

A Project report

on

Hardware Implementation of a Fragile Digital Image Watermarking Methodology

For the partial fulfilment of the requirements for the degree of B. Tech in

Electrical Engineering

by

Sanjay Das (11701615041)

Under the supervision of

Dr. Tirtha Sankar Das (External Supervisor)

**Associate Professor, Dept. of ECE, Ramkrishna Mahato Government
Engineering College**

&

Mr. Sarbojit Mukherjee (Internal Supervisor)

Assistant Professor, Dept. of Electrical Engineering, RCCIIT



Department of Electrical Engineering

RCC INSTITUTE OF INFORMATION TECHNOLOGY

CANAL SOUTH ROAD, BELIAGHATA, KOLKATA – 700015, WEST BENGAL

Maulana Abul Kalam Azad University of Technology (MAKAUT)

© 2019

CERTIFICATE of APPROVAL



To whom it may concern

This is to certify that the project work entitled “**Hardware Implementation of a Fragile Digital Image Watermarking Methodology**” is the bona fide work carried out by **Sanjay Das (11701615041)** , a student of B.Tech in the Dept. of Electrical Engineering, RCC Institute of Information Technology (RCCIIT), Canal South Road, Beliaghata, Kolkata-700015, affiliated to Maulana Abul Kalam Azad University of Technology (MAKAUT), West Bengal, India, during the academic year **2018-19**, in partial fulfillment of the requirements for the degree of Bachelor of Technology in Electrical Engineering and that this project has not submitted previously for the award of any other degree, diploma and fellowship.

Signature of the External Guide

Name:

Designation:

Signature of the Internal Guide

Name:

Designation:

Signature of the HOD

Name:

Designation:

Signature of the External Examiner

Name:

Designation:

DECLARATION



“I do hereby declare that this submission is my own work conformed to the norms and guidelines given in the Ethical Code of Conduct of the Institute and that, to the best of my knowledge and belief. It contains no material previously written by another neither person nor material (data, theoretical analysis, figures, and text) which has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgement has been made in the text.”

.....

Sanjay Das (11701615041)

Registration No.: 151170110353 OF 2015-2016

Date:

Place:

CERTIFICATE of ACCEPTANCE



This is to certify that the project titled “**Hardware Implementation of a Fragile Digital Image Watermarking Methodology**” carried out by

Name	Roll No.	Registration No:
Sanjay Das	11701615041	151170110353 of 2015-2016

is hereby recommended to be accepted for the partial fulfilment of the requirements for B.Tech degree in **Electrical Engineering** from **Maulana Abul Kalam Azad University of Technology, West Bengal.**

Name of the Examiner

Signature with Date

1.

.....

2.

.....

3.

.....

4.

.....

Date:

Place:

ACKNOWLEDGEMENT

It is my great fortune that I have got opportunity to carry out this project work under the supervision of **Dr. Tirtha Sankar Das (External Supervisor)**, Associate Professor, Dept. of ECE, Ramkrishna Mahato Government Engineering College, Purulia-723103 and **Mr Sarbojit Mukherjee (Internal Supervisor)**, Assistant Professor, Dept. of EE, RCC Institute of Information Technology, Canal South Road, Beliaghata, Kolkata-700015, both affiliated to Maulana Abul Kalam Azad University of Technology (MAKAUT), West Bengal, India. I express my sincere thanks and deepest sense of gratitude to my guides for their constant support, unparalleled guidance and limitless encouragement.

I wish to convey my deepest gratitude to Associate Prof. (Dr.) Debasish Mondal, HOD, Department of Electrical Engineering, RCCIIT and to the authority of RCCIIT for providing all kinds of infrastructural facility towards the research work.

I would also like to convey my heartfelt gratitude to all the faculty members and staffs of the Department of Electrical Engineering, RCCIIT for their whole hearted cooperation to make this work turn into reality.

Needless to say, without all the above help and support, the writing and production of this thesis would not have been possible.

Full Signature of the Student

SANJAY DAS (11701615041)

Place:

Date:



Contents

<i>List of Nomenclature</i>	2
<i>List of Acronyms</i>	3
<i>List of Tables</i>	4
<i>List of Figures</i>	5
<i>Abstract</i>	6
1. Introduction	7
2. Theory	9
2.1. Information Hiding Techniques	10
2.2. Steganography	10
2.3. Digital Image Watermarking	12
2.4. Hardware Implementation	20
3. Literature Survey	22
4. Proposed Model	29
4.1. Watermark Embedding Mechanism	29
4.2. Watermark Extraction Mechanism	32
5. Hardware Architecture of the Proposed Scheme	34
5.1. Embedding Architecture	34
5.2. Extraction Architecture	36
6. Observations and Results	38
6.1. Performance Analysis	38
6.2. Results of Hardware Simulation	42
7. Conclusion	46
8. References	47

List of Nomenclatures

- I_m = Medical Image
- $J(V)$ = Clustered Image
- I_b = Binary Image
- I_{frag} = Fragmentation of Binary Image (I_b).
- I_{mask} = Mask Image
- T_{bits} = Encrypted text watermark
- $I_{watermarked}$ = Watermarked Image
- $I_{decoded}$ = Decoded watermark bits

List of Acronyms

ROI	Region Of Interest
LSB	Least Significant Bit
FPGA	Field Programmable Gate Array
DCT	Discrete Cosine Transform
PSNR	Peak Signal to Noise Ratio
SSIM	Structural Similarity Index
UIQI	Universal Image Quality Index
IF	Image Fidelity
BPP	Bits Per Pixel
RTL	Register Transistor Logic

List of Tables

Table 6.1(a).	Imperceptibility and bit hiding capacity results	Page 40
Table 6.1(b).	Fragility Test	Page 41
Table 6.2(a).	Device utilization for Embedding	Page 43
Table 6.2(b).	Device utilization for Extraction	Page 44

List of Figures

Fig. 2.1.	Different types of Information Hiding Techniques	Page 10
Fig. 2.2(a).	Classifications of Steganography	Page 11
Fig. 2.2(b).	Steganography process	Page 12
Fig. 2.3(a).	Embedding Process	Page 14
Fig. 2.3(b).	Decoding Process	Page 15
Fig. 2.3(c).	Comparator	Page 15
Fig. 2.3(d).	Different types of watermark	Page 16
Fig. 2.3(e).	Schematic representation of visible watermarking	Page 17
Fig. 2.3(f).	Block diagram of watermarking	Page 18
Fig. 4.1.	Block Diagram of Watermark Embedding Technique	Page 30
Fig. 4.2.	Block Diagram of Watermark Extraction Technique	Page 32
Fig. 5.1.	Architecture for embedding	Page 34
Fig. 5.2.	Architecture for extraction	Page 36
Fig. 6.1.	Different steps of mask generation for formation of watermarked image	Page 39
Fig. 6.2(a).	RTL schematic of Embedding	Page 42
Fig. 6.2(b).	RTL schematic of Extraction	Page 43
Fig. 6.2(c).	Simulation for Embedding	Page 44
Fig. 6.2(d).	Simulation for Extraction	Page 45

ABSTRACT

Human society has been improved significantly in the past few decades due to the scientific and technological breakthroughs it has been blessed with. One of those breakthroughs is the transition of the information sharing medium from analogue to digital domain. As Digital information is discrete in nature, it has the capability of being transferred as well as processed at a greater rate than its analogous counterpart. That's why digital information has become dominant in latest technology. But, with this ease of convenience of diverse digital media information like images, video and audio, the issues of copyright infringement have also increased at a startling rate. So, to curb this problem, the authors have concentrated on the field of Digital Watermarking, wherein the original owner intentionally embeds some distinct data onto the media for establishing the authenticity of the owner and preventing copyright violation. Here the field of Digital Image Watermarking has been specifically explored, which is a subset of the former domain. Digital images in different fields like in medical, astronomical, artistic etc. as well as in general cases, on one hand, flourishes the prospect of their better and diverse analysis, but on the other hand it increases the possibilities of falsified representation and compromising infringement of information. In this specific domain of Digital Image watermarking, a distinctly identifiable information is implanted within the image (the cover picture) and that embedded data is kept imperceptible to the naked eye. Here an intelligent algorithm has been devised to find the Region of Interest (ROI) to be utilized for embedding and extraction. These bits to be encrypted for greater security are called watermark bits for their imperceptibility to the exterior world. And for widespread recognition and applicability of this projected scheme, the embedding and extracting methods have been realized using Field Programmable Gate Array (FPGA). In this technique first the original image is clustered. Then by thresholding, an initial binary image is produced which is then fragmented into smaller images. So in conclusion this technique can intelligently be utilized to detect the black region of interest in the original image, where the watermark bits are to be embedded at the sending end and extracted at the receiving end. This embedded information will be damaged and will differ from the extracted information, if any third party tries to access the data without any authentic permission, hence called fragile.

Chapter 1

1. Introduction

In this modern age the developments in the process of information exchange has helped human society to reach new heights. One of the most significant improvements being the transmission of information exchange process from analogue continuous form to digital discretized form [1] due to the merits the later provides like faster processing rate, lower noise disturbance, higher power efficiency etc.

Because of these above mentioned advantages in accordance the newest developments in the field of data connectivity, information exchange process around the globe in the forms of image, audio, video etc. has become more faster and easier than ever before. And with this much ease of availability and accessibility as on one hand any complicated problem can be looked upon, analysed and solved by experts around the globe without any delay to ease up people's lives, on the other hand the possibilities of malpractices like data-falsification, privacy problems [2], false-representation, copyright violation [3][4] etc. increases. Mainly in the fields of medical, defence, surveillance etc. where the issues of data security and privacy are most significant we must use those technologies which prevent our information from being mishandled.

Now to find a solution to this problem various techniques of information hiding [5] within the digital media have been developed all over the world to validate the authenticity of the original owner. One of the most recognized among these information hiding or encryption methods is Digital Watermarking, where a secretive and distinctly identifiable information is implanted on the original media without any change of the important core information of the media from the original one. Additionally this is done so that these changes remain as much imperceptible as it can be to the human senses.

Here we have focussed on the area of Digital Image Watermarking, which is a subset of the former domain and concentrates only on the media of digital images. First a distinct data is concealed in the image in the sending end before transmission, then after transmission that data is extracted from the image and compared against the embedded data. Now if those embedded and extracted data are equal then it's concluded that no unauthorized third party involvement has occurred in between and vice versa due to the fact that the watermark is fragile and it's damaged under any circumstance of unauthorized third party involvement. Robust watermarking techniques [6] used in various fields are not being focussed on here by the author. Steganography is a part of Information hiding methodology which helps to implant data in the content which helps to verify the content at the receiver end and from the above explanation it's clear that this is the method we have utilized here.

Additionally here we will concisely converse about different types of Information Hiding techniques in the following portion of the report.

Chapter 2

2. Theory:

Small descriptions of the renowned methodologies for Watermark Embedding and Extraction are given below in a classified mannerism for the purpose of building up the environment to illustrate our proposed model.

As in this modern age with the technological advancements the connectivity of people from different parts of the world and the rate of information exchange has risen tremendously, the need for privacy and copyright protection has immensely increased in the same time period.

And to quench this need many models have been devised keeping in mind the specific requirements to be fulfilled depending on the field, into which it has been implemented. As for an example robust techniques are used in defence related fields for secure communication under any circumstances and in medical imaging mostly fragile techniques are utilized for the purpose of intimating and preventing involvement of unauthorized party in the communication process. The different processes have been briefly described below.

The fragile watermarking technique or method devised and verified here in this report incorporates a Bit Replacement Method as its core philosophy for Embedding and Extraction of the encrypted data concealed or implanted into the digital images. And these processes are well illustrated in following chapters.

2.1. Information Hiding Techniques

The various types of information hiding techniques are illustrated in the figure-2.1 given below.

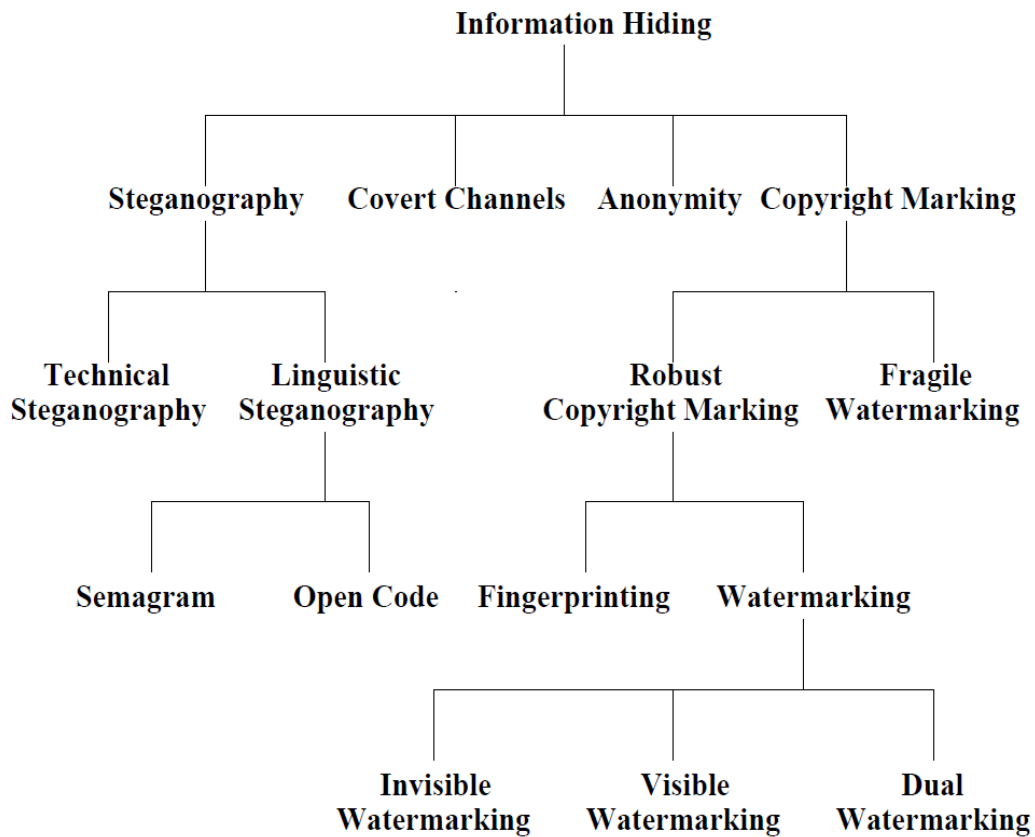


Figure-2.1. Information Hiding Techniques

2.2. Steganography

Steganography is a part of Information hiding methodology which helps to implant or conceal data within the content to be transmitted and helps to verify and validate the authenticity of the original architect of the content at the receiver end. There are two types of steganography illustrated in the figure-2.2(a).

- **Technical Steganography:** The scientific techniques to hide a distinct message, for example the usage of microdots, invisible ink, and other size reduction methods etc. within a digital media, are named as the process of Technical Steganography.
- **Linguistic Steganography:** The scheme of steganography that attempts for linguistic robustness by paying attention to linguistic criteria. Linguistic steganography conceals the distinct data within the carrier in a number of non-apparent means and is further categorized as semagrams or open codes.
 - Semagrams: These systems conceal message by utilizations of symbols or signs. A pictorial semagram utilizes innocent-looking or ordinary physical objects to express a message, such as smiley faces, doodles etc. A text semagram camouflages a message by adapting the form of the transporter text, for instance elusive changes in font type or size, handwritten text, additional spaces etc.

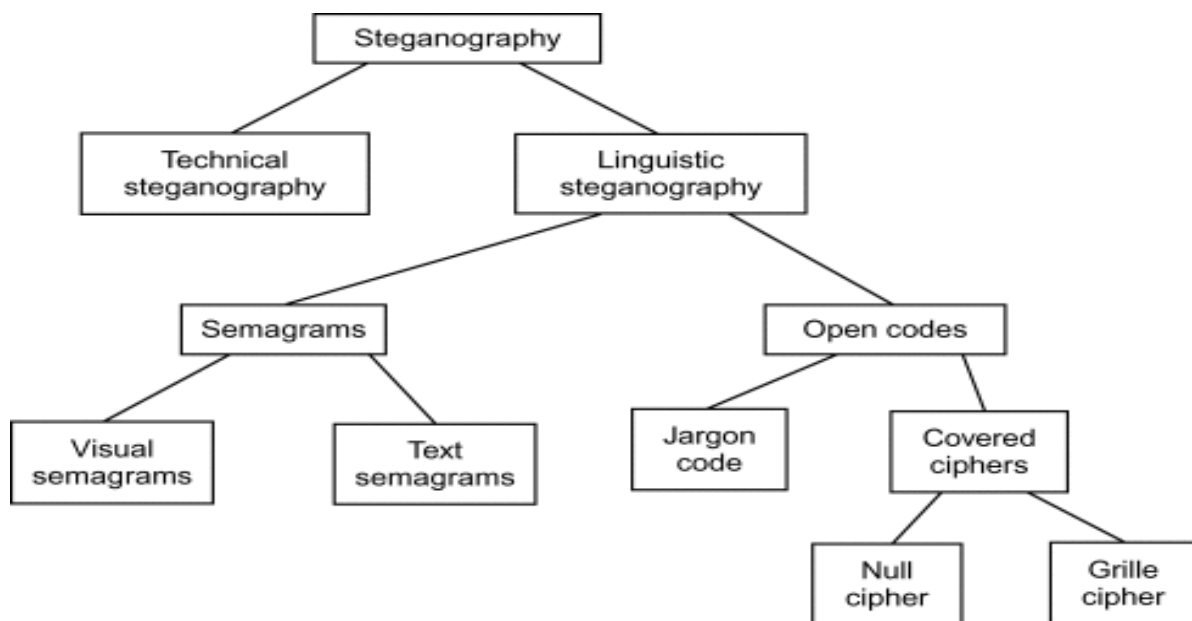


Figure-2.2(a). Classifications of Steganography

- Open codes: Open codes conceal a message in an appropriate carrier message in means that are imperceptible to an unwary observer. The carrier message is occasionally called the overt communication while the hidden message is called the covert communication.

- **Steganography Process:** The different terminologies and their roles are briefly discussed below and shown in figure-2.2(b).
 - Message: The data to be concealed within the carrier object.
 - Carrier Object: The object or the file to transmitted carrying the hidden data to be transmitted.
 - Encoder: The mechanism that carries out the encryption process of the message to be transmitted, into the carrier file.
 - Stego Object: This is the main encrypted message which will pass through unauthorized channel like internet. Where-
(Stego message = Embedded Data + Stego key)
 - Stego key: This is the secret key which is required to validate the content at receiver-end.
 - Decoder: This is the process of decoding stego message to extract the embedded data.

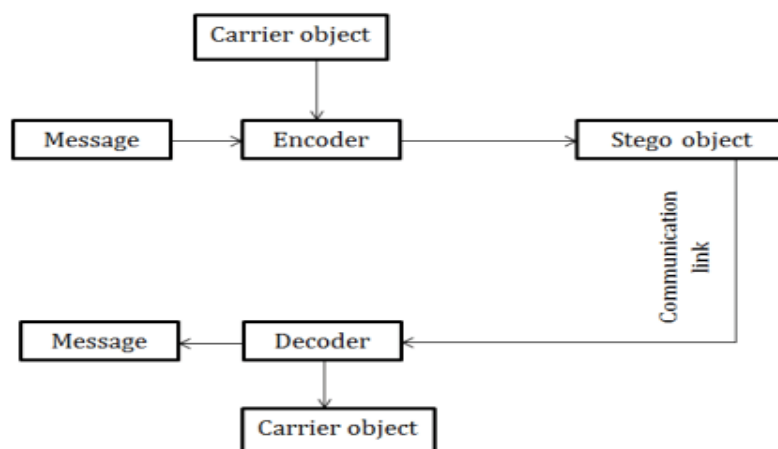


Figure-2.2(b). Steganography Process

2.3. Digital Image Watermarking

In this modern age of connectivity, sharing information has become so easy that it has developed to be extremely challenging to authenticate genuineness of that content. To find a solution to this problem among various methodologies watermarking technology has gained prominence due to the wonderful job in the field. Watermark is a distinctly identifiable information in the form of a text, audio or even in video format to be embedded onto the

original digital media under consideration before transmitting it. And a software or a specific algorithm is used to decrypt the message at the receiving end to compare it with the embedded message to prevent the whole process from copyright violation.

Digital watermark is a type of encrypted information which is implanted before transmitting the content over an un-authorized channel (like internet). This will be tested at the receiving end to authenticate genuineness of that content and also to validate the authenticity of the original architect of the digital content. In Digital Watermarking generally LSB (Least Significant Bit) replacement method is utilized.

The data to be embedded onto the content can be in a text, image, audio or even in video format and this embedding process will be realised using a specific algorithm at the sending end. Then this encrypted data will be extracted by particular algorithm or software at receiving end. If the extracted watermark matches with the previous embedded watermark then it's concluded that the content is a genuine one. Digital watermarking is mainly useful to validate the ownership and authenticity of the content, thereby provides a feasible solution to the problem of copyright violation. Digital watermarking is applicable to all forms of digital media like image, video and audio. But the authors over here have focused only on the images in the watermarking process.

➤ **Different Steps in Watermarking Process:** Watermarking is an information hiding technology where a message transferred into watermark bits is implanted onto the digital media in the sending end and decrypted at the receiving end through specific software and compared against each other to validate the genuineness of the content and authenticity of the owner. The steps are discussed below.

- **Embedding:** In Embedding, the original image is embedded with a pre-determined, uniquely distinguishable encrypted data to produce watermarked image. Here we denote the Main Image as MI, the Watermarked Image as WI, and the Embedded Data as ED. Here the embedding function (blocked as '**EMBEDDING**') takes the Main Image (MI) and embeds it with a predetermined Encrypted data ED, and produces the Watermarked Image WI which will be transmitted via communication channel. The data ED has been encrypted over here for

further safety improvements. The process is shown in the following figure-2.3(a).

$$WI = \text{EMBEDDING} (MI, ED)$$

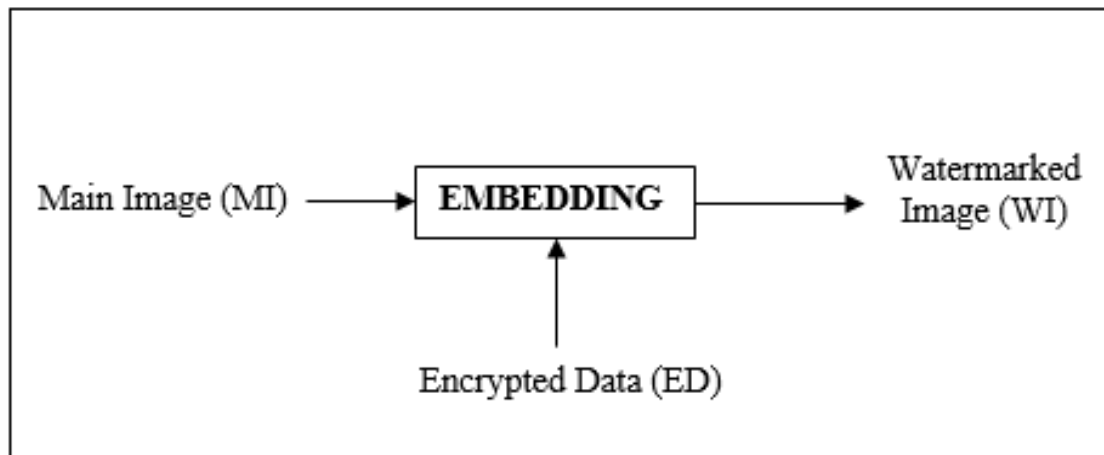


Figure-2.3(a). Embedding Process

- **Decoding:** In Decoding process, the encrypted data is extracted from the watermarked image through the decoding function taking main image and watermark image is taken as arguments. Then this encrypted data extracted here is compared with the encrypted data implanted in the embedding process to find whether any type of unauthorized accessing of the content during the transmission has occurred or not. Due to the assurance of the fact that under any irregular occurrence in the communication channel the embedded encrypted data in the content will be damaged, 1'b 1 result from the comparator ($ED = ED'$) validates the genuineness of the content as well as the authenticity of the original owner but otherwise concluded to be tampered in the process. The figure-2.3(b). shown below illustrates a simple line diagram of this process.

$$ED' = \text{DECODING} (MI, WI)$$

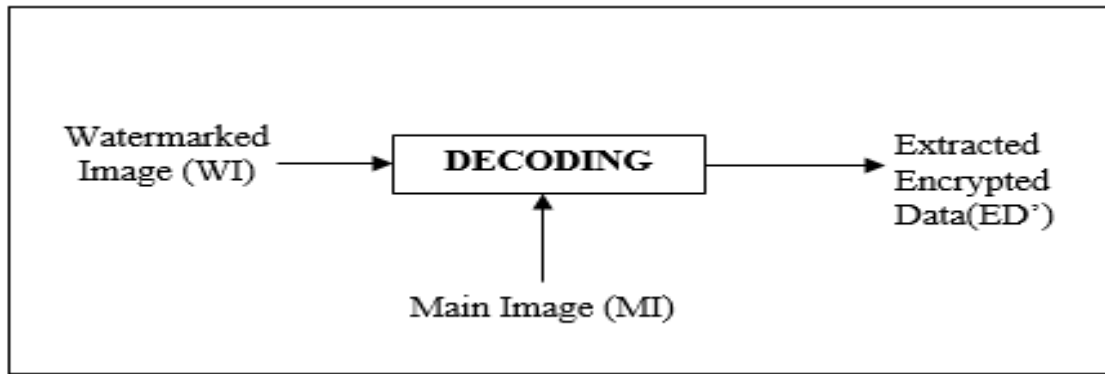


Figure-2.3(b). Decoding Process

So, If the result of the comparator is 1 (that means those two data are same) then the received watermarked image is determined to be the genuine image, else if the comparator output is 0 (that means those two data are not same) then the received watermarked image is deemed to be the tampered image. The comparator section is shown in figure-2.3(c).

$$R = \text{COMPARATOR}(ED', ED) = 1, \text{ if } ED' = ED, \text{ else } 0.$$

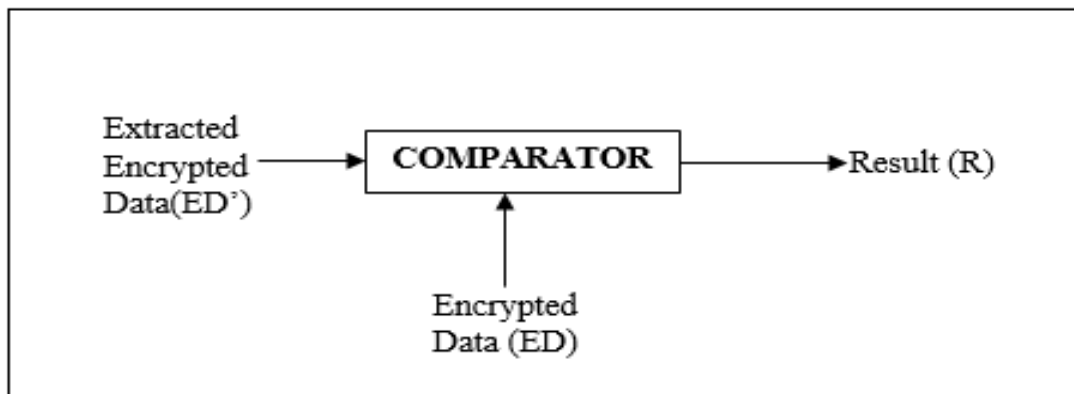


Figure-2.3(c). Comparator

➤ **Different modes of Digital Watermarking:**

In the following figure-2.3(d) different modes or types of digital watermarking techniques are classified in accordance with their working domain, type of document, human perception and application real life.

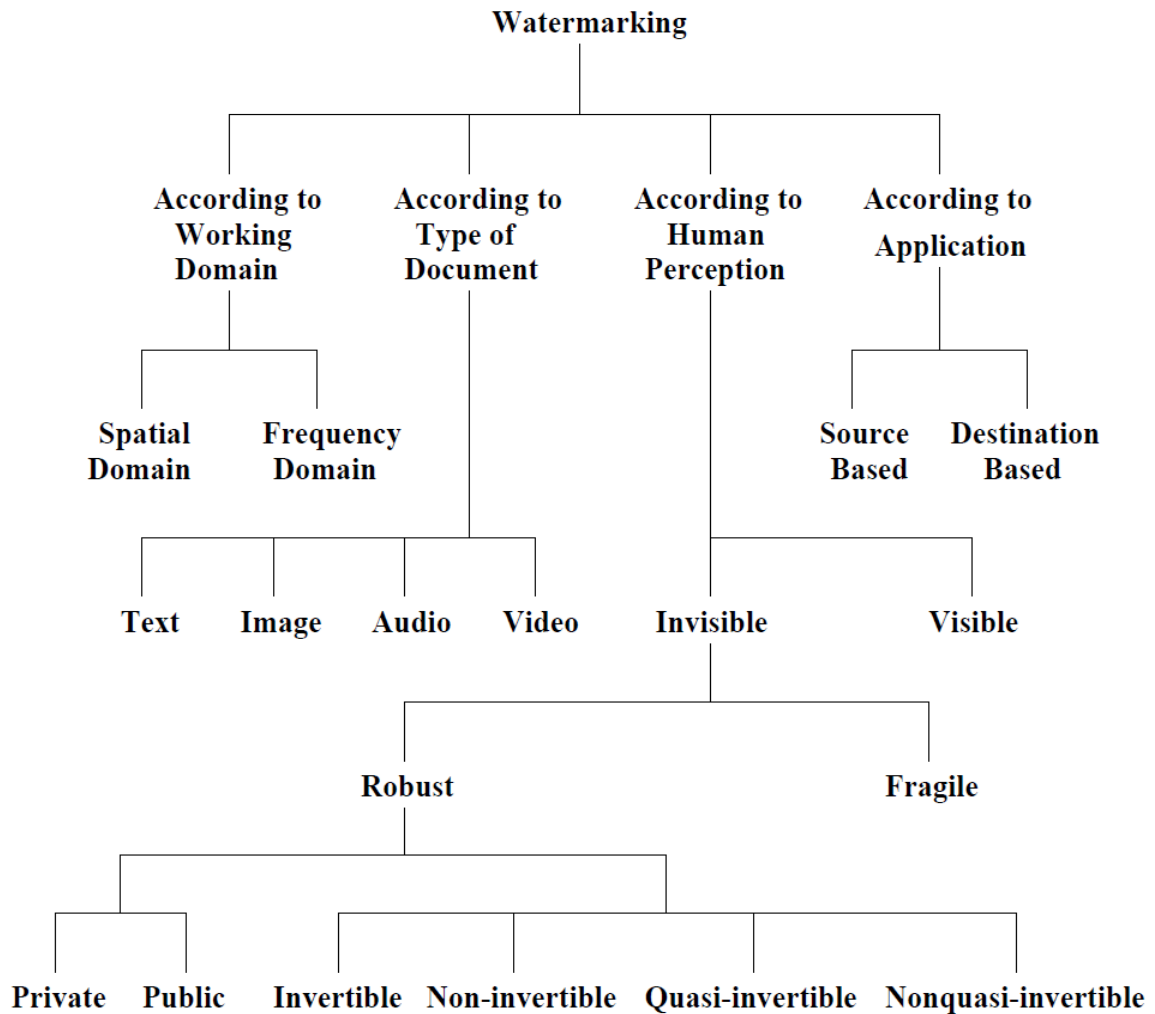


Figure-2.3(d). Classification of different types of watermarking techniques.

Depending on the type of the media content where watermarking will be executed, this process can be classified into four types. These are,

- a) **Image Format:** The file content to be watermarked is of the image type format and the watermark may be in noise form like pseudo-random Gaussian noise, or in data form like text, image, video etc.

- b) **Video Format:** The file content to be watermarked is of the video format. Digital video is a sequence of still images, which are loaded at constant frame rate in a device. So all image watermarking techniques can be applied here.
- c) **Audio Format:** The file content to be watermarked is of the audio format. And the watermark is usually Pseudo-noise embedded into the actual audio.
- d) **Text Format:** The file content to be watermarked is of the audio format. And the watermark used are of two types, visible (use of different types of signs) and invisible (use of spaces).

Depending on the level of Human Perception watermarking can also be categorized into four different types. Those are as follows,

- a) **Visible Watermarking:** In this type of watermarking depicted below in figure-2.3(e) the watermark embedded onto the original image is of perceptible logo type impressions related to the ownership of the content. This type of watermarking is used generally in commercial cases, where the owner intends to show his ownership in a direct manner.

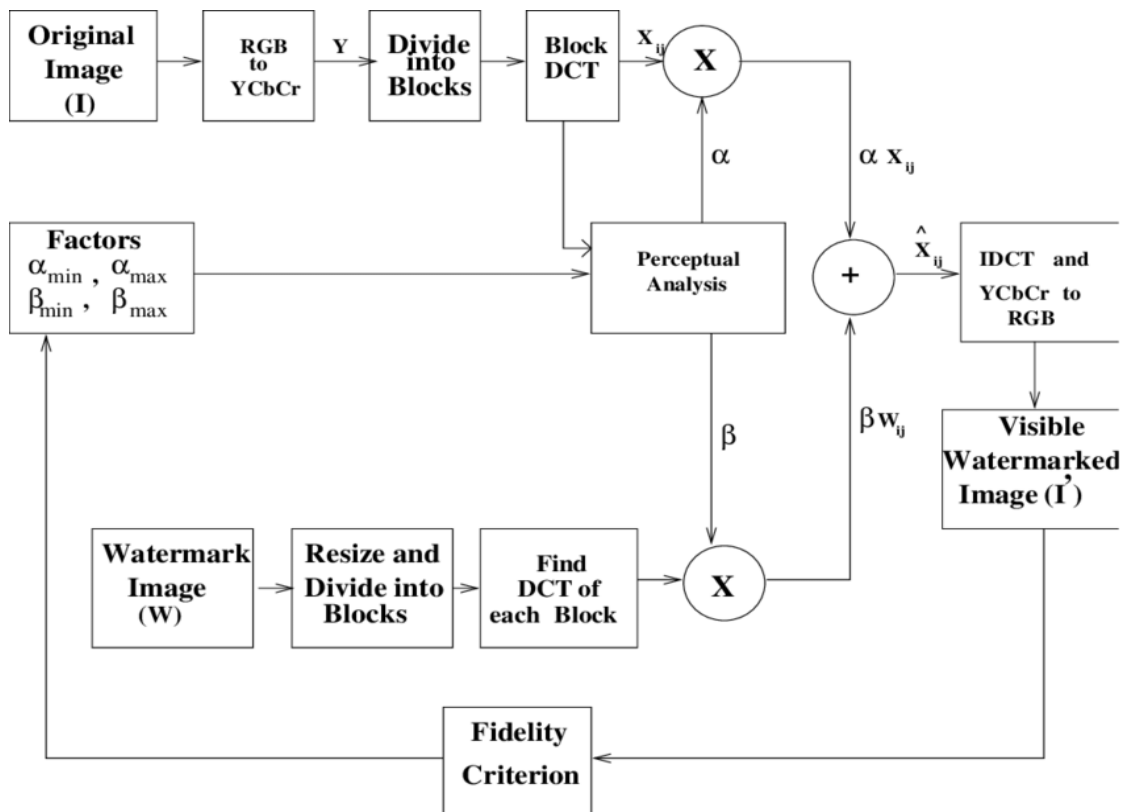


Figure-2.3(e). Schematic representation of visible watermarking.

- b) **Invisible Fragile Watermarking:** In this type of watermarking the watermark is embedded into the digital content in an imperceptible manner. And any unauthorized third party involvement in the transmission process will definitely destroy the watermark concluding an insecure transmission, hence called fragile.

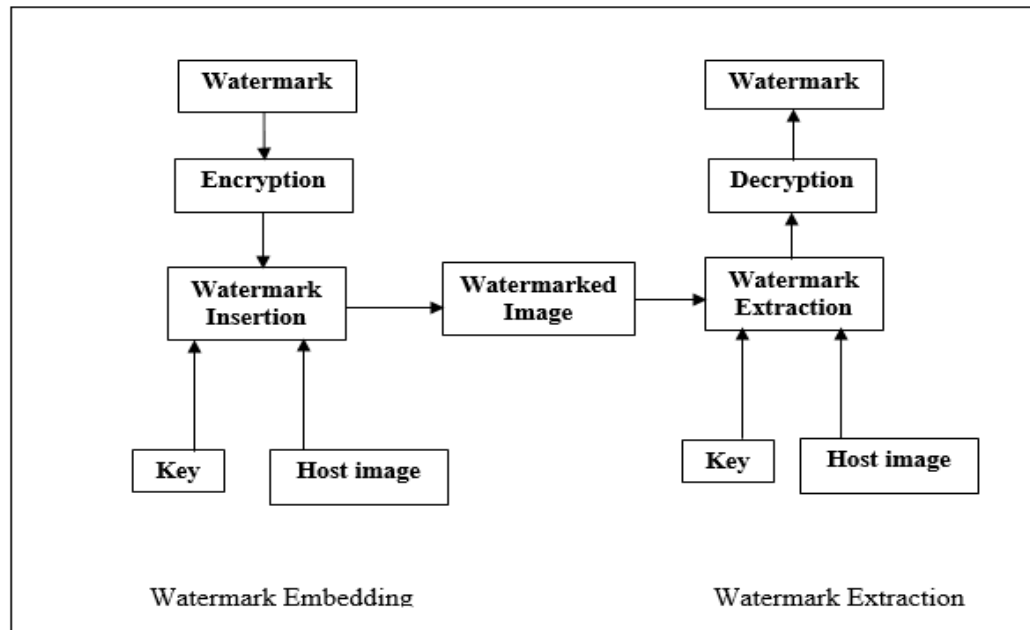


Figure-2.3(f). Block diagram of watermarking.

- c) **Invisible Robust Watermarking:** In this type of watermarking also the watermark is embedded into the digital content in an imperceptible manner. But any unauthorized third party involvement in the transmission process can not destroy the watermark concluding a fruitful transmission under any circumstances, hence called robust. This type of watermarking method is usually used in defence and intelligence fields concerning national security and other official activities. This process is used to identify any alteration is happened or not after storing the water mark.

- d) **Dual Watermarking:** Dual watermarking can be defined as the combination of visible watermarking and invisible watermarking.

Depending on the domain, watermarking can also be categorized into two different types. Those are as follows,

- a) **Spatial Domain Watermarking:** Spatial domain watermarking techniques are methods where watermarking is done directly on the pixel bits of an image or video type digital content. LSB (Least Significant Bit) manipulation is one of this type of watermarking techniques.

- b) **Frequency Domain Watermarking:** Here in this type of watermarking techniques the watermark is a type of noise embedded into a small portion of the large frequency bandwidth used for transmission of the original digital content. This type of watermarking is utilized in cases demanding robustness.

➤ **Application of Digital Watermarking:**

Digital watermarking is utilized for a widespread array of applications like, Copyright protection, where an encrypted security information is embedded into the original content as a proof of the authentic ownership of the actual architect, Source tracking, where different recipients are given dissimilarly watermarked content to track the networking roots harbouring malpractices with more ease, Broadcast monitoring, where TV news frequently covers watermarked video from international agencies for secure transmission and distribution of its content etc. There are also other applications like, Fraud and Tampering Detection, where after the content is tampered in the process of transmission by any unauthorized third party trying to access or tamper the content of the file, the recipient figures out this tampering and intimates the sender that a case of tampering has been detected and requests him to investigate communication channel. The method incorporated in the above mentioned application of Fraud and Tampering Detection robust type of watermarking techniques. Content management, video authentication etc. are the other types of usages of this technology.

Digital Image Watermarking is a subset of Digital Watermarking illustrated in the above segment. The author has mainly focussed here to develop a secure and fragile Digital Image Watermarking Technique, upon whose operation the developed watermarked image though different from the original one becomes imperceptible to the naked eye. In medical field for the purpose of better diagnosis, the methodology of

medical imaging, which centres on the construction of graphic depictions of the interior organs and tissues of a human body, arose. CT-scan, X-ray, MRI, molecular imaging, ultrasound are a number of the common fields of medical imaging. In the field of astronomy for the purpose of better understanding of the universe imaging techniques in that field also arose. Similarly technological advancements in various fields helped to increase the usage of digital imaging and analysis techniques tremendously. And with these tremendous improvements in technology on one hand flourished the prospects of analysis of intricate problematic situations in various fields instantly like, better medical treatment for the patient as the condition of the patient can be diagnosed through tested medical images by any prominent doctor present in any corner of the world or analysing an image concerning national security or confidential information to be exchanged via a non-secure communication channel etc., on the other hand it raises apprehensions over unauthorized content access, manipulation and data management issues . To elucidate better, one of the aspects of cloud computing is that it serves as a virtual storage machine and hence the same storage space can be used by multiple instances of multiple applications. So these delicate information can be manhandled for one's or any group's self-centred requirements resulting in unforeseeable repercussions. This undesired phenomena asks for some pre-emptive efficient ways to solve the problem. Hence, the need for Fragile Digital Image Watermarking technique arises which destroys all embedded confidential data from a digital image when attacked by illegitimate operators indicating an insecure transmission channel. The fragility condition of the watermark ensures that if a malicious user tries to extract the watermark by dishonest ways, then the watermark information will get totally destroyed, thereby prohibiting the extraction of watermark data by anyone who is not supposed to extract it and thus sensitive information, stored as watermark, continues to withhold its authenticity.

2.4. Hardware Implementation:

The devised algorithm for the proposed watermarking technique is simulated in the Verilog software and a synthesizable hardware RTL schematic has been produced to prove the assurance of its FPGA (Field Programmable Gate Array) realizability in reality with the intention of assuring hardware realization of an application specific integrated circuit for a widespread use in the modern society to curb the issue of copyright infringement for highly secured digital images.

It has to be ensured that the processing speed should be fast enough to avoid choking in data flow and also a platform which is totally application dependent is needed. Thus the hardware implementation reduces hardware scheme area, increase speed of performance and decrease power consumption. The hardware architecture of the real time application of watermarking can be easily developed, which also guarantees low computational cost. FPGAs ensure fast processing speed and field programmability, thus the hardware architecture can be further modified as and when required without incurring any additional cost typically involved with custom IC fabrication. Therefore, the author decided to develop the hardware architecture using FPGA to build a fast prototyping module for verifying design concepts and performance in regard of this algorithm.

Chapter 3

3. Literature Survey:

Steganography is a type of cryptography where secret information are encrypted in such a way that it cannot be perceived from outside. As suggested by T. Ogihara, D.Nakamura, N.Yokoya, by using DCT (Discrete Cosine Transform) we can vary the locally encrypted data in accordance with the properties of original image [8]. As suggested by the authors, in Discrete Cosine Transform the secrets data are encrypted into high frequency components of the image. It is more advantageous because it encrypts more data with less distortion in main image.

Information hiding is a part of Steganography where the secret data are embedded in to the digital media content (like image, video) to verify the authenticity of that media content. It is more helpful to detect whether there is any kind of copyright protection issue and tampering issue or not. As per suggested by W. Bender, D. Gruhl, N. Morimoto and A. Lu., the degree of secret data is modified in accordance with the properties of digital media [9].

Steganography is a kind of art which prevents the detection of encrypted message. Many methods such as invisible ink, microdots, digital signature, and spread spectrum are included in this technology. There is a bit difference between Cryptography and Steganography. As per suggested by N. F. Johnson and S. Jajodia, in Cryptography encrypted message cannot be understood but steganography encrypted message cannot be observed [10]. So if we apply these two methods by combining with each other the outcome will become stronger encryption. In Steganography the interceptor, who intercepts the hidden message, may even not know whether there is any kind of encrypted message.

Steganography is a kind of hidden communication. As proposed by L. M. Marvel, C. G. Boncelet and C. T. Retter, Spread Spectrum Image Steganography is more advanced where the encoder system can encode and decode the secret message by maintaining size and dynamic range of original image [11]. The encrypted message is recovered by a specific key.

This method is specially applied in covert channel communication, image tampering proofing etc.

Cryptography is an interesting part of communication system. As proposed by O. E. Thompson, using of single-pulsed tone in cryptographic system results better effective utilization of frequency and maintaining security in this process is relatively high [12]. This method also ensures higher speed of transmitting message, higher capacity and message service can be simultaneously happened with other service on a common channel.

In cryptographic ensemble system the error rate of word can be measured by the function which is proposed by D. J. Torrieri [13]. The error rate of word corresponds to the error rate of bit of plain text. Degradation of the system can be calculated with respect to PSK (Phase-shift Keying) and white Gaussian noise. By using this method we can easily calculate the differential encoding on a Cryptographic System.

There are two types of methodology in Cryptography which is examined by W. Diffie and M. Hellman, which reduce the requirement of secret key distribution channel and deliver to the equivalent of written signature [14]. This is due to the wide-range application of telescoping channel which have given to the requirement for new cryptographic system.

System Network Architecture (SNA) manages the orderly transportation of data from source to Destination of communication Network. By Adding Cryptographic function ensures the security of data during transportation. The Cryptographic function mainly modifies, distribute and verify the data when it passes through the communication channel. As suggested by R. E. Lennon [15], by associating cryptography the unprotected communication channel becomes as secure as compared to the protected host centre.

Watermark is mainly used to detect if there is any kind of tampering happened in the content or not. It includes change of pixel values, size if image etc. Watermarking is very in several fields like medical, military where data authenticity is utmost priority. As suggested by Ping Wah Wong, at the time of verification, the method uses a public cryptographic key, which can be accessed by any person without exchanging the secret key [16]. Watermarking is very important in many applications. Such as Verification of image which is captured by camera,

whether there is any kind of post manipulation is happened or not, to authenticate a specific medical image if there is any kind of tampering happened or not. Watermarking is mostly used where the secret key is not possible to exchange or the authorized person does not desire to share secret key with any other person.

As proposed by J. Fridrich, M. Goljan and Rui Du, there are two new invertible watermarking procedures for validation of digital image which is in JPEG format [17]. In the previous, the virtual authentication of image watermarking schemes results some small amount of distortion, but in the new method if any kind of noise or distortion happened in the main image at the time of authentication, the entire distortion can be removed without hampering the original image data. In the first method the whole process based on lossless compression of biased bit stream which is generated from the corresponding quantized JPEG image. In the second step, the procedure modifies the previously quantized matrix to achieve lossless embedding of one bit DCT (Discrete Cosine Transform) coefficient. By enabling both these we can get distortion free embedded data and duration of this process is very short. This new method also ensures integrity protection highly confidential image such as medical image, military image etc.

Invertible image watermarking is a new process of image authentication. As suggested by J. Domingo-Ferrer and F. Sebe, Spread Spectrum invertible watermarking system can be used to authenticate the main image without creating any kind of noise or distortion in the main image [18]. Another application of invertible image watermarking is multi-level access of watermarked images, which depends on the clearance. The main user has a control to mark the image to gain in precision.

Watermarking is used to protect the copyright information in various kinds of media such as image, audio, video content. Copyright protection is necessary to protect the creator's content from being duplicated. In today's era watermarking of 3D graphical model has become a new challenge. As proposed by T. Harte and A. G. Bors strings of bit is embedded in the form of graphical structure of the main graphical object by changing the value of location of certain vertices [19]. The main criterion of choosing vertices is to reduce the overall distortion in the watermarked object. This technique can be applied in various 3D graphical models including the industrial models.

The necessity of reversible watermarking method is to combine subliminal management information with lossless media to detect the authentication. As suggested by C. De

Vleeschouwer, J. -. Delaigle and B. Macq, the Circular interpretation of bijective transformations is created to implement a method that abides by all quality along with functional requirements of lossless watermarking [20]. Different benchmarking test has approved this method.

As proposed by Ming Sun Fu and O. C. Au, SCED (Self-conjugate error diffusion) is a method of watermarking where user can hide visual patterns in a single error diffused halftone image [21]. When the halftone image is folded or it is overlapped, the hidden pattern becomes visible. In simulation result we can clearly see the halftone image has good visual quality and the hidden patterns of halftone image are clearly visible.

As proposed by R. G. van Schyndel, A. Z. Tirkel and C. F. Osborne, we can create undetectable digital water mark on standard 512/spl *512/spl intensity image with an 8 bit gray scale [22]. This digital watermarking method is able to carry such information as authorization and authentication codes, or an essential codes for image interpretation. This method is mainly used in image tagging, copyright protection, counterfeit protection. There are total two steps in this method. In the first step bit plane manipulation of LSB (Least Significant Bit) is done which gives fast and easy decoding. The second step entirely based on utilization of linear addition of the watermark to the image data which is more difficult to decode and as result it offers more security. This digital watermarking method also offers some image processing, such as averaging which is going to take place in the image without tampering the watermark after recovery. This method is compatible with MPEG and JPEG image processing.

In today's era revolution of internet has changed everything. Everything is easily accessible from everywhere via internet protocol. But as a result the ownership of data is not maintained properly. That's why chance of duplicating documents is increasing day by day. To curb this issue Digital watermarking technology plays a significant role. Digital watermarking is proposed in such a way that it can identify owner, creator, distributor and consumer of that particular document. Its objective is to watermark a specific document which can be recovered by using a specific computer program [23]. As suggested by H. Berghel and L. O'Gorman, it is also used to track the image which is also distributed illegally. Modern digital watermarking is capable to large scale dissemination simple and cost effective. Digital

watermarking is helpful to watermark a specific document uniquely and it can be traced. The watermarked image is capable to identify the buyer as a source.

The Digital watermarking method which is proposed by L. Boney, A. H. Tewfik and K. N. Hamdy [24], we can embed digital watermark in a digital audio signal. Watermarking is a technique where we can attach digital label by hiding copyright and other hidden information into the embedded data. The watermark should be undetectable by the user and it should protect the main digital content which is intended to tampering. In the proposed method the watermark is generated by filtering a PN-sequence by using a filter which is used to approximate the frequency masking characteristics of audio signal. It is measured in the time domain so that we can use temporal masking. This method is highly effective to protect an audio signal from copyright issue.

A watermark is a kind of invisible mark which is embedded into the original image to protect it from being duplicated. This mark is capable to identify the owner as well as authorized consumer. It should not be lossy compression which creates noise in the main image at the time of watermarking. It should be tolerant to the quality loss compression with the help of transform coding and vector quantization. Normal image processing method such as low pass filtering, trimming, converting and rescaling should be independent from removing the watermark. As suggested by J. J. K. O. Ruanaidh, W. J. Dowling and F. M. Boland [25], in the phase watermarking method of digital image method Spread Spectrum Communication techniques along with matrix transformation can be used to build watermark which is more secure from tampering the content and this is also visually imperceptible. The method is mainly used in grey scale digital image. This method also proposes the method of conveying the watermarked information.

Digital watermarking is a method to watermark an image, audio and even in video file. The method, which is proposed by Chiou-Tung Hsu and Ja-Ling Wu [26], we can easily watermark in a video content. The main objective of Watermarking method is to hide the secret information in the signal to discourage the malicious person from doing tampering or the copying from the original content. In the proposed method we can predict types of MPEG standard to watermark both intraframe and non-intraframe blocks with different residual masks. The results of the proposed method show difference between the watermark frames and non-watermark frames. This method also results advance clipping of MPEG compression.

The digital watermarking method by using wave length based fusion, which is proposed by D. Kundur and D. Hatzinakos [27], is used mainly in still image watermarking where the watermark embedding process uses a multi resolution technique. The original image is mainly required to restore the main image. The simulation results also show the robustness in JPEG image compression which is lossless and noise free and it uses additive filtering.

Digital watermarking is a robust technology to embed the copyright information in the digital content. Various types of watermarking types have been invented so far to protect the digital media content. As suggested by S. C. Cheung and D. K. W. Chiu [28], in this method we can use this as a document distribution protocol, which is different from conventional techniques. In this method sensitive information are left behind. Here document management policies are not reinforced. The reinforced document needs a support in a document sharing protocol. This method is helpful to prevent from sharing the digital content. This method also provides a registration certificate to detect the identity of the end user. This method is also helpful in document check-in and document check-out process.

In medical image watermarking the main content such as patient details, history, disease details and symptoms are transmitted in such a way so that the total memory required to store the content is reduced. This is not only helpful to reduce size but also it significantly increases the security of data. [29] As suggested by D. Anand and U. C. Niranjana, this process is also cost effective. The encryption method, which has been taken before transmission of message, provides inaccessibility to the unauthorized person.

Due to necessity of privacy and security issue of medical documents, we use digital medical image watermarking technique to conceal the important information from being unauthorized distribution. [30] As suggested by G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland and R. Collorec, the proposed method named "Relevance of watermarking in medical imaging" is used to work as a complementary role with respect to the existing security system. Here the authors represent two different methods. One of which is tracing and authentication of image and the second is to control the integrity of Patient's record.

A wavelet-based watermarking method, [31] which is proposed by A. Giakoumaki, S. Pavlopoulos and D. Koutouris, is used to protect the confidential medical information. This method can embed multiple watermarks which fulfills different purposes. It contains the

digital signature of doctor which is used as authentication. It also contains a caption of watermark of patient's information and examination related data. It is capable of data integrity control. That's why these added functions provide better security protection of medical data and also provides better control of medical data distribution and managing those data with the help of this method is become easier. With the help of this method, we can automatically reject the tampered data

To authenticate that a captured from a particular camera and if there is any kind of post modification happened or not we use watermarking based authentication algorithm. In FPGA based watermarking technique the watermarking components are implemented in VHDL. After that those are simulated, synthesized and installed in FPGA device. [32] To achieve semi fragile properties which survive some amount of compression as suggested by Hyun Lim, Soon-Young Park, Seong-Jun Kang and Wan-Hyun Cho , in the proposed method DCT coefficient quantization is used. In the proposed method at the beginning the watermark bits are embedded in to LSB (Least Significant Bit) of DCT coefficient which is in medium frequency range. The whole system mainly consists in three parts. Those are LCD controller with image capture part, Embedding watermark part and the last is camera control unit. Many tests have been taken so far to test the performance of the FPGA implemented digital camera. It is shown from various results that the outcome of FPGA based camera is far better than the software and sensor enabled digital camera and also the processing time in FPGA based digital is much lower. Along with that the watermarked image can easily transmitted to the PC without any kind of hassle. The quality of the transmitted image is also better and crisp compared to the other.

As suggested by H. A. Farouk and M. Saeb, in the proposed method, named "An FPGA implementation of a special purpose processor for steganography, the secret key is known to the both transmitter and receiver [33]. If other person by any chance came to know the existence of the message, he cannot able to recover it. This method is mainly based on micro architecture of Field Programmable Gate Array.

Chapter 4

4. Proposed Model:

The author has proposed a unique scheme of embedding and extraction of the encrypted watermark in this proffered methodology, where Bit Replacement Method is incorporated as the core mechanism. And the bits replaced are the two LSBs of every 8-bit image pixels in the ROI of the Cover image. The two parts of this scheme is illustrated below with simple block diagrams.

4.1. Watermark Embedding Mechanism:

Here to generate an intelligent digital image watermarking methodology the author has devised an intelligent watermark embedding block diagram as shown in figure-4.1 to create the watermark embedded Watermarked Image (WI).

The grayscale equivalent of different digital images, picked up from open source database, are the initial requirements as per Figure 1 using the equation

$$I_m = g(a, b); 0 < a < x, 0 < b < y, g(a, b) \in \{0, \dots, 255\}$$

Where I_m is the main image having dimension $x \times y$.

Clustering is a specific technique, which is a subset of Image Segmentation technology, wherein the content of the image or its dataset is divided into precise clusters which ultimately enables a high level mechanism to extract certain specific aspects of the image. Thus, the original image is made to undergo the K-means clustering algorithm as per the relation given below.

$$J(V) = \sum_{i=1}^c \sum_{j=1}^{C_i} (||X_i - V_j||)^2$$

Where, ' $||X_i - V_j||$ ' is the Euclidean distance between X_i and V_j , ' C_i ' is the number of data points in i th cluster and ' c ' is the number of cluster centres

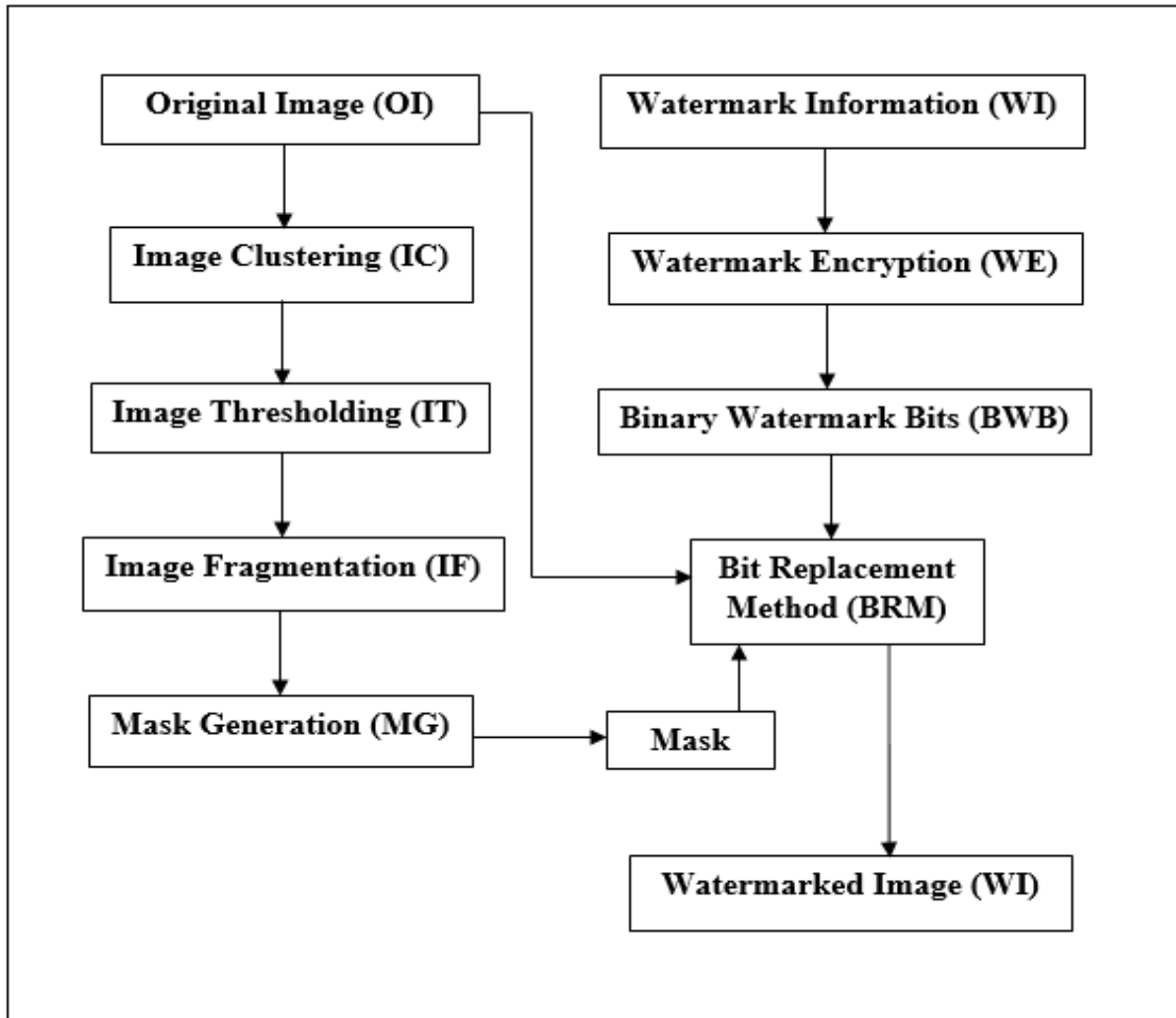


Figure-4.1. Block Diagram of Watermark Embedding Technique.

The resulting clustered image is utilized to produce an initial binary image by the method of thresholding as shown in below.

$$I_b = g(c, d); 0 < c < x, 0 < d < y, g(c, d) \in \{0,1\}, g(c, d) = 0 \text{ if } < \text{threshold limit, else } 1.$$

This binary image (I_b) is fragmented into multiple smaller images that is into 16 x 16 number of images as

$$I_{frag} = \text{Fragment}(I_b)$$

Where I_{frag} is the result after fragmentation of I_b . These fragmented images are carefully examined and in whichever smaller fragment any white pixel is found to occur, that entire fragmented image block is transformed into a sub-image having only white pixels.

Thereafter, all the sub-images are joined to generate the ultimate mask of the original image as shown in the relation,

$$I_{mask} = T(I_{frag})$$

Where $T(I_{frag})$ is the transformation of the individual fragments into the whole image. After this the scheme distinctly identifies the black ROI of the original image wherein the encrypted text watermark bits are to be hidden. The white regions of the image are of medical, as well as other field related importance, hence the author strictly wanted to hide information only in the outer black surface. Many a times, small protruding cells, tissues are present in the medical images, stars, distant nebulas are present in astronomical images and similarly in other fields also these small important portions exist in the main image. Though these small parts might not be distinctly perceivable to the human eye, are preserved to the best capacity by Image Thresholding (IT) and Image Fragmentation (IF) methods. Also, it had been observed that in case of the medical images of certain organs, black pixels are found to occur within the organ region.

The Watermark Information (WI) generally in text form is first encrypted in the Watermark Encryption (WE) block. Then the encrypted text watermark is transformed into Binary Watermark Bits (BWB), shown in the below relation as,

$$T_{bits} = E(Text)$$

Where T_{bits} are the encrypted watermark bits obtained from the encryption function $E(Text)$. These are embedded into the original medical image in the ROI in accordance with the Mask (M) through the Bit Replacement Method (BRM) to generate the Watermarked Image (WI) using the following relation,

$$I_{watermarked} = Embedding(I_m, I_{mask}, T_{bits})$$

The above algorithm carefully provides an intelligent means to dissect the region of interest of the image for watermarking automatically depending upon the original image used, without interfering with the regions of the image which are of importance to the related field fraternity.

4.2. Watermark Extraction Mechanism:

In the following, the figure-4.2 represents the block diagram of extraction of the watermark embedded into the Original Image (OI). The mask is again generated in a similar way to the embedding process. Along with this Mask, the Watermarked Image (WI) is given as inputs to the decoding block, and the watermark bits are decoded from the watermarked image using the following relation,

$$I_{decoded} = Extraction(I_{mask}, I_{watermarked})$$

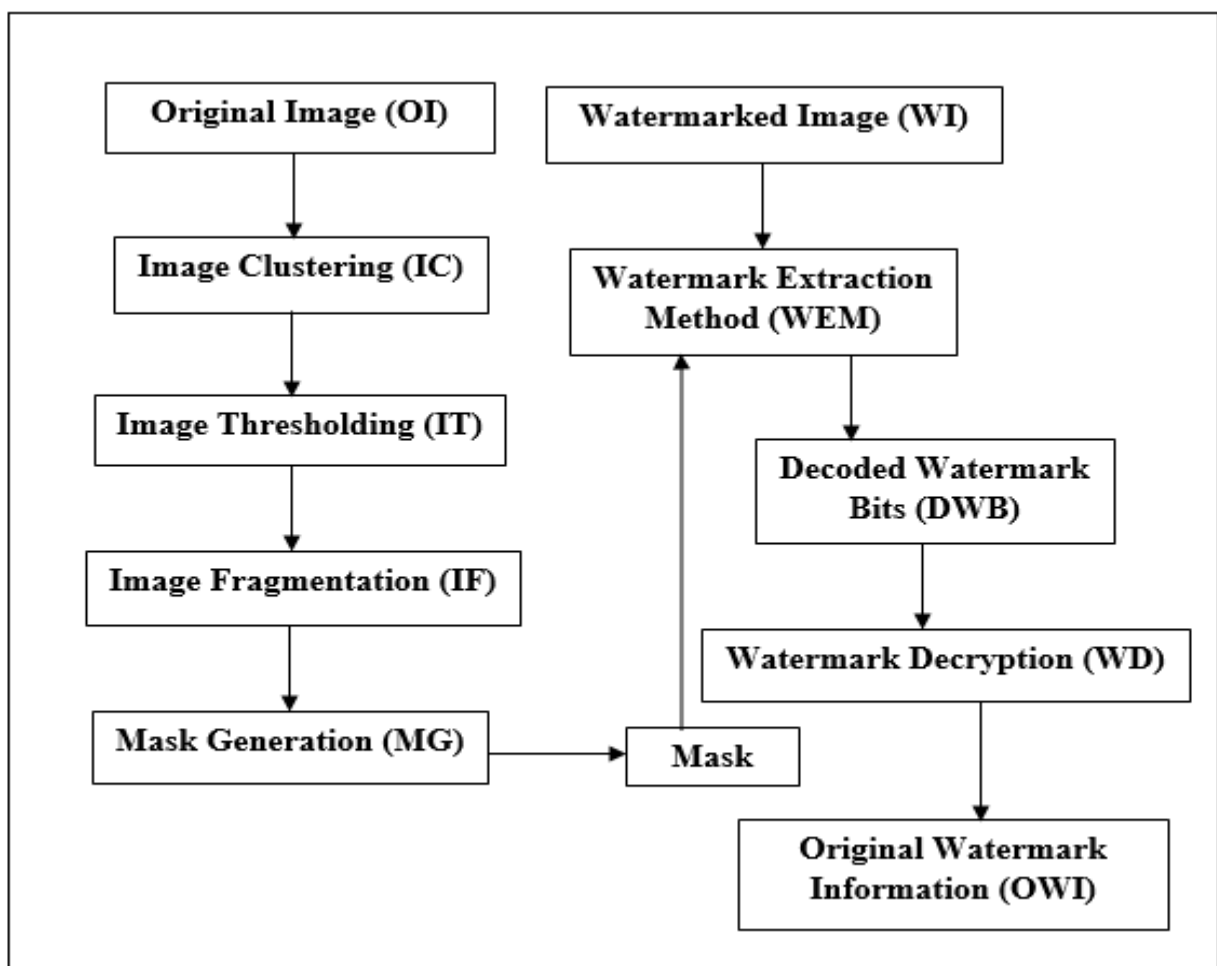


Figure-4.2. Block Diagram of Watermark Extraction Technique.

Where I_{decoded} are the Decoded Watermark Bits (DWB) and then these are decrypted to generate the original text information that was concealed into the original image as,

$$\text{Text} = D(I_{\text{decoded}})$$

Where $D(I_{\text{decoded}})$ is the decryption function.

So, the above algorithm first generates the mask from the original image in similar way to the Embedding process. And the decoding or the Extraction block operating on this mask and the Watermarked Image (WI) extract the watermark bits, which after decryption are transformed into the Watermark Text, which is to be compared with the text used in the Embedding process to verify the authenticity of the image and the security of the communication channel.

Chapter 5

5. Hardware Architecture of the Proposed Scheme:

For the ambition of designing an adaptable and diversely applicable hardware, the use of modern FPGA (Field Programmable Gate Array) is favoured due to fact that FPGA in recent times is exerting a flawless performance in various fields. The author has implemented this watermark embedding and extracting mechanism using the Xilinx (ISE version 13.2) on the Spartan FPGA series device xc7a30t-3csg324. And the language used to set up our scheme is Verilog and the inputs to our system are given manually.

In this system there are two distinct subdivisions illustrated below with figures.

5.1. Embedding Architecture:

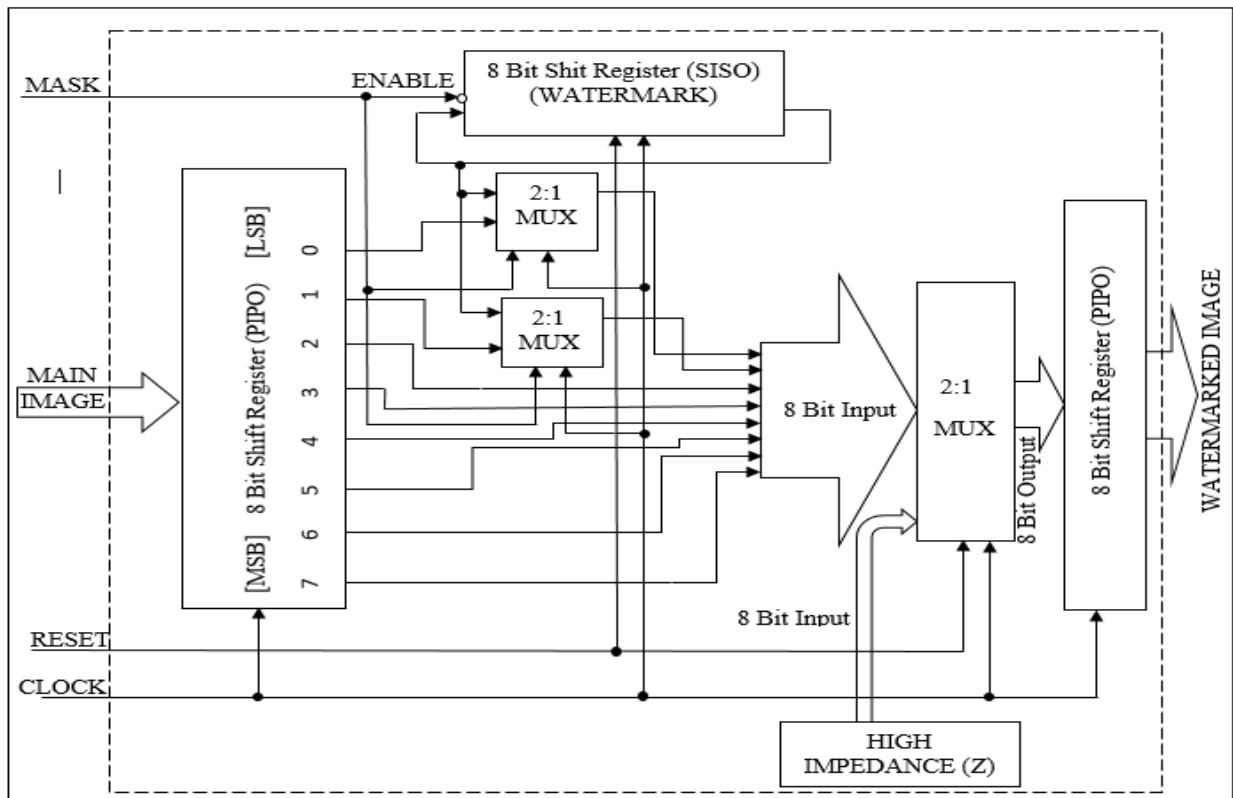


Figure-5.1. Architecture for Embedding.

The hardware architecture of the Embedding Mechanism is depicted in Figure-5.1 below. The inputs to the system are original image pixel, mask bit, reset, and clock.

First the original image pixels are taken into an 8 bit PIPO (Parallel Input Parallel Output) shift register, whose bit positions are depicted as 7, 6, 5, 4, 3, 2, 1, and 0. Among those bit positions bit values from 7 to 2 are given to the 8-bit output PIPO shift registers' 7 to 2 positions directly without any operation. The rest two bits from 1 and 0 positions are given to second input positions of two 2x1 multiplexers, and the first input positions takes a watermark bit as input. The output of the multiplexers goes to the 0th and 1st positions of the output register, and the value of those outputs depends on the mask bit value given to the selector port of the multiplexers. So the mask value decides the corresponding watermark bit is embedded onto the present pixel or not (yes if mask value is 0, else no) or bits are replaced by the watermark or not. And each time a watermark bit is embedded onto the pixel the watermark bit is updated accordingly. The reset and clock inputs are required to respectively restart and synchronize the system.

4.2. Extraction Architecture:

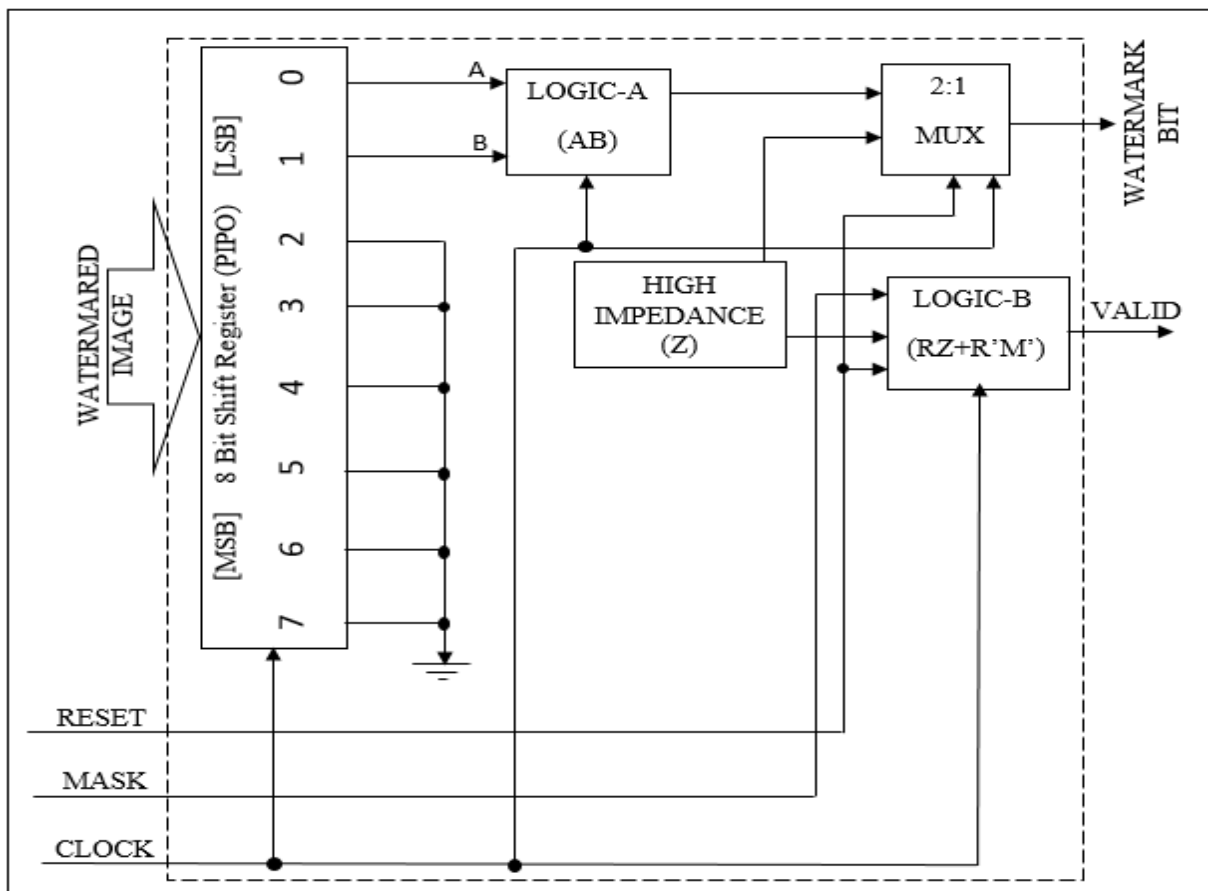


Figure-5.2. Architecture for Extraction.

The architecture shown in the Figure-5.2 is the hardware architecture of the Extraction mechanism used in this scheme. The watermarked image, mask, reset and clock are the four inputs to this architecture block. As for the output part, there are watermark bit and a valid bit to validate that watermark data (if 0 watermark bit is not valid, else valid). The input watermark image bits are taken in an 8 bit PIPO (Parallel Input Parallel Output) shift register. These bits are marked as 7, 6, 5, 4...0 from the MSB to the LSB. The bits from 7 to 2 positions are grounded as they are not important to calculate the watermark bit. The rest two bits are taken as inputs to a block named Logic-A (the function of this block is applying AND logic to the inputs) and whose output is fed into the first input of a 2x1 multiplexer, whose second input is fed from a high impedance block. And the selector port of the multiplexer is controlled by the reset input of the system. The output

of this multiplexer is taken out from the system as the watermark. There is also another block called Logic-B (the function of this block is calculating the equation $(RZ+R'M')$ and the result is given as output), which takes three inputs named mask (M), high impedance (Z) and reset (R), and the output is taken out of the system as an output named VALID, whose value denotes the recent output from the multiplexer is a valid watermark or not (If 1 it's valid, else not valid). The clock input is used to synchronize all the blocks of the system.

That's how through errorless application of the above two hardware architectures watermark embedding onto digital image and extraction of those watermark bits from those images can be executed. The results gotten from applying and simulating this algorithm are discussed in the following.

Chapter 6

6. Observations and Results:

Upon modelling this scheme we have tested the model using various standard inputs to see, if the model is performing satisfactorily and can be applied in real life situations to execute the purposes it has been devised to fulfil flawlessly.

And the results gotten after the experiments on this system has been well documented and verified in the below portion of this report.

6.1. Performance Analysis:

Diverse X-Ray, USG, CT scan and MRI etc. medical images, and other general digital images of dimension 256x256, are picked up from open source database for experimental verification of the scheme. Figure-5.1 vividly shows the different steps of the mask formation which ultimately helps in embedding the watermark into the medical images to generate the ultimate watermarked image. The algorithm has been tested on the different images, results of some of which are shown in figure-6.1.

Table 6.1(a) shown below evidently institutes the bit hiding capacity and the imperceptibility results for the proposed technique. Where PSNR stands for Peak Signal to Noise Ratio, UIQI stands for Universal Image Quality Index, SSIM stands for Structural Similarity Index, IF stands for Image Fidelity and BPP stands for Bits Per Pixel. Time is the duration of time in seconds needed for the embedding mechanism.

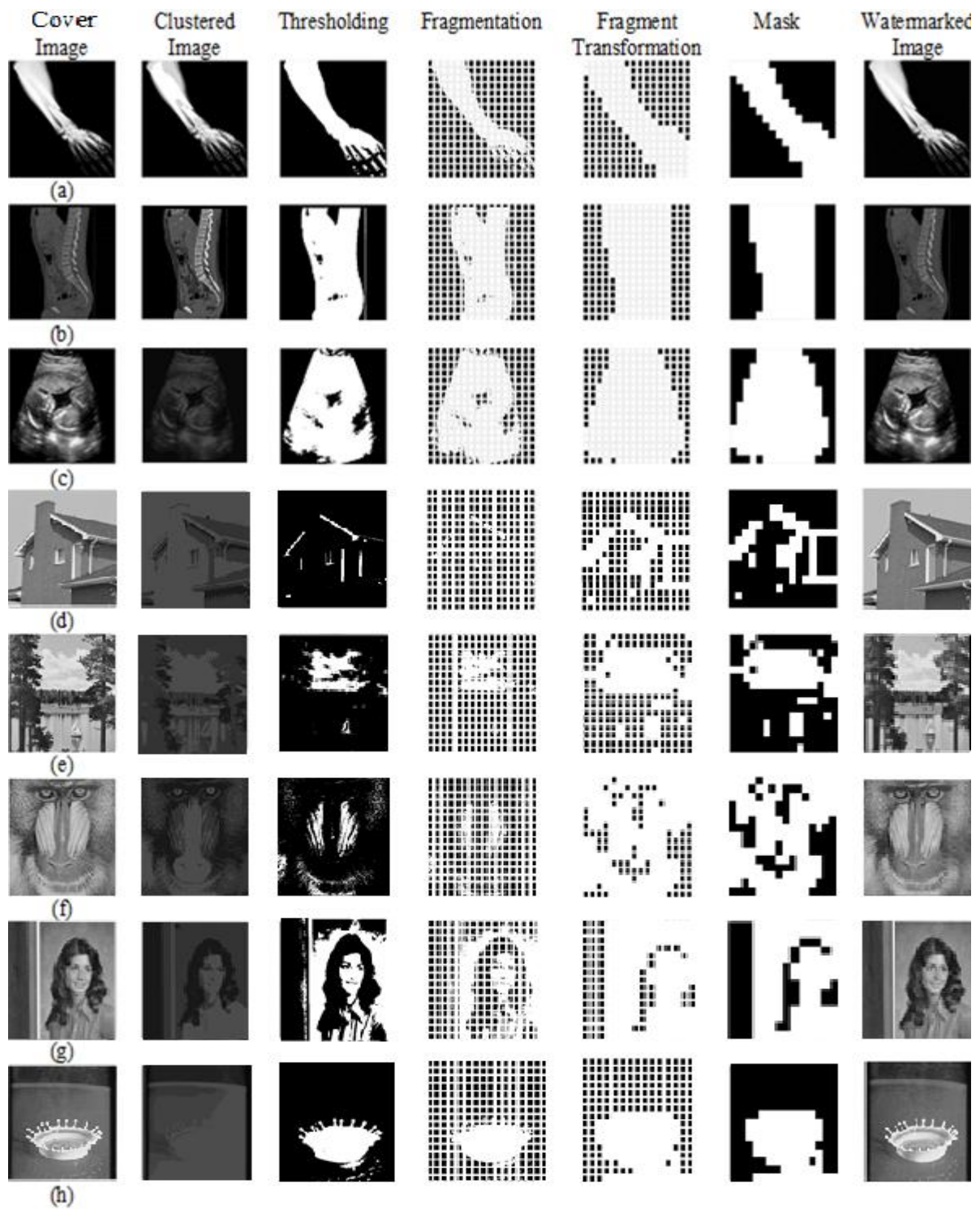






Figure-6.1. Different Steps of mask generation for subsequent formation of watermarked image.

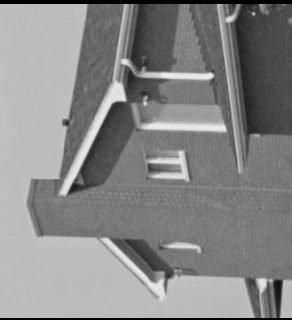

Table 6.1(a) Imperceptibility and Bit hiding capacity results.

Image	PSNR	UIQI	SSIM	IF	BPP	Time(sec)
(a)	62.645	0.387	0.599	0.999	1.68	9.367
(b)	54.486	0.582	0.833	0.998	1.23	6.827
(c)	68.139	0.738	0.845	0.999	0.74	4.023
(d)	46.650	0.837	0.974	0.994	0.75	12.256
(e)	54.457	0.835	0.946	0.999	0.5	10.349
(f)	44.005	0.869	0.981	0.989	0.39	2.471
(g)	51.275	0.971	0.991	0.998	0.74	4.462
(h)	75.921	0.757	0.849	0.999	0.73	4.312
(i)	57.286	0.341	0.588	0.999	1.83	10.689
(j)	58.624	0.804	0.871	0.999	0.59	3.496
(k)	51.759	0.905	0.969	0.998	0.33	2.102
(l)	59.6	0.772	0.87	0.999	0.65	3.962
(j)	44.147	0.735	0.949	0.989	0.78	4.667
Average	55.93	0.796	0.866	0.998	0.838	6.07

Now the Table-6.1(b) shown below institutes the fact that the final watermarked image is fragile in nature and with assistance of that fact no mischievous handler can excerpt the watermark from the watermarked image. So as a result of this fragility the embedded watermark won't be extracted in its original form, if the image is exposed to any type of image processing attacks illustrated below in Table-6.1(b).

Table-6.1(b) Fragility Test

Image Processing Attack	Image Condition	Decoded Result
No attack		<p>Command Window</p> <pre>Original Word encoded: ID_No.-ABCD9876 Decoded encrypted text: JFbRt44IKMOEEEE Decrypted text: ID_No.-ABCD9876</pre>
Gaussian Noise		<p>Command Window</p> <pre>Original Word encoded: ID_No.-ABCD9876 Decoded encrypted text: (The corresponding binary bits are all 0) Decrypted text: (Nothing to be displayed)</pre>
Poisson Noise		<p>Command Window</p> <pre>Original Word encoded: ID_No.-ABCD9876 Decoded encrypted text: (The corresponding binary bits are all 0) Decrypted text: (Nothing to be displayed)</pre>
Median Filtering		<p>Command Window</p> <pre>Original Word encoded: ID_No.-ABCD9876 Decoded encrypted text: (The corresponding binary bits are all 0) Decrypted text: (Nothing to be displayed)</pre>
Erode		<p>Command Window</p> <pre>Original Word encoded: ID_No.-ABCD9876 Decoded encrypted text: (The corresponding binary bits are all 0) Decrypted text: (Nothing to be displayed)</pre>

<p>Rotation</p> 	<p>Command Window</p> <pre>Original Word encoded: ID_No.-ABCD9876 Decoded encrypted text: (The corresponding binary bits are all 0) Decrypted text: (Nothing to be displayed)</pre>
<p>Crop</p> 	<p>Command Window</p> <pre>Original Word encoded: ID_No.-ABCD9876 Decoded encrypted text: (The corresponding binary bits are all 0) Decrypted text: (Nothing to be displayed)</pre>

6.2. Results of Hardware Simulation:

The following figures shows us the results of the simulation of the algorithm on the hardware platform of Xilinx ISE 13.2. The required code is scripted in Verilog Hardware Description Language. The RTL Schematics are depicted in figure-6.2(a) and figure-6.2(b).

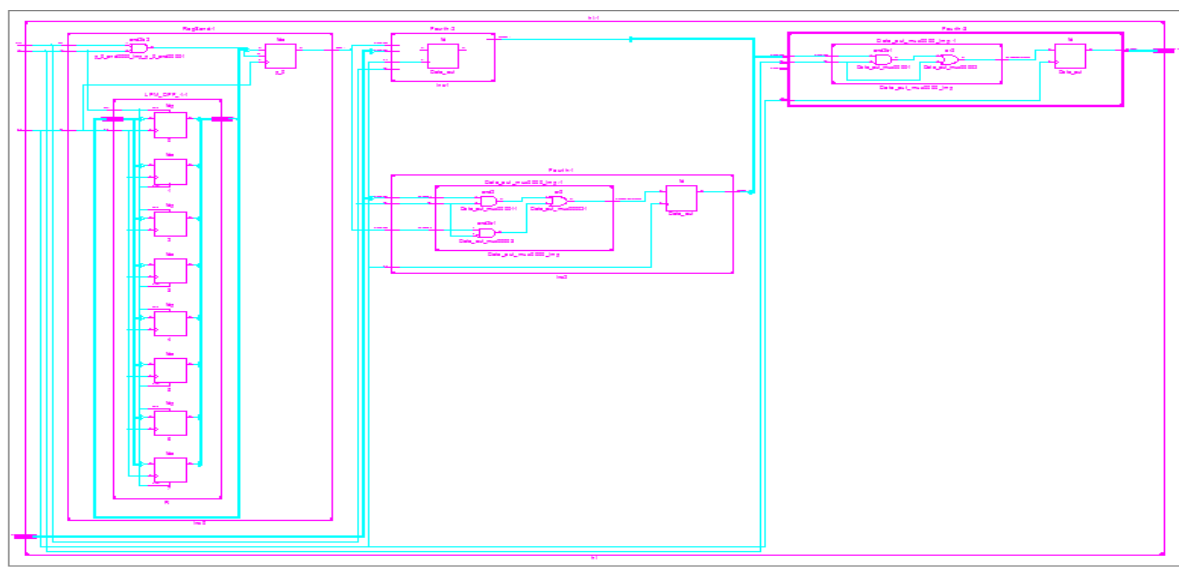


Figure-6.2(a). RTL Schematic of Embedding

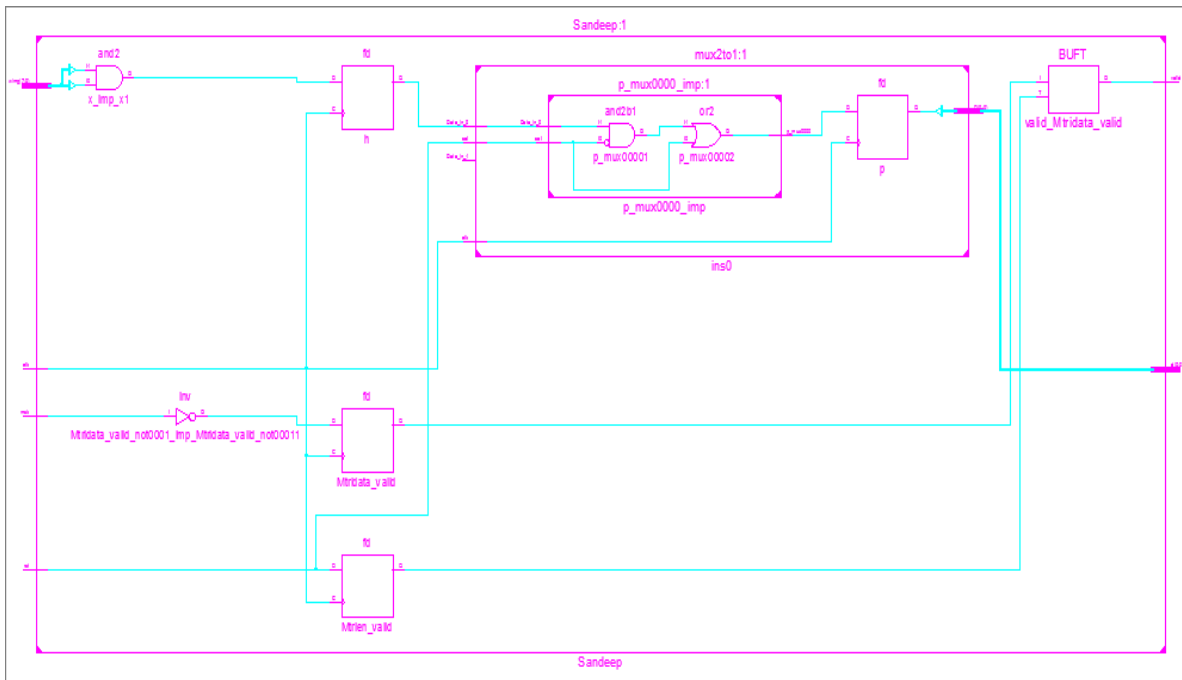


Figure-6.2(b). RTL Schematic of Extraction

Device utilization summary or application synopsis for the device has been illustrated in Table-6.2(a) and Table-6.2(b) shown below. The evidence from these two tables validate the fact that estimated disbursement for the synthesis is negligible as a miniscule percentage of the logic devices available are incorporated in our design. The values of the grey image pixels to be watermarked are diversified over an extended range of practical inputs in accordance with the modelled system to assess and complement the proper functioning of the synthesized schematic.

Table-6.2(a). Device Utilization for Embedding

Device Utilization Summary (estimated values) Encoder			[-]
Logic Utilization	Used	Available	Utilization
Number of Slices	7	4656	0%
Number of Slice Flip Flops	13	9312	0%
Number of 4 input LUTs	3	9312	0%
Number of bonded IOBs	19	190	10%
Number of GCLKs	1	24	4%

Table-6.2(b). Device Utilization for Extraction

Device Utilization Summary (estimated values)Decoder			[-]
Logic Utilization	Used	Available	Utilization
Number of Slices	1	4656	0%
Number of Slice Flip Flops	2	9312	0%
Number of 4 input LUTs	1	9312	0%
Number of bonded IOBs	7	190	3%
Number of GCLKs	1	24	4%

The watermarked image pixels acquired at the output of the Embedding system is taken in as input to the Decoding or Extracting system along with the corresponding mask bit. And after extraction and decryption mechanism the watermark obtained is exactly equal to the watermark embedded into the image pixels in embedding mechanism, and this is precisely shown in Figure-6.2(c) and Figure-6.2(d). This brilliantly institutes the fact that the modelled scheme is operating competently.

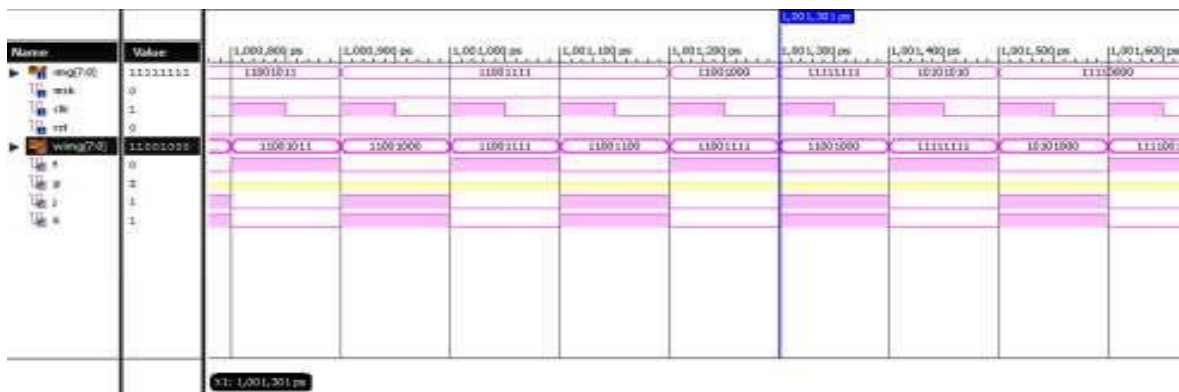


Figure-6.2(c). Simulation of Embedding

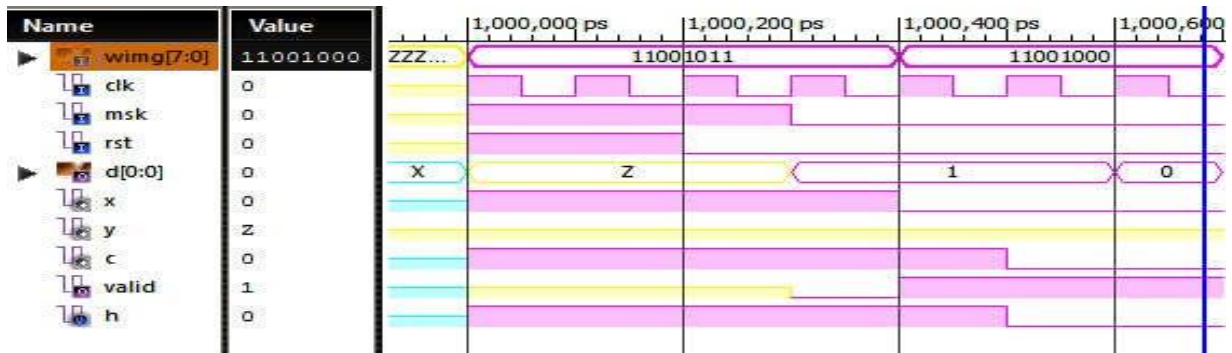


Figure-6.2(d). Simulation of Extraction

Moreover, the average usage of logic devices for Embedding and Extraction schemes are calculated as 2.8% and 1.4% correspondingly. In comparison with other schematics of Digital Image Watermarking it is concluded to be less complex than them but in effectiveness and efficiency it contests with them with its performance.

Chapter 7

7. Conclusion:

The modelled system consolidates a spatial domain digital image watermarking technique, which incorporates a bit replacement mechanism as its core embedding process. The brilliance of the projected scheme is its merits over other methods in parametric performances like higher Peak Signal to Noise Ratio value, Bits per Pixel etc. A random encoded text bit together with the intelligent binary masked image are utilized here to determine the authenticity and proficiency of the designed methodology. The delicacy or fragility feature of the watermark is confirmed by testing this technique in the face of some of the usual image processing strikes and it assures that an attacker cannot extract the watermark from the embedded medical image. Therefore this devised scheme affirms the dual benefit of greater analysis of medical and general cases and protection from copyright violation issues. Mentioning dual benefit in the former line we have highlighted the benefits of our proposed methodology to be able to hide the watermark bits in the ROI and being able to maintain the regions of significance unhampered as well. This design has been effectuated in the hardware architecture using FPGA anchored on hardware realization for wider acceptance and swifter exercitation of the scheme. The proffered method thus has been able to generate an intelligent technique for selection of ROI for digital images and thereby succeeded in realizing the watermarking algorithm.

Chapter 8

8. References:

- [1] Abhishek Basu & Subir Kumar Sarkar, "On the Implementation of Robust Copyright Protection Scheme Using Visual Attention Model", *Information Security Journal: A Global Perspective*, 22:1, 10-20, 2013.
- [2] G. P. S. Tejay, "Introduction to Cybercrime in the Digital Economy Minitrack," 2012 45th Hawaii International Conference on System Sciences, Maui, HI, USA, 2012, pp. 3040-3040.doi: 10.1109/HICSS.2012.346.
- [3] Thomas J. Holt, Bernadette H. Schell, "Hackers and Hacking: A Reference Handbook", Santa Barbara, CA, ABC-CLIO, 2013.
- [4] K. S. Wilson and M. A. Kiy, "Some Fundamental Cybersecurity Concepts," in *IEEE Access*, vol. 2, pp. 116-124, 2014. doi: 10.1109/ACCESS.2014.2305658.
- [5] Mohanty, S.P., "Digital watermarking: a tutorial review". Report, Department of Electrical Engineering, Indian Institute of Science, Bangalore, India (1999).
- [6] R. Eswaraiyah and E. Sreenivasa Reddy, "Robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest," in *IET Image Processing*, vol. 9, no. 8, pp. 615-625, 8 2015. doi: 10.1049/iet-ipr.2014.0986.
- [7] Mouna Jouini and Latifa Ben Arfa Rabai, "Comparative Study of Information Security Risk Assessment Models for Cloud Computing systems". The 6th International Symposium on Frontiers in Ambient and Mobile Systems (FAMS 2016). *Procedia Computer Science*. Volume 83, 2016, Pages 1084-1089. <https://doi.org/10.1016/j.procs.2016.04.227>.
- [8] T. Ogihara, D. Nakamura and N. Yokoya, "Data embedding into pictorial images with less distortion using discrete cosine transform," *Proceedings of 13th International Conference on Pattern Recognition*, Vienna, Austria, 1996, pp. 675-679 vol.2.doi:10.1109/ICPR.1996.546908
- [9] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for data hiding," in *IBM Systems Journal*, vol. 35, no. 3.4, pp. 313-336, 1996.doi: 10.1147/sj.353.0313

- [10] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," in *Computer*, vol. 31, no. 2, pp. 26-34, Feb. 1998. doi: 10.1109/MC.1998.4655281
- [11] L. M. Marvel, C. G. Boncelet and C. T. Retter, "Spread spectrum image steganography," in *IEEE Transactions on Image Processing*, vol. 8, no. 8, pp. 1075-1083, Aug. 1999. doi: 10.1109/83.777088
- [12] O. E. Thompson, "Cryptographic signaling applied to radio communication circuits," in *IRE Transactions on Vehicular Communications*, vol. 9, no. 2, pp. 17-24, Aug. 1960. doi: 10.1109/IRETV1.1960.32958
- [13] D. J. Torrieri, "Word Error Rates in Cryptographic Ensembles," in *IEEE Transactions on Aerospace and Electronic Systems*, vol. AES-9, no. 6, pp. 901-905, Nov. 1973. doi: 10.1109/TAES.1973.309665
- [14] W. Diffie and M. Hellman, "New directions in cryptography," in *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, November 1976. doi: 10.1109/TIT.1976.1055638
- [15] R. E. Lennon, "Cryptography architecture for information security," in *IBM Systems Journal*, vol. 17, no. 2, pp. 138-150, 1978. doi: 10.1147/sj.172.0138
- [16] Ping Wah Wong, "A public key watermark for image verification and authentication," *Proceedings 1998 International Conference on Image Processing. ICIP98 (Cat. No.98CB36269)*, Chicago, IL, USA, 1998, pp. 455-459 vol.1. doi: 10.1109/ICIP.1998.723526
- [17] J. Fridrich, M. Goljan and Rui Du, "Invertible authentication watermark for JPEG images," *Proceedings International Conference on Information Technology: Coding and Computing*, Las Vegas, NV, USA, 2001, pp. 223-227. doi: 10.1109/ITCC.2001.918795
- [18] J. Domingo-Ferrer and F. Sebe, "Invertible spread-spectrum watermarking for image authentication and multilevel access to precision-critical watermarked images," *Proceedings International Conference on Information Technology: Coding and Computing*, Las Vegas, NV, USA, 2002, pp. 152-157. doi: 10.1109/ITCC.2002.1000379
- [19] T. Harte and A. G. Bors, "Watermarking graphical objects," *2002 14th International Conference on Digital Signal Processing Proceedings. DSP 2002 (Cat. No.02TH8628)*, Santorini, Greece, 2002, pp. 709-712 vol.2. doi: 10.1109/ICDSP.2002.1028189
- [20] C. De Vleeschouwer, J. -. Delaigle and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," in *IEEE Transactions on Multimedia*, vol. 5, no. 1, pp. 97-105, March 2003. doi: 10.1109/TMM.2003.809729
- [21] Ming Sun Fu and O. C. Au, "Self-conjugate watermarking technique for halftone images," in *Electronics Letters*, vol. 39, no. 4, pp. 356-358, 20 Feb. 2003. doi: 10.1049/el:20030273

- [22] R. G. van Schyndel, A. Z. Tirkel and C. F. Osborne, "A digital watermark," Proceedings of 1st International Conference on Image Processing, Austin, TX, 1994, pp. 86-90 vol.2. doi: 10.1109/ICIP.1994.413536
- [23] H. Berghel and L. O'Gorman, "Protecting ownership rights through digital watermarking," in Computer, vol. 29, no. 7, pp. 101-103, July 1996. doi: 10.1109/2.511977
- [24] L. Boney, A. H. Tewfik and K. N. Hamdy, "Digital watermarks for audio signals," Proceedings of the Third IEEE International Conference on Multimedia Computing and Systems, Hiroshima, Japan, 1996, pp. 473-480. doi: 10.1109/MMCS.1996.535015
- [25] J. J. K. O. Ruanaidh, W. J. Dowling and F. M. Boland, "Phase watermarking of digital images," Proceedings of 3rd IEEE International Conference on Image Processing, Lausanne, Switzerland, 1996, pp. 239-242 vol.3. doi: 10.1109/ICIP.1996.560428
- [26] Chiou-Tung Hzu and Ja-Ling Wu, "Digital watermarking for video," Proceedings of 13th International Conference on Digital Signal Processing, Santorini, Greece, 1997, pp. 217-220 vol.1. doi: 10.1109/ICDSP.1997.628022
- [27] D. Kundur and D. Hatzinakos, "A robust digital image watermarking method using wavelet-based fusion," Proceedings of International Conference on Image Processing, Santa Barbara, CA, 1997, pp. 544-547 vol.1. doi: 10.1109/ICIP.1997.647970
- [28] S. C. Cheung and D. K. W. Chiu, "A watermarking infrastructure for enterprise document management," 36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the, Big Island, HI, USA, 2003, pp. 10 pp.-. doi: 10.1109/HICSS.2003.1174246
- [29] D. Anand and U. C. Niranjana, "Watermarking medical images with patient information," Proceedings of the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society. Vol.20 Biomedical Engineering Towards the Year 2000 and Beyond (Cat. No.98CH36286), Hong Kong, China, 1998, pp. 703-706 vol.2. doi: 10.1109/IEMBS.1998.745518
- [30] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland and R. Collorec, "Relevance of watermarking in medical imaging," Proceedings 2000 IEEE EMBS International Conference on Information Technology Applications in Biomedicine. ITAB-ITIS 2000. Joint Meeting Third IEEE EMBS International Conference on Information Technol, Arlington, VA, USA, 2000, pp. 250-255. doi: 10.1109/ITAB.2000.892396
- [31] A. Giakoumaki, S. Pavlopoulos and D. Koutouris, "A medical image watermarking scheme based on wavelet transform," Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE Cat. No.03CH37439), Cancun, 2003, pp. 856-859 Vol.1. doi: 10.1109/IEMBS.2003.1279900

- [32] Hyun Lim, Soon-Young Park, Seong-Jun Kang and Wan-Hyun Cho, "FPGA implementation of image watermarking algorithm for a digital camera," 2003 IEEE Pacific Rim Conference on Communications Computers and Signal Processing (PACRIM 2003) (Cat. No.03CH37490), Victoria, BC, Canada, 2003, pp. 1000-1003 vol.2. doi: 10.1109/PACRIM.2003.1235953
- [33] H. A. Farouk and M. Saeb, "An FPGA implementation of a special purpose processor for steganography," Proceedings. 2003 IEEE International Conference on Field-Programmable Technology (FPT) (IEEE Cat. No.03EX798), Tokyo, Japan, 2003, pp. 395-398. doi: 10.1109/FPT.2003.1275785
- [34] D. Ziener and J. Teich, "FPGA core watermarking based on power signature analysis," 2006 IEEE International Conference on Field Programmable Technology, Bangkok, 2006, pp. 205-212. doi: 10.1109/FPT.2006.270313
- [35] Abhishek Basu et al. "Some Studies on Quality Metrics for Information Hiding", National Conference on Recent Innovations in Computer Science & Communication Engineering, 2016. ISBN: 978-93-86005-02-1
- [36] A. Mestiri, A. Kricha, A. Sakly and A. Mtibaa, "Watermarking for integrity, authentication and security of medical imaging," 2017 14th International Multi-Conference on Systems, Signals & Devices (SSD), Marrakech, 2017, pp. 475-481. doi: 10.1109/SSD.2017.8166967.
- [37] Abhishek Basu et al., "On the implementation of a secure medical image watermarking", National Conference on Frontline Research in Computer, Communication and Device (FRCCD), 2015.

