-art overview." *IEEE Signal processing magazine* 17.5 (2000): 20-46.

- [69] Cox, Ingemar J., and Matt L. Miller. "Review of watermarking and the importance of perceptual modeling." *Human Vision and Electronic Imaging II*. Vol. 3016. International Society for Optics and Photonics, 1997.
- [70] Cox, Ingemar J., Matthew L. Miller, and Jeffrey A. Bloom. "Watermarking applications and their properties." *Information Technology: Coding and Computing, 2000. Proceedings. International Conference on*. IEEE, 2000.
- [71] De Vleeschouwer, Christophe, J-F. Delaigle, and Benoit Macq. "Invisibility and application functionalities in perceptual watermarking an overview." *Proceedings of the IEEE* 90.1 (2002): 64-77.
- [72] Lari, Mohammad Reza Akbarzadeh, Sedigheh Ghofrani, and Des McLernon. "Using Curvelet transform for watermarking based on amplitude modulation." *Signal, Image and Video Processing* 8.4 (2014): 687-697.
- [73] Lu, Chun-Shien, and Hong-Yuan Mark Liao. "Video object-based watermarking: a rotation and flipping resilient scheme." *Image Processing, 2001. Proceedings. 2001 International Conference on*. Vol. 2. IEEE, 2001.
- [74] Noorkami, Maneli, and Russell M. Mersereau. "A framework for robust watermarking of H. 264-encoded video with controllable detection performance." *IEEE Transactions on Information Forensics and Security* 2.1 (2007): 14-23.
- [75] Ramkumar, Mahalingam, and Ali N. Akansu. "On the design of data hiding methods robust to lossy compression." *IEEE Transactions on multimedia* 6.6 (2004): 947-951.
- [76] Hwang, Dong-Choon, Kyung-hoon Bae, Jung-Hwan Ko, and Eun-Soo Kim. "3D watermarking scheme in stereo vision system." In *Applications of Digital Image Processing XXVIII*, vol. 5909, p. 590928. International Society for Optics and Photonics, 2005.
- [77] Ohbuchi, Ryutarou, Hiroshi Masuda, and Masaki Aono. "Watermarking three-dimensional polygonal models through geometric and topological modifications." *IEEE Journal on selected areas in communications* 16.4 (1998): 551-560.

[78] Wu, Han-Zhou, Yun-Qing Shi, Hong-Xia Wang, and Lin-Na Zhou. "Separable reversible data hiding for encrypted palette images with color partitioning and flipping verification." *IEEE Transactions on Circuits and Systems for Video Technology* 27, no. 8 (2016): 1620-1631.

[79] Dutta, Tanima, and Hari Prabhat Gupta. "A robust watermarking framework for High Efficiency Video Coding (HEVC)-Encoded video with blind extraction process." *Journal of Visual Communication and Image Representation* 38 (2016): 29-44.

6.1. LIST OF PUBLICATIONS

Journal Papers Published/Accepted:-

1. **Jabir Ali**, Satya Prakash Ghrera, “CWEA: A Digital Video Copyright Protection Scheme”, in International Journal of Computer Information Systems and Industrial Management Applications. ISSN 2150-7988 Volume 10 (2018) pp. 009-017. [Indexed- **Scopus**, **and** **IET** **Inspec**] **Published**
http://www.mirlabs.org/ijcisim/regular_papers_2018/IJCISIM_2.pdf
2. **Jabir Ali**, Satya Prakash Ghrera “A novel method for copyright protection of digital videos using SWEA and ZPA technique”, in International Journal of Engineering & Technology (UAE), ISSN 2227-524X, Volume 7 No. (2.9) (2018) DOI: [10.14419/ijet.v7i2.9.10547](https://doi.org/10.14419/ijet.v7i2.9.10547) pp. 90-96. [Indexed -**Scopus**, **ProQuest(USA)**] **Published**
<https://www.sciencepubco.com/index.php/ijet/article/view/10547>
3. Jabir Ali et al., “A lightweight buyer-seller watermarking protocol based on time-stamping and composite signal representation””, in International Journal of Engineering & Technology (UAE), ISSN **2227-524X**, **Volume** 7 (4.6) (2018) pp. 39-41, [Indexed - **Scopus**, **ProQuest(USA)**] **Published.**
<https://www.sciencepubco.com/index.php/ijet/article/view/20230/9491>
4. **Jabir Ali et al.** “Performance Enhancement of Edge Detection Methods for Human Bone Fracture X-ray Image Using Graphical Processors”, in International Journal of Computer Sciences and Engineering, E-ISSN: 2347-2693, Volume-6, Issue-7, July 2018, pp 888-894. [Indexed in UGC Approved, Google scholar]. **Published.**

Conference Paper Published/ Accepted:-

5. **Jabir Ali** and Satya Prakash Ghrera “A secure method of copyright protection for digital videos using Split Watermark Embedding Algorithm”, in Fourth International Conference on Image Information Processing (**ICIIP-21-23 DEC 2017**), pp. 569-573,2017. *Jaypee University, Solan, Himachal Pradesh, India* [**IEEE**] **Published**
<https://ieeexplore.ieee.org/document/8313781/>

6. **Jabir Ali** and Satya Prakash Ghrera “A robust approach of copyright protection for digital videos using zero padding algorithm technique” in International Conference on Futuristic Trends in network and communication Technology (FTNCT-09 -10 Feb 2018) Jaypee University, Solan, Himachal Pradesh. **Springer** [Indexed in **Scopus, IET**] **Published**

7. **Jabir Ali** and Satya Prakash Ghrera, “An effective and robust approach of copyright protection for digital videos using blue chrominance watermark embedding algorithm”, in International Conference on new technological opportunities in networking and sciences-2018 newtons-2018, [Indexed in **Scopus**] **Accepted**

8. **Jabir Ali et. al**, “A lightweight buyer-seller watermarking protocol based on time-stamping and composite signal representation”, in International Conference on new technological opportunities in networking and sciences-2018 newtons-2018, [Indexed in **Scopus**] **(Accepted & Presented)**