## CHAPTER 1 INTRODUCTION

Now-a-days it is very significant to concern with the digital information is used for intellectual rights and its protection. In this way, the advanced signal processing is very useful in digital watermarking concerns of theft of copyright and multimedia information. The research is going on digital watermarking in many institutes as applications. The purpose of this study are problems occurs and its remedies intervention of copyright and multimedia information. Problem of digital watermarking and motivation are introduced in this chapter.

## Background

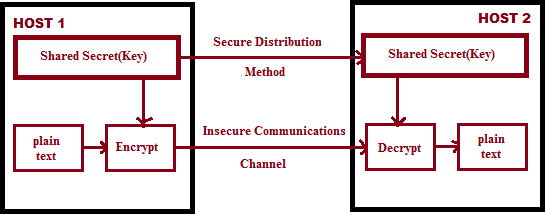
There are many times used of cryptography and steganography for communication purpose and in reply form in earlier stage for revolution against Persian and American as invisible ink which was glow in brightness [1-3]. In World War, the steganography was used for hiding the messages using dots and dashes [4]. The Germans would shroud information in as microdots decreasing the information measure or some other record. [5]. Moreover, the stegnography was used by digital watermarking for audio and video communication.

## Techniques for hiding the information

* + 1. **Cryptography**

Cryptography as the investigation of mystery (crypto) composing (graphy) and characterized as the arithmetic science as information back. It permits two individuals, generally known as Alice and Bob, to speak with one another safely sending and not to alter information. The strategy for masking the cipher text so as to conceal its data is encryption and the scrambled content is known as cipher text. The way toward returning cipher text to its unique content is unscrambling. Figure

1.1 shows the process of cryptography [1].



**Figure 1.1: Cryptography used for Transfer of Information**

* + 1. **Steganography**

Steganography defines as the secret and covered writing which is taken from the Greek [1] as dealers are exchange the data threw e-mails or by spies for communications. Give us a chance to think about that Alice, who needs to impart a mystery message m to Bob, chooses arbitrarily an innocuous message or spread item C. The message to be shared is then implanted into C, by utilizing key K (called stego-key), and the cover object C is changed to stego object S. This stego item can be transmitted to Bob without raising any doubt. This ought to be done so that an outsider knowing just the obviously innocuous message S can't recognize the presence of the mystery. The spread article could be any information, for example, picture documents, composed content or computerized sound. In an ideal framework, a typical spread item ought not to be recognizable from the stego object, neither by a human nor by a PC searching for factual examples [6].

Alice transmits the stego object S to Bob over an unreliable channel. Bounce can reproduce the message m by utilizing a similar key K as utilized by Alice during installing the message in the spread article. The extraction procedure ought not to require any information of the spread article.

Any individual viewing the correspondence ought not to have the option to choose whether the sender is sending covers with messages inserted into them. At the end of the day, an individual with various spread items ought not mindful telling any information. The implanted information is to be imparted by stego in inconspicuous strategy and seen information isn't send for the wellbeing reasons. These are the mystery information and secured all the inconspicuous messages [6].

* + 1. **Digital Watermarking**

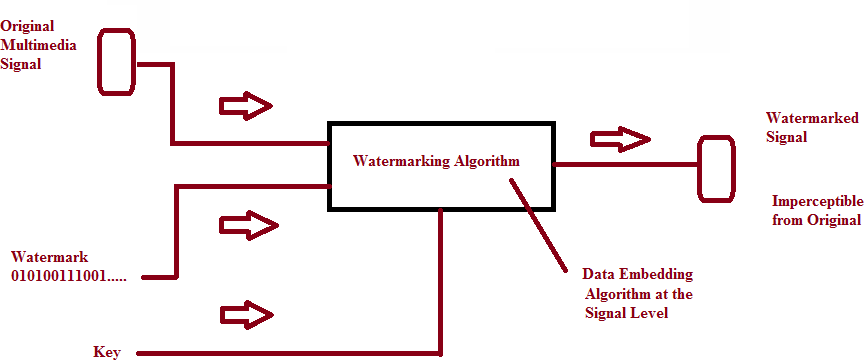
To protect digital information at large scale against illegal manipulation, need a suitable technology that facilitate to avoid threats of intellectual property theft and unlawful tampering without any negotiation. The original messages in digital form arises because of information in digitally stored is easily copied rather than analogy.

So the digital watermarking is used for better and it may be comprised of codes and for signal interpretation. Because of special detector used in this technology, different images are drawn by codes [7]. It has following properties:

* + - 1. Non-obstructive; it should be unperceivable for host signal.
      2. Discreet; not authorized for some mean data and watermark sinking for some places.
      3. Extracted; The data must be full of reliability for watermarking signal.
      4. Robustness; the watermark must be so that modification is going on easy process of data distortion and for other applications.

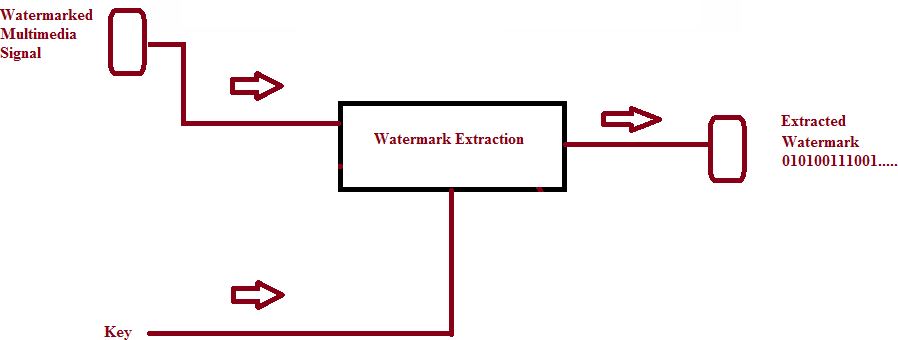
The following Figure 1.2 and 1.3 shows a basic process of watermarking in which it is cleared that a watermark exhibits a sequence of binary data and applied in a special way for the purpose. This information is used for embedded system in regular process by the

watermark and this procedure consists of hoist signal regarding watermark and then to be interoperate according to the embedded system and watermark.



**Figure 1.2: Process of embedded of watermark**

The embedded design is used for reliable purpose and completed the whole process of watermark. The watermark has some basic features such as recoverable in different disturbances conditions and changeable situations, it must be secure without any unwanted information and data even not accessible different messages, it must be non-removable. After that it must be assured that watermark is secure for a given embedded system and necessary codes for every place and entity. Accept this; it is also ensure that digital watermarking is not assurance for any undisturbed data and authentication and resist messages of unwanted with a scientific and significantly proof or evidence.



**Figure 1.3: Process of extraction of watermark**

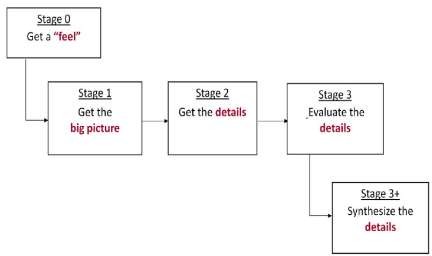
Many researchers have done a good work on the digital watermarking and its algorithm design, for improvement its reliability with many obstacles and complexity according to the utmost requirements of industries and moreover the digital watermarking system. So the digital watermarking system is broadly used for multimedia communications and its different applications with its security and reliability.

# CHAPTER-2 LITERATURE REVIEW

A writing survey is important to think about the examination zone and what issue around there has been explained and should be illuminated in future. A legitimate writing audit gives strong foundation to a respectable research work. To begin an examination work, the initial step is to discover the issue of research and to pick explicit targets of need. There has been numerous strategies and procedures characterized by the scientists to experience through and land at certain finish of research destinations. So as to pick explicit destinations of research on need to pursue a commonplace procedure to land at the finish of uniqueness, curiosity and centrality of the issue in a particular territory/sub region. One needs to begin with a more extensive space of some territory/sub zone and keeping in mind that doing investigation of writing thin down the area to explicit purpose of issue to settle on. Writing overview incorporates the investigation of different wellsprings of writing in the territory of research. It incorporates finding the related material from magazines, books, look into articles, logical research papers distributed in different meetings, diaries and exchanges. Study and understanding the writing other than logical research papers is bit simple as it expounds the ideas in basic and illustrative strategies. In the meantime these substance can't be considered as base to touch base at the finish of surrounding research goals as it isn't upheld through legitimate survey by different scientists working in the territory. Audit of a logical research paper is a monotonous activity. It needs the earlier learning of the region of research. The logical research papers are profoundly organized, minimized and exact in clarification. One may take couple of days to couple of weeks to comprehend an examination paper distributed in standard companion looked into diaries. The specialists need to receive certain way for doing writing audit of such writing. One of the run of the mill procedures was trailed by us to make a writing survey and edge the goals of research. The procedure chart is appeared in Fig 2.1, which incorporates into every one of the five phases characterized as under:

### Review process

* + 1. Stage 0: Get the Feel
    2. Stage 1: Get Big Picture
    3. Stage 2: Get the Details
    4. Stage 3: Evaluate the Details
    5. Stage 3 +: Synthesize the Details.



### Figure 2.1 Review Process Stages

The survey procedure is isolated into five phases so as to make the procedure straightforward and versatile by each analyst. As it reflects from the writing that while starting the finding of research goals, it is important to begin with a more extensive space of any region/sub region of intrigue and thin down to explicit issue, the procedure portrayed in the outline incorporates the narrowing down alongside the exploration destinations as result with support of the issue. The subtleties of different stages pursued are exhibited beneath.

#### Stage 0: Get a “feel”:

This stage is the start of writing audit process wherein one needs to comprehensively choose his/her territory of intrigue and begin looking through the logical research papers from legitimate sources. This stage gives the subtleties to be checked while beginning writing review with a more extensive area and ordering them as indicated by necessities. It needs to experience a portion of the data rapidly to get the vibe of the paper. The data expected to quickly think

about the paper is what the paper manages? What is length of the paper? Who is the distributer? What are the substance of the paper and so forth? Despite the fact that this stage does not actually order the examination papers, it supports to proceed. The procedure embraced under this stage incorporates following exercises.

* + - * Read the title.

 

* + - * Look at the figures
      * Read the section/sub-section headings.

#### Stage 1: Get a “picture”:

So as to comprehend the paper comprehensively and get a thought whether the paper precisely have a place with the examination zone/sub territory chose or it strays, if digresses how much, these ideas are clarified this stage, known as Get Big Picture. It helps in characterizing the examination papers as indicated by key issues and narrowing down the review. The papers are chosen through the stage 0, are handled through this stage characterized into various gatherings. The gatherings of research papers are set up as indicated by basic issues and application sub territories. So as to comprehend the paper, it is important to discover the responses to specific inquiries by perusing the Title, Abstract, presentation, end and segment and sub area headings. Following are the issues to be replied during this stage.

* + - * What research area / sub-topic does the paper fall under?
      * What problem does the paper attempt to solve?
      * What is the motivation for this problem?
      * Why is this paper needed – i.e. what is related work and why is it not sufficient 
      * Broadly, how does the paper solve the problem?
      * How do the authors defend the solution?
      * What category of paper is this?

#### Stage 2: Get the “details”

Stage2 manages going inside and out of each exploration paper and comprehend the subtleties of philosophy used to legitimize the issue, avocation to centrality and oddity of the arrangement approach, exact inquiry tended to, significant commitment, scope and confinements of the work exhibited. Littler arrangement of papers needs to experience this stage and concentrate the information required for its usage in research. The accompanying Table demonstrates the inquiries and the plausible areas in the exceedingly organized research paper.

### Table 2.1: Stage 2 questions along with probable location of answers in the papers

|  |  |
| --- | --- |
| **What You are looking for?** | **Where to find it?** |
| What problem does the paper attempt to  solve? | Introduction, Problem definition |
| What is related work? What are gaps? | Introduction, Literature Survey or Related  Work |
| What Contribution does the paper claim-  idea, Technique, Proof, Surprising result etc? | Introduction, Conclusion |
| How does the paper solve the problem? | Solution, Experiment, Figures |
| How do the authors defend the solution? | Methodology, Experiment, Results |
| What is the precise research question |  |

|  |  |
| --- | --- |
| addressed? | Introduction, Problem Definition |
| Why is it believed that solution works,  better than previous? | Solution approach, Figures |
| What are assumptions, scope? | Problem Definition, Solution approach |
| What are details of proposed solution – argument, proof, implementation, experiment? | Solution, System details, Experiment, Methodology, figures |
| What evidence is provided? | Figures, Results |
| What is the take-away message from the  paper? | Overall |

#### Stage 3: “Evaluate the details”:

After getting the details like key issue / problem, solution approach, hardware / software setup, experimental design, results obtained, advantages and limitations presented by the researchers, it is necessary to evaluate these details with some standard aspect to compare, correlate, and generalize the concepts & methods presented by the authors with reference to other similar works. This stage provides an insight how to deal with evaluation of the details presented by the researchers and generalize the concept. In the beginning it is not possible to evaluate these details, as it needs to check as relative and comparative aspects in relation to the works presented by the researchers. Therefore it is necessary for the researcher to complete stage 2 for all the selected paper, prepare a comparative study chart of all the papers and then proceed for this stage. In order to evaluate the details certain questions have been framed and presented below. This stage evaluates the details in relation to significance of the problem, Novelty of the problem, significance of the solution, novelty in approach, validity of claims etc. Some of the

questions below can be answered independently without going into the details of other papers. Questions related to this analysis are:

* + - * Is the research problem significant?
      * Is the problem novel?
      * Is the solution approach novel?
      * Are the contributions significant?

 

alternate approaches of solution been explored?

* + - * Are assumptions valid? Has paper violated assumptions?
      * Are the claims valid?
      * Are the different parts of the paper consistent?
      * Are the figures, graphs, diagrams precise?
      * Does the paper flow logically?
      * What is the paper trying to convince you of? Does it succeed?

#### Stage 3+: “Synthesize the detail”:

Stage 3 deals with evaluation of the details presented and generalization to some extent. This stage deals with synthesis of the data, concept & the results presented by the authors. This stage does not only require the understanding of other research papers but requires creative thinking and good knowledge in the area / sub area of research. Here imagination of situations different from those presented and expected results has to be predicted. In short it uses interpolation and extrapolation to find out the gaps in the published research. In order to understand the process and estimate the stage, questions have been framed that needs to be answered after in depth and critical analysis of all the data presented in the literature review. The literature excluded or classified in other groups through stage 1 and 2 shall also be of help to answer these questions.

* + - * What are some alternative approaches to address the research problem?
      * Could there be a different way to substantiate the claim?
      * Are their counter-examples or arguments against the paper‟s claims?
      * Are all assumptions identified and validated?
      * How can the research results be improved?
      * How can the results be generalized?
      * What are the new ideas and open problems suggested by this area?

A detailed review of 41 research papers on Digital watermarking published within the period of year 1990 to year 2017 has been undertaken. The review process based on the three stage analysis was adopted. The papers have been taken from various publications as like IEEE Transaction, conference etc. For all the 41 research papers, this process was exercised by us of whom the final findings and the outcomes have been discussed in the next chapter. This process helped us to easily classify the literature, evaluate, synthesize, summarize and build the problem statement of my research proposal.

### Categorical Review in Digital Watermarking

All research papers under the following sections, would describe the particular issues found in the area along with the summaries of the papers reviewed under each issue, followed by issue- wise findings and common findings. A table with papers under particular issues has been included, which would help in understanding some specific findings of each research paper. All the papers reviewed are based on four issues which are shown below. The review summary of each paper is described as follows:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **S.**  **No** | **Issue** | **IEEE**  **Transaction** | **IEEE**  **Conference** | **IEEE**  **Proceedings** | **IEEE**  **Symposium** | **Total paper** |
| 1 | Perceptual Transparency | 6 | 1 | 0 | 1 | 8 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2 | Payload of the Watermark | 5 | 2 | 1 | 0 | 8 |
| 3 | Robustness | 3 | 4 | 2 | 2 | 11 |
| 4 | Others | 0 | 3 | 1 | 0 | 4 |

### Table 2.2: Various Issues in Digital Watermarking

* + 1. **Issue 1: Perceptual Transparency**

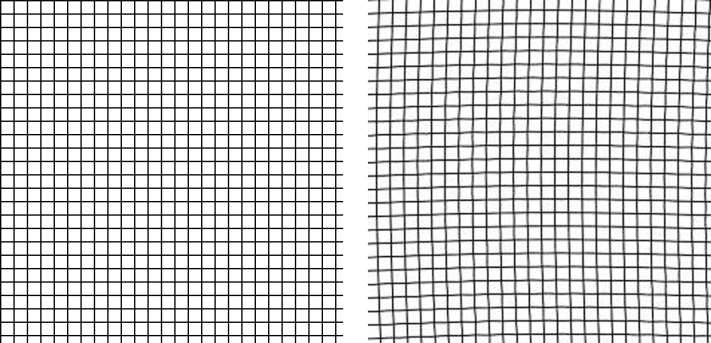
The embedded system used in watermarking algorithm does not affect any existing data and no one can make a difference between original data and watermark data [11]. But changes in data is always present when it is compared with original data and no one can access this type of data originally and also with modifications for comparison. So there is requirement to compare both the watermark and original data.

**[FABIEN A. P. PETITCOLAS, et-al, 1999]** It is regularly felt that interchanges might be verified by encoding the traffic, however this has once in a while been satisfactory by and by. Æneas the Tactician, and other traditional essayists, focused on strategies for concealing messages as opposed to for enciphering them, albeit current cryptographic procedures began to create during the Renaissance, This paper find that Wilkins still favored covering up over figuring since it stimulates less doubt. This inclination perseveres in numerous operational settings right up 'til today. For instance, a scrambled email message between a known street pharmacist and someone not yet under doubt, or between a worker of a barrier contractual worker and the international safe haven of an unfriendly power, has clear ramifications. So the investigation of correspondences security incorporates encryption as well as traffic security, whose quintessence lies sequestered from everything data. This control incorporates such innovations as: spread range radio, which is broadly utilized in strategic military frameworks to anticipate transmitters. This paper gave an outline of data stowing away by and large and steganography specifically. This paper took a

gander at a scope of utilizations and attempted to put the different strategies in chronicled setting so as to clarify the connections between them, the same number of as of late proposed frameworks have neglected to gain from verifiable experience. This paper at that point portrayed various assaults on data concealing frameworks, which between them crush the vast majority of the present contenders in the copyright stamping business. This paper have depicted an apparatus, StirMark, which breaks huge numbers of them by including sub perceptual bending, and this paper have portrayed a custom assault on reverberation covering up. This prompted a discourse of stamping when all is said in done. This paper depicted a portion of the issues in building a general hypothesis and the functional necessities that stamping plans and steganographic frameworks may need to meet. This paper propelled the recommendation that it is unrealistic to request that any one checking plan fulfill these necessities all the while, that will be, that "the stamping issue," as here and there portrayed in the writing, is over indicated. That does not, obviously, imply that specific stamping issues are insoluble. Both chronicled point of reference and late development furnish us with a wide scope of apparatuses, which whenever connected brilliantly ought to be adequate to tackle a large portion of the issues that this paper meet by and by.



* + - 1. (b)



(c) (d)

### Fig 2.2. : When applied to images, the distortions introduced by StirMark are almost unnoticeable. “Lena” (a) before and (b) after StirMark with default parameters. (c), (d) For comparison, the same distortions have been applied to a grid.

**[Nima Khademi Kalantari, et-al, 2010]** In this paper, a novel course of action for quantizer levels in the Quantization Index Modulation (QIM) technique is proposed. Because of perceptual favorable circumstances of logarithmic quantization, and so as to tackle the issues of a past logarithmic quantization based technique, we utilized the pressure capacity of µ-Law standard for quantization. In such manner, the host sign is first changed into the logarithmic area utilizing the µ - Law pressure work. At that point, the changed information is quantized consistently and the outcome is changed back to the first area utilizing the backwards work. The scalar strategy is then stretched out to vector quantization. For this, the greatness of each host vector is quantized on the outside of hyper circles which pursue logarithmic radii. Ideal parameter µ for both scalar and vector cases is determined by the host signal circulation. Also, incorporation of a mystery key in the proposed strategy, like the vacillate balance in QIM, is presented. Execution of the proposed strategy in the two cases is investigated and the systematic deductions are checked through broad reproductions on counterfeit sign. The strategy is additionally reproduced on genuine pictures and its presentation is contrasted and past scalar and vector quantization-based strategies. Results demonstrate that this strategy highlights more grounded a watermark in examination with ordinary

QIM and, subsequently, has better execution while it doesn't experience the ill effects of the disadvantages of a recently proposed logarithmic quantization calculation.

**[Giulia Boato, et-al, 2009]** This paper exhibits a novel and adaptable benchmarking device dependent on genetic calculations (GA) and intended to evaluate the vigor of any advanced picture watermarking framework. The fundamental thought is to assess vigor as far as perceptual quality, estimated by weighted pinnacle signal-to-clamor proportion. Through a stochastic methodology, we advance this quality measurement, by finding the negligible corruption that should be presented in a stamped picture so as to expel the inserted watermark. Given a lot of assaults, picked by the thought about application situation, GA bolster the improvement of the parameters to be allocated to each preparing task, so as to acquire a plain picture with perceptual quality as high as could be expected under the circumstances. Broad trial results exhibit the adequacy of the proposed assessment apparatus. This paper shows an inventive benchmarking device to assess the strength of any advanced watermarking system considering the nature of the plain pictures as far as saw quality. Subsequently, another measurement dependent on WPSNR is presented. The objective is to expel the watermark from a substance while augmenting perceptual quality. In this way, given a lot of assaults, creators search for a parameterization ready to evacuate the watermark, upgrading the WPSNR of the plain picture. This nonlinear advancement issue is bolstered by GA. The viability of the present apparatus has been exhibited by broad reenactments calling attention to the shortcomings of two surely understood strategies. Creators likewise bring up that with the proposed apparatus, it is conceivable to reasonably think about two diverse watermarking calculations playing out a similar sort of watermark recuperation (to be specific, either both discovery and both translating).

**[A. V. Subramanyam, et-al, 2012]** Digital Asset Management Systems (DAMS) by and large handlemedia information in a packed and scrambled structure. It is some of the time important to watermark these packed encoded media things in the compacted scrambled space itself for alter location or proprietorship presentation or copyright the executives purposes. It is a test to watermark these compacted scrambled streams as the pressure procedure would have stuffed the data of crude media into a low number of bits and encryption would have randomized the packed piece stream. Endeavoring to watermark such a randomized piece stream can cause an emotional corruption of the media quality. In this manner it is important to pick an encryption plot that is

both secure and will permit watermarking in an anticipated way in the compacted scrambled area. In this paper, we propose a vigorous watermarking calculation to watermark JPEG2000 packed and scrambled pictures. The encryption calculation we propose to utilize is a stream figure. While the proposed strategy installs watermark in the packed scrambled space, the extraction of watermark should be possible in the decoded area. We examine in detail the installing limit, vigor, perceptual quality and security of the proposed calculation, utilizing these watermarking plans: Spread Spectrum (SS), Scalar Costa Scheme Quantization Index Modulation (SCS-QIM), and Rational Dither Modulation (RDM).

**[Saraju P. Mohanty, et-al, 2005]** Watermarking is the procedure that inserts information called a watermark, a tag, or a name into an interactive media object, for example, pictures, video, or content, for their copyright insurance. As indicated by human discernment, the computerized watermarks can either be noticeable or undetectable. An obvious watermark is an auxiliary translucent picture overlaid into the essential picture and seems unmistakable to a watcher on a cautious investigation. The imperceptible watermark is installed so that the alterations made to the pixel esteem is perceptually not seen, and it very well may be recuperated distinctly with a suitable translating instrument. This paper shows another Very Large Scale Integration (VLSI) engineering for actualizing two unmistakable advanced picture watermarking plans. The proposed engineering is intended to go for simple incorporation into any current advanced camera system. To the creators' learning, this is the first VLSI design for actualizing noticeable watermarking plans. A model chip comprising of 28 469 doors is actualized utilizing 0.35-m innovation, which devours 6.9-mW control while working at 292 MHz.

**[Nima Khademi Kalantari, et-al, 2009]** This paper displays a Multiplicative Patchwork Method (MPM) for sound watermarking. The watermark sign is inserted by choosing two subsets of the host sign highlights and adjusting one subset multiplicatively with respect to the watermark information, though another subset is left unaltered. The technique is actualized in wavelet area and estimation coefficients are utilized to install information. So as to have a mistake free location, the watermark information is embedded uniquely in the edges where the proportion of the vitality of subsets is between two predefined values. Additionally so as to control the imperceptibility of watermark inclusion, we utilize an iterative calculation to achieve an ideal quality for the watermarked sound sign. The nature of watermarked sign is assessed in every cycle utilizing

Perceptual Evaluation of Audio Quality (PEAQ) strategy. The likelihood of blunder is likewise determined for the watermarking plan and recreation results demonstrate the legitimacy of the diagnostic deductions. Recreation results demonstrate that MPM is hearty against different basic assaults, for example, commotion expansion, sifting, reverberation, MP3 pressure, and so on. In contrast with the first interwoven technique and its changed variants, and some ongoing strategies, MPM gives more heartiness and indiscernibleness of the watermark inclusion.

**[R. Reyes, et-al, 2010]** This paper shows an open video watermarking calculation, whose power relies upon the installing vitality, which must be constrained because of the debasement of video arrangement brought about by a similar watermark signal. The proposed calculation implants a perceptually unmistakable double example, for example, proprietor's logotype. Initially the video groupings are portioned by every scene, and after that the parallel watermark example is implanted into Discrete Wavelet Transform (DWT) area of the haphazardly chosen scene squares. To expand the security of the proposed plan, the biary watermark example is mapped to a clamor like twofold example utilizing a disorderly blending strategy, before its implanting. Reenactment results demonstrate the watermark impalpability and power against a few assaults, for example, clamor pollution, outline dropping, outline averaging and casing swapping; the assessment results likewise demonstrate that the removed watermark example is adequately clear, in spite of the fact that the watermarked video grouping may endured a few assaults.

**[Chuntao Wang, et-al, 2012]** Accomplishing power, indistinctness and high limit at the same time is vital in computerized watermarking. This paper shows another educated picture watermarking plan with high heartiness and rearranged unpredictability at a data rate of 1/64 bit/pixel. Right off the bat, a Taylor Series Approximated Locally Optimum Test (TLOT) finder dependent on the Hidden Markov Model (HMM) in the wavelet space is created to handle the issue of inaccessibility of accurate implanting quality in the beneficiary because of educated inserting. At that point dependent on the TLOT indicator and the idea of grimy paper code structure, new HMM-based round codes are built to give a powerful tradeoff among strength and twisting. The procedure of educated installing is planned as an advancement issue under the vigor and mutilation requirements and the Genetic Algorithm (GA) is then utilized to take care of this issue. Additionally, the perceptual separation in the wavelet area is likewise formed and joined

into the GA-based streamlining. Reenactment results exhibit that the proposed educated watermarking calculation has high vigor against normal assaults in sign handling and demonstrates an equivalent execution to the cutting edge plot with an extraordinarily decreased number-crunching multifaceted nature.

#### Issue 2: Payload of the Watermark

The application is based on the data storage in watermarking technique and it’s sufficient also confirmed by its technique. This is observed from several literature reviews that there are requirement of twenty bits per second an audio based watermarking system and this is the minimum requirement [12, 13]. If anyone wants to reserve property rights like ISBN or ISRC, then should go for copy right which makes work more secure and confidential [14]. There are possibilities to secure of any data as audio or/and video with embedded system using proper watermarking technology. This is depends upon the data needed in unit scheme and it is also expanded in multiple spreading data and segments. So basically, the range of embedded data is spread and enhanced by the payload technique of watermarking. Similarly the digital and video dat is also may be speeded by proper using of watermarking technology.

**[Joseph \_O Ruanaidh, et-al, 1999]** This paper displays another methodology for the safe and strong copyright insurance of advanced pictures. It depicts a framework for producing advanced watermarks and for exchanging watermarked pictures. The framework depends on another watermarking strategy, which is strong against picture change methods, for example, pressure, pivot, interpretation, scaling and editing. It utilizes tweak of the greatness segments in Fourier space to implant a watermark and a going with layout and, during watermark extraction, peruses a format in the log polar change of the recurrence area. The format is utilized for examining scaling and revolution endured by the watermarked stego-picture. The location of the watermarks is additionally conceivable with no requirement for the first spread picture. What's more, the framework applies unbalanced cryptographic conventions for various purposes, to be specific embedding=detecting the watermark and moving watermarked information. The open key method is connected for the development of a single direction watermark inserting and the confirmation capacity to distinguish and demonstrate the uniqueness of the watermark. Lawful contest goals is bolstered for the various watermarking of an advanced picture without uncovering the private keying data.

**[Xinge You, et-al, 2010]** As a successful strategy for copyright insurance of computerized items against illicit use, watermarking in wavelet area has as of late gotten significant consideration because of the attractive multiresolution property of wavelet change. All in all, pictures can be spoken to with various goals by the wavelet decay, closely resembling the Human Visual Framework (HVS). Typically, human eyes are unfeeling toward picture singularities uncovered by various high recurrence subbands of wavelet decayed pictures. Thus, including watermarks into these singularities will improve the intangibility that is an ideal property of a watermarking plan. That is, the capacity for uncovering singularities of pictures assumes a key job in planning wavelet-based watermarking calculations. Shockingly, the current wavelets have a constrained capacity in uncovering singularities in various bearings. This spurs us to build new wavelet channel banks that can uncover singularities every which way. This paper use unique symmetric networks to develop the new nontensor item wavelet channel banks, which can catch the singularities every which way. Observational examinations will demonstrate their points of interest of uncovering singularities in correlation with the current wavelets. In light of these new wavelet channel banks, creators propose an altered critical contrast watermarking calculation. Exploratory outcomes demonstrate its promising outcomes.

**[Chip-Hong Chang, et-al, 2010]** Most VLSI watermarking methods don't permit various authorships of different Intellectual Property (IP) centers to be distinguished legitimately in the field after the IPs have been coordinated, created and bundled into chip. Watermark embedded at the Design-for-Testability (DfT) organize makes its immediate recognition after chip bundling conceivable, yet it ensures just the downstream situation and-directing plan, and is defenseless against expulsion assault as the test rationale is free of the practical rationale. This paper propose a freely distinguishable watermarking plan to overcome any issues between IP insurance and IP the executives. The structure is watermarked by methods for Synthesis-for-Testability (SfT), where the test and utilitarian rationales of the IP are consolidated and combined without utilizing searchable flip-flops. Watermarked imperatives are forced on the output chain requesting issue in the SfT procedure with the goal that responsibility for inserted IP can be openly distinguished by legal IP suppliers, purchasers and buyers by infusing a particular test vector in the field. The overhead because of the watermark inclusion is limited by a closest neighbor look calculation for flip-flop reordering. As the output capacity is a fundamental piece of the structure in the

combination procedure of the IP creation, the watermark is more diligently to be expelled in respect to other sweep chain watermarking plans whose test circuits are consistently autonomous of the IP usefulness. To discourage and follow IP falseness by the licensees, a provable instrument is proposed to empower numerous authorships of various IP centers in a solitary chip to be openly verified in the field. Examinations performed with ISCAS89 and LGSyn93 benchmark circuits demonstrate that the proposed watermarked plans have low structure overheads, and the probabilities of happenstance and evacuation diminish quickly with expanded watermark and sweep chain length.

**[Pei-Yu Lin, et-al, 2009]** This paper presents a unique dual watermarking mechanism for digital media that implants an identifiable pattern into the spatial domain and an invisible logo into the frequency domain. Certainly, visible watermarking is vital for shielding online resources from unlawful reproduction. Due to the perceptibility of embedded patterns, though, watermarked digital media are weak to the in painting attack and shared signal processing operations. Using hybrid strategies, simulation results display that the novel method can repel these attacks. In specific, the new mechanism permits lawful subscribers to restore an unmarked image, whereas other dual watermarking schemes do not. This feature brands it appropriate for protecting artistic and valuable media.

**[Pei-Ju Chiang, et-al, 2011]** Printer recognizable proof dependent on printed archives can give criminological data to ensure copyright and confirm legitimacy. Notwithstanding characteristic highlights (inherent marks) of the printer, balancing the printing procedure to implant explicit highlights (extraneous marks) will further broaden the encoding limit and deciphering exactness. One of the key issues with inserting outward marks is that the implanting ought not debase the picture quality, yet should be discernible by a recognition calculation.

In this paper, we will exhibit the plausibility of installing code successions in electrophotographic halftone pictures by regulating dab measure through laser power balance. Creators created comparing inserting and discovery calculations to implant and concentrate data. Exploratory outcomes demonstrate that utilizing a 600 dpi local goals printer's default halftone calculation, we can encode 5 bits of data in each 310 printer check lines or roughly every 0.5 inches

**[Min-Jeong Lee, et-al, 2010]** Numerous unlawful duplicates of computerized video creations for film discharge can be found on the Internet before their official discharge. During the illicit replicating of film, composite geometric mutilations generally happen because of the point of the camcorder in respect to the screen. We propose a novel video watermarking dependent on spread range way that fulfills the necessities for securing advanced film. It empowers the identifier to separate the implanted message as well as gauge the position where the camcorder recording is made. It is certain that the proposed Position Estimating Model (PEM) can pass judgment on the seat in a performance center with a Mean Absolute Error (MAE) of (33.84, 9.53, 50.38) cm. Exploratory outcomes utilizing different kinds of movies demonstrate that the introduced technique gives the scientific model to recognizing and researching the position of the pirate.

**[Luiz Octavio Massato Kobayashi, et-al, 2009]** The growing adoption of information structures in healthcare has directed to a situation where patient statistics safekeeping is more and more being observed as a critical issue. Allowing patient information to be in danger may lead to irreversible damage, physically, morally, and socially to the patient, potentially trembling the trustworthiness of the healthcare institution. Medicinal images play a crucial role in such context, given their importance in diagnosis, treatment, and research. Therefore, it is vital to take measures in order to prevent tampering and determine their provenance. This stresses implementation of security mechanisms to guarantee information integrity and authenticity. There are a plenty of works done in this field, based on two major approaches: use of metadata and use of watermarking. Though, there still are restrictions for both approaches that must be properly addressed. This paper presents a novel method using cryptographic means to advance trustworthiness of medical images, providing a stronger link between the image and the information on its integrity and authenticity, without negotiating image quality to the end user. Use of Digital Imaging and Communications in Medicine structures is also an advantage for ease of development and deployment.

**[Yu-Hsun Lin, et-al, 2011]** The content protection for picture based 3D information is getting more significance with the development of minimal effort 3D show gadgets. The Depth-Image- Based Rendering (DIBR) 3D picture is one of the picture based 3D information which comprises of the middle picture and the profundity picture created by the substance supplier. The left-eye picture and the right-eye picture are rendered from the middle picture and the profundity picture

at the substance buyer side. The visually impaired watermarking for DIBR 3D picture is infrequently contemplated in the writing. In this paper, a novel visually impaired various watermarking plan is proposed to manage the substance security issue of DIBR 3D pictures. Other than the standard prerequisite of common symmetry among reference designs for various watermark implanting, we found that appropriate installing request plays a considerably increasingly significant job in watermarking the DIBR 3D pictures. Exploratory outcomes demonstrate that the proposed plan is powerful against the JPEG pressure and clamor including assaults. All the more strikingly, it is discovered that the proposed watermarking can likewise endure enormous range varieties of the profundity picture during rendering.

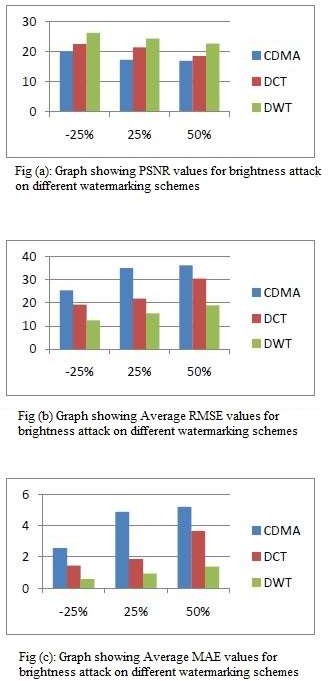
#### Issue 3: Robustness

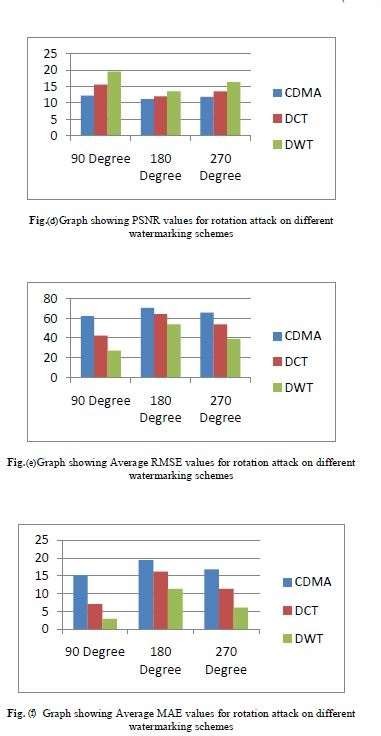
The watermarking technology must have the property of robustness of its original data and similarly other stored data. It can be modify and with its proper way and not be degraded by some other means such as copy rights, property rights, etc. It may be not a loose and false informatics according to the user applications such as digital-analog information’s, analog-digital information or any other forms and its conversion and changeable modes and operation. Only the watermark user may have to rights it’s changeable and other embedded uses and applications. [15]. It is also have the property rights to remove any data or information and knowing about the removed watermark data and sources. The removed data is so as that these may be unusable and not to embedded in other form in any type of work.

**[Jia-Shiang Chen, et-al, 2011]** This study employed the optical reactions of occasional structures, various variable capacities with adequate multifaceted nature, to build up a cryptographic plan. The attributes of structures could be conveyed effectively with the ciphertext, a progression of numbers containing plaintext messages. Two streamlining techniques using a hereditary calculation were received to create the occasional structure profile as a basic encryption/unscrambling key. The strength of strategies was additionally affirmed under different points of confinement. The ciphertext must be unscrambled by alluding to the codebook in the wake of gaining the pre-decided optical reaction. The secrecy and huge limit of the plan uncovered the improved coding techniques here while the accomplishment of the plan was exhibited with the conveyance of a precedent message. An optical cryptographic plan using the optical reactions of intermittent structures for plaintext message was created by this examination. The encryption

and unscrambling steps were partitioned into stages and clarified utilizing a false situation. The upsides of this plan incorporate its high level of productivity, vigorous age of keys, huge limit, and high level of adaptability. Two improvement strategies advantage the inquiry proficiency of agreeable structure measurements and their power was exhibited under different breaking points. Such power really offers the likelihood for numerous clients inside plan which are separated by their marks. The work of sham writings and numerous wavelengths further guarantees the extraordinary adaptability of the plan. Contrasted with most known plans, the capacity of proposed plans to oppose assault turns out to be a lot more grounded at little expense. We trust that the progression of the created cryptographic plan guarantees the security of data, extends the utilization of optics, and gives an effective route in seeking intermittent structures utilizing wanted optical reactions.

**[Harsh K Verma, et-al, 2009]** The ongoing appearance in the field of interactive media proposed a numerous offices in transport, transmission and control of information. Alongside this headway of offices there are bigger dangers in validation of information, its authorized use and security against unlawful utilization of information. A great deal of computerized picture watermarking strategies have been planned and actualized to stop the unlawful utilization of the advanced mixed media pictures. This paper looks at the strength of three diverse watermarking plans against brilliance and turn assaults. The strength of the watermarked pictures has been confirmed on the parameters of PSNR (Peak Signal to Noise Ratio), RMSE (Root Mean Square Error) and MAE (Mean Absolute Error). This paper centers around the power of the watermarking systems browsed all the three spaces of watermarking against splendor and revolution assault. The key finish of the paper is that the Wavelet space watermarking procedure is the best and most hearty plan for the watermarking of computerized sight and sound pictures. This work could further be stretched out to the watermarking motivation behind another advanced substance like sound and video.





### Fig 2.3: (a,b,c,) : Result of Brightness Attack, (d,e,f) : Result of Rotation Attack

**[Sebastiano Battiato, et-al, 2000]** This paper shows a novel watermarking plan to sum up a past proposition by similar creators. In this paper to watermark the picture adds up to process the hues in the image as focuses in the Color Opponency space and to balance every single one of them by an irregular vector. As an additional imperative, so as to keep away from picture quality corruption, the balance connected ought to be to such an extent that a shading isn't moved outside of a little circle. The watermarking calculation forms the hues in the image as focuses in the Color Opponency space and balances every single one of them, inside an appropriate imperceptive zone, by an irregular vector. To improve power we propose to parcel the entire

pixels populace into "shading sets": each set assembles pixels with a similar shading. Each shading set, surpassing a given cardinality, is thus haphazardly parceled into three subsets. Every last one of these subsets is subsequently controlled in various reasonable ways. The watermark is acquired keeping up a record of the factual appropriation of the three subsets. Thorough hypothetical measurable examination demonstrates that this methodology is powerful as for the most widely recognized tasks of picture preparing.

**[Maha Sharkas, et-al, 2007]** Image watermarking has turned into a significant device for licensed innovation assurance and verification. In this paper a watermarking strategy is proposed that fuses two watermarks in a host picture for improved insurance and strength. A watermark, in type of a PN succession (will be known as the optional watermark), is implanted in the wavelet space of an essential watermark before being installed in the host picture. The method has been tried utilizing Lena picture as a host and the camera man as the essential watermark. The implanted PN arrangement was noticeable through relationship among other five successions where a PSNR of 44.1065 dB was estimated. Besides, to test the strength of the strategy, the watermarked picture was presented to four kinds of assaults, to be specific pressure, low pass sifting, salt and pepper clamor and luminance change. In all cases the auxiliary watermark was anything but difficult to identify notwithstanding when the essential one is seriously contorted.

**[Jen-Sheng Tsai, et-al, 2011]** A novel feature region selection method for robust digital image watermarking is watermarking is proposed in this paper. This strategy plans to choose a no overlapping highlight district set, which has the best heartiness against different assaults and can safeguard picture quality however much as could be expected after watermarked. It initially plays out a reproduced assaulting method utilizing some predefined assaults to assess the power of each competitor include district. As indicated by the assessment results, it at that point receives a track- with-pruning methodology to look through an insignificant essential list of capabilities which can oppose the most predefined assaults. So as to upgrade its protection from unclear assaults under the requirement of safeguarding picture quality, the essential list of capabilities is then stretched out by including into some assistant element areas. This work is planned as a multidimensional backpack issue and comprehended by a hereditary calculation based methodology. The trial results for StirMark assaults on some benchmark pictures bolster our desire that the essential list of capabilities can oppose all the predefined assaults and its augmentation can improve the power

against vague assaults. Contrasting and some notable component based strategies, the proposed technique displays better execution in hearty advanced watermarking.

**[Kwangtaek Kim, et-al, 2010]** This paper shows a strategy to improve watermark heartiness by misusing the concealing impact of surface harshness on watermark perceivability. Its thought is to adjust watermark solidarity to neighborhood surface unpleasantness dependent on the information that human eyes are less delicate to changes on a rougher surface fix than those on a smoother surface. So as to evaluate human affectability to surface harshness of polygonal lattices, we led a thorough psychovisual analysis to get human watermark discovery edges as an element of surface unpleasantness. The outcomes can be utilized to adaptively choose watermark quality as indicated by nearby surface harshness during the watermark implanting process. To test the thought, creators connected it to the adjusted forms of two prominent 3-D watermarking techniques, one proposed by Benedens and one by Cayre and Macq. Test results demonstrated that this methodology improves watermark power when contrasted with the first calculations. Further investigations demonstrated that the normal watermark quality permitted by this unpleasantness versatile technique was bigger than that by the first Benedens' and Cayre and Macq's strategies while guaranteeing watermark impalpability. This was the fundamental explanation behind the improved strength saw in our analyses. Along these lines paper presume that abusing the concealing property of human vision is a suitable method to improve the vigor of 3-D watermarks, and can conceivably be connected to other 3-D computerized watermarking systems.

**[Fabrizio Guerrini, et-al, 2011]** High Dynamic Range (HDR) pictures speak to the future arrangement for advanced pictures since they permit exact rendering of a more extensive scope of luminance esteems. Notwithstanding, today extraordinary sorts of preprocessing, all things considered known as Tone-Mapping (TM) administrators, are expected to adjust HDR pictures to right now existing showcases. Tone-Mapped pictures, in spite of the fact that of decreased powerful range, have in any case high caliber and henceforth hold some business esteem. In this paper, we propose an answer for the issue of HDR picture watermarking, e.g., for copyright inserting, that ought to endure TM. Along these lines, the necessities forced on the watermark include subtlety, a specific level of security, and power to TM administrators. The proposed watermarking framework has a place with the visually impaired, recognizable class; it depends on

the Quantization Index Modulation (QIM) worldview and utilizes higher request measurements as an element. Trial investigation indicates positive outcomes and shows the framework viability withcurrent condition of-craftsmanship TM calculations.

**[Xiang-Yang Wang, et-al, 2009]** The vast majority of the past sound watermarking plans are strong to regular sign handling assaults, however show serious issues when looked with de- synchronization assaults. To take care of the issues related with these methodologies (see the ''Related Work'' sidebar for more subtleties), this paper propose a sound watermarking plan dependent on Support-Vector-Machine (SVM) hypothesis to secure against de-synchronization assaults by utilizing sound insights characteristics3 and a synchronization code procedure. Test results with SVM demonstrate that our proposed plan is indistinct, hearty against basic sign handling, and vigorous against de-synchronization tackles among the different issues to be unraveled in advanced sound watermarking, creating strength against de-synchronization assaults is a standout amongst the most testing. De-synchronization assaults that reason relocation among inserting and recognition after some time make it hard for a watermark to endure. A disadvantage of this sound watermarking strategy is that it has a lower intangibility of the entire sound watermark framework. Future research work will address this issue by, as per content examination of music, choosing progressively stable element vectors for SVM preparing to improve the impalpability of the entire sound watermark framework.

**[Chih-Chin Lai, et-al, 2010]** The primary goal of building up a picture watermarking system is to fulfill both impalpability and power prerequisites. To accomplish this goal, a crossover picture watermarking plan dependent on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) is proposed in this paper. In this methodology, the watermark isn't installed legitimately on the wavelet coefficients yet rather than on the components of solitary estimations of the spread picture's DWT subbands. Exploratory outcomes are given to represent that the proposed methodology can withstand an assortment of picture handling assaults.

**[Federica Battisti, et-al, 2011]** Low-cost personal computers, wireless access technologies, the Internet, and computer-equipped classrooms permit the plan of novel and correlative systems for showing computerized data security in electrical designing educational module. The difficulties of the current advanced data time require specialists who are adequately ready to balance theft,

fraud, copyright encroachment, etc. Computerized watermarking is one conceivable system for battling robbery, which comprises of the addition of undetectable however powerful data to secure the information. In this paper, another showing approach, intended for testing understudy aptitudes and advancing in mixed media information assurance, is displayed. This comprises of a circulated security game where understudies contend by first utilizing the created watermarking strategies and after that assaulting each other's techniques, along these lines checking their power. Gatherings of understudies from various colleges and nations play against one another, endeavoring to bargain other groups' concealing frameworks while shielding their very own information from assaults. The proposed technique can be considered as an engaging methodology for animating learning, collaboration, and group rivalry. The viability of the encouraging strategy is checked by an understudy study and their scholastic outcomes.

**[Pik Wah Chan, et-al, 2005]** We have seen a blast of information exchange in the Internet and the broad utilization of computerized media. So, advanced information proprietors can rapidly and enormously move mixed media reports over the Internet. This prompts wide enthusiasm for mixed media security and interactive media copyright insurance. We propose a novel cross breed computerized video watermarking plan dependent on the scene change examination and blunder revision code. Our video watermarking calculation is powerful against the assaults of casing dropping, averaging and measurable examination, which were not comprehended adequately before. We begin with a total review of momentum watermarking advances, and saw that none of the current plans is fit for opposing all assaults. As needs be, we propose installing various pieces of a solitary watermark into various scenes of a video. We at that point break down the qualities of various watermarking plans, apply a half and half way to deal with structure a super watermarking plan that can oppose the majority of the assaults. To expand the vigor of the plan, the watermark is refined by a blunder revising code, while the rectifying code is installed as a watermark in the sound channel. It enhances the nature of the watermarked video. The adequacy of this plan is confirmed through a progression of examinations, in which various standard picture handling assaults are led, and the power of our methodology is shown utilizing the criteria of the most recent StirMark test.

#### Issue 4: Others

**[Hui-Yu Huang, et-al, 2010]** The increasing popularity of the web implies that advanced mixed media are transmitted all the more quickly and effectively. What's more, individuals are extremely mindful for media proprietorship. In any case, advanced watermarking is a productive and promising intends to secure scholarly properties. In view of the licensed innovation consideration in the data time, how to secure the individual possession is critical and a fundamental plan. In this paper, we propose a powerful video watermarking strategy dependent on a pseudo-3-D Discrete Cosine Transform (DCT) and Quantization Index Modulation (QIM) against a few assaults. The watermark is mostly embedded into the uncompressed area by altering the relationship between's DCT coefficients of the chosen squares, and the watermark extraction is visually impaired. This methodology comprises of a pseudo-3-D DCT, watermark inserting, and extraction. A pseudo-3- D DCT, which is taken DCT change twice, will be first used to ascertain the installing factor and to acquire the valuable messages. Utilizing the QIM, we implant the watermark into the quantization districts from the progressive crude casings in the uncompressed space and record the relative data to make a mystery installing key. This mystery installing key will further apply to extraction. Exploratory outcomes exhibit that the proposed technique can endure separating, compressions, luminance change, and clamor assaults with a decent imperceptibility and vigor.

**[Yu-Ping Wang, et-al, 2009]** In this paper, we propose semifragile watermarking calculation for the validation of 3D models dependent on vital invariants. A watermark picture is installed by adjusting the indispensable invariants of a portion of the vertices. So as to alter the fundamental invariants, the places of a vertex and its neighbors are moved. To separate the watermark, all the vertices are tried for the implanted data, and this data is joined to recoup the watermark picture. The quantity of parts of the watermark picture that can be recouped will decide the confirmation choice. Test tests demonstrate that this strategy is powerful against typical use adjustments presented by unbending changes, design transformations, adjusting blunders, and so forth and can be utilized to test for pernicious assaults, for example, work altering and trimming. An extra commitment of this paper is another calculation for registering two sorts of basic invariants.

**[Xiaotian Xu, et-al, 2009]** A Binned Dirty-Paper Code (DPC) isolates a lot of Codewords into various containers. The Codeword in the canister that has the greatest connection with the side

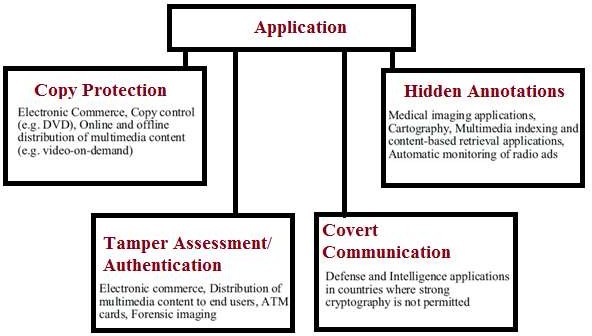
data is chosen as the transmitted filthy paper codeword. This letter determines and checks the scientific Bit-Error Rate (BER) articulation of binned symmetrical square code utilized as DPC in watermarking applications. The BER patterns of such symmetrical DPC under consistent code length or steady code rate obliges are broke down. At last, we propose another class of DPC dependent on binned bi-symmetrical codes and exhibit its BER execution increase over symmetrical DPC.

**[Xiaoyu Feng, et-al, 2011]** The Digital Imaging Technology has developed dangerously for sight and sound applications lately. The requirement for the copyrighted digitalized media winds up critical these days. A methodology for the computerized copyright security is to utilize progressed watermarking systems, where watermarks can uncover the proprietorship characters. As a rule, the watermarks are inserted into picture or video signals. In this paper, we will research advanced watermarking procedures and propose another ideal watermarking plan. At the point when various inserted watermarks are considered, another investigation for the Signal-to-Interference-in addition to Noise-Ratios (SINRs) concerning the subject sign and the watermark sign is completed. The target quality measure for the computerized watermarking applications ought to basically comprise of both sign to-obstruction in addition to commotion proportion for the subject sign and closeness coefficients for the watermarks. So as to advance the previously mentioned target measure, we structure a novel effective scale-factor improvement plot, which can prompt the greatest generally speaking SINR for both subject sign and watermarks. Reproduction results are additionally exhibited to delineate the adequacy of our proposed technique.

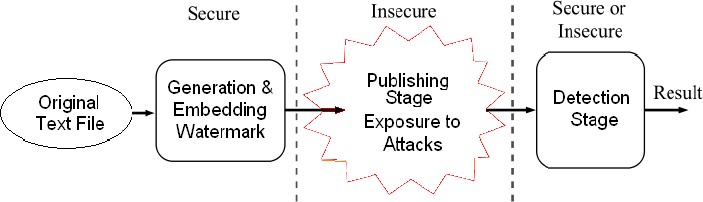
* 1. **Motivations**

This section presented different applications of watermarking and its significance in protection of several data and messages exist in watermarking with condition of security and reliability of data and messages. Many researchers were discussed about the limitations of conventional digital watermarking system and suggested to new technology used in it.

Digital watermarking is suitable for audio-video phenomenon as it has good secured for the original matters and data in digital form with its protection features and conversion of data [8, 9].

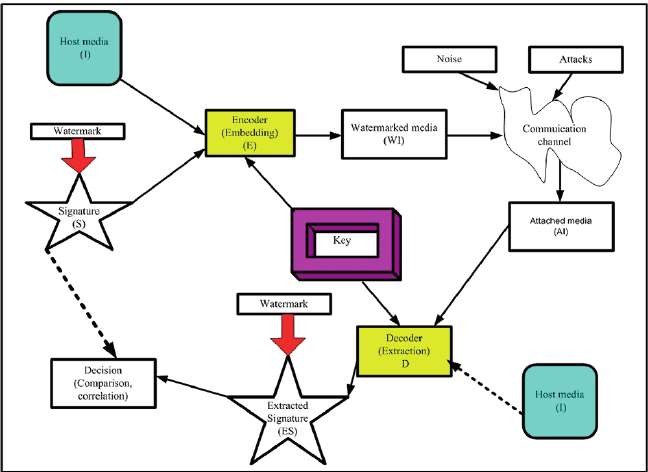


### Figure 2.4: Digital Watermarking Technology Uses [9]



**Figure 2.5: Properties of Digital Watermarking**

The significance of digital watermarking and its various applications are well known as in digital versatile disk (DVD), MP3, MPEG-4, JPEG2000, and the International Federation of the Photographic Industry (IFPI). Truth be told, the Galaxy Group, comprised of Hitachi Ltd., IBM Corp., NEC Corp., Pioneer Electronic Corp., and Sony Corp. has as of late settled upon a video standard for DVD copy assurance. [10].



**Figure 2.6: Functions of Digital watermarking**

## Solution Approaches

* + 1. **Watermark-Object Selection**

The form of embedded system is to be selected so as it is secret and understanding for the owner and respond ate of the original data such as in the image form, data form, text form or any other form. But there are some constraints to represent in this method for the person or any owning person. So it is necessary to robustness and secure for further processing.

The coding which is used for watermarking technology is so that a single error in this embedded change all the meaning of message even for an easy task or any task.

## Insertion Domain

Watermark embedded system consists of video, images, etc. The watermark technique having mainly two categories. One in which modification of images is done directly and other form is related to transformation and its associated coefficients. Both forms are used the embedded sytem for domain of different types of data and messages. [17].

**Spatial Domain Watermarking:** The first technique related to the spatial domain in which directly transformation is done for different messages and data such as data regarding the public domain and shows a simple and straightforward based on the algorithm. So the images remain original at particular location for image consideration and in public domain with security [18-20]. This level of watermarking has two main functions as follows:

* Recovery of watermarking for public domain
* Predictive coding for psycho visual watermark management

**Transfer Domain Watermarking:** This technique of watermarking transforms the images and data with some special transform features including embedded system and transformation coefficients. Then for obtain the digital image, reverse process is applied for particular project and data. This technique has many advantages such as robustness against transformations [21-28]. This technique includes mainly following properties:

* Discrete Fourier Transform
* Discrete Cosine Transform (DCT)
* Mellin-Fourier Transform (DFT)
* Discrete Wavelet Transform
* Spread Spectrum

### Algorithm categorization

Watermarking techniques is divided is also according to the alogorithms exist in domain which contains some basic features such as private, reverse, readable, blindness, etc. in different situations [29]. Main ideas of this concept are following types:

**Blind and Non-Blind:** The watermarking technology as well as algorithm is basically two types as blind and non-blind. A blind watermarking technology not requires the secret and original data and also not requires embedded system. The comparison between original and embedded data is so not required. This data is also known as private procedure and in this type of technique the data is hidden, less robust and disturbing data as comparison to other technique as known as non-blind [30]. On the other hand, a non-blind watermark technique requires original and embedded data and messages with security purpose. This technique is useless and less efficient when used as an algorithm mode as comparison to blind type technique [31, 32]. So there is requirement a suitable technique between two of this techniques and compromises both the advantages and demerits.

**Private and Public:** The other category of watermark technology as defined as private and non- private also known as public. In the private mode all the data are reserve with owner mode and rights of this mode is always associated with single person as well as ownership. In this type of watermark scheme, nobody can access any data in authorized mode. This technique is a part of blind mode and only authorized person can signify the messages and data. In this technique the flow of data is not possible without any permission of private or owner. It is also always related to host person. On the other hand, the public watermarking scheme is used by anyone and it consists of both private and public mode of operation [33]. The internet data uses are type of this type of watermarking scheme and no one shows the name and authorization of data and messages.

**Readable and Detectable**: In the readable mode of watermarking scheme, the data are readable without any prior information and knowing but in the other mode as detectable, it is necessary to knowing the suitable data. In the other mode of operation, the data is only verified with coding which makes it private and provide ownership of data. But in the readable mode of operation, no requirement to verify any type of coding.

**Reversibility and Invertibility**: In the reverse mode of operation, the data can removed from the original location after detection and in the other hand, the invertibility mode the data is not removed from the original location. In this type of watermarking scheme, the data can be gives the false information and not linking with true multimedia. The practical applications in this mode are always persist in wider range.

### Conclusions

The application is based on the data storage in watermarking technique and it’s sufficient also confirmed by its technique. This is observed from several literature reviews that there are requirement of twenty bits per second an audio based watermarking system and this is the minimum requirement [12, 13]. If anyone wants to reserve property rights like ISBN or ISRC, then should go for copy right which makes work more secure and confidential [14]. There are possibilities to secure of any data as audio or/and video with embedded system using proper watermarking technology. This is depends upon the data needed in unit scheme and it is also expanded in multiple spreading data and segments. So basically, the range of embedded data is spread and enhanced by the payload technique of watermarking. Similarly the digital and video dat is also may be speeded by proper using of watermarking technology.

The first technique related to the spatial domain in which directly transformation is done for different messages and data such as data regarding the public domain and shows a simple and straightforward based on the algorithm. So the images remain original at particular location for image consideration and in public domain with security [18-20]. This level of watermarking has two main functions as follows:

* Recovery of watermarking for public domain
* Predictive coding for psycho visual watermark management

To protect digital information at large scale against illegal manipulation, need a suitable technology that facilitate to avoid threats of intellectual property theft and unlawful tampering without any negotiation. The original messages in digital form arises because of information in digitally stored is easily copied rather than analogy.

So the digital watermarking is used for better and it may be comprised of codes and for signal interpretation. Because of special detector used in this technology, different images are drawn by codes [7]. It has following properties:

1. Non-obstructive; it should be unperceivable for host signal.
2. Discreet; not authorized for some mean data and watermark sinking for some places.
3. Extracted; The data must be full of reliability for watermarking signal.
4. Robustness; the watermark must be so that modification is going on easy process of data distortion and for other applications.

# CHAPTER-3

**PROBLEM STATEMENT AND OBJECTIVES**

## OBJECTIVES

The main objectives are as follows:

* + 1. To study several techniques of digital watermarking and suggest an appropriate technique for communicate the secure and reliable data.
    2. To synthesize the importance of proposed work against other techniques.

## ORGANISATION OF THE THESIS

The central idea of the thesis work is to survey the various techniques used for digital watermarking of multimedia images. Based on the studies conducted, the available watermarking techniques are applied to produce a new watermarking method that can work on different formats of color images. The watermarking is done on all the individual planes of the color images and the final watermark is constructed from the intersection of the watermark recovered from all the three planes. The effectiveness of the watermarking schemes is evaluated against Gaussian noise addition and JPEG compression attacks, to show that the recovered final watermark is visually superior and more recognizable in comparison to the one obtained from the individual R-G-B planes or the one obtained from grayscale images with the same test parameters.

**Chapter 1** This chapter gives a brief introduction about information hiding techniques and presents the motivation for performing digital watermarking.

**Chapter 2** This chapter describes methodology to study research paper and how to find issues, solution, and summary of various reference research papers, solution approaches and motivation

**Chapter 3** This chapter discusses problem statement and objectives of the work.

**Chapter 4** This chapter discusses the methodology used for implementing the proposed work.

**Chapter 5** This chapter discusses about watermark embedding and extraction

**Chapter 6** This chapter discusses the experimental results for normal watermark embedding and extraction.

**Chapter 7** This chapter concludes the thesis work with overall result summary and the scope for future work.

## CHAPTER 4

* 1. **Proposed Methodology**

## METHODOLOGY ADOPTED

In this section, needs of digital watermarking and embedded with color images as well as methodology adopted for the same is discussed. In this aspect, the rights of property with intellectual images, color images and multimedia images in different plane are discussed. The different planes of watermarking scheme and other extra schemes are also used for the purpose and methodology favour. Finally, the watermarking with authentification and intersection is also observed and applied to the different color planes with embedded system.

As discussed above, the first technique related to the spatial domain in which directly transformation is done for different messages and data such as data regarding the public domain and shows a simple and straightforward based on the algorithm. So the images remain original at particular location for image consideration and in public domain with security.

This technique of watermarking transforms the images and data with some special transform features including embedded system and transformation coefficients. Then for obtain the digital image, reverse process is applied for particular project and data. This technique has many advantages such as robustness against transformations.

### Watermarking based on threshold correlation

The threshold correlation technique of watermarking scheme consists of embedded system and many properties related to this. In these two techniques of watermarking, working in spatial mode is easy and less robust. In this mode of operation decoding and encoding of data and messages are selected with PN block sequence and then prepare a watermark stage with embedded system. The watermark sequence is to be checked by bit of message as 0 or 1. The procedure is to be repeated and expanded for all stages and then contributes with image of watermarking done.

Then the algorithm related to pseudo-random noise is applied and correlation between noise and watermark is done with computer technique. No check the correlation for threshold value and detection of watermark is available in the exceeding stage. This method is repeated again and again for obtains accuracy of watermark. This is used for multiple bit checking and technology also. Now the correlation factors at mean values of particular block of watermarking scheme with the PN sequence is applied for detection of watermarking.

### To Embed:

* + 1. Generate a PN sequence equal to the size of the block.
    2. Process the image into blocks.
       1. Define a watermarking mask of size equal to the cover image.
       2. For each message bit:
          1. If the bit is ‘0’

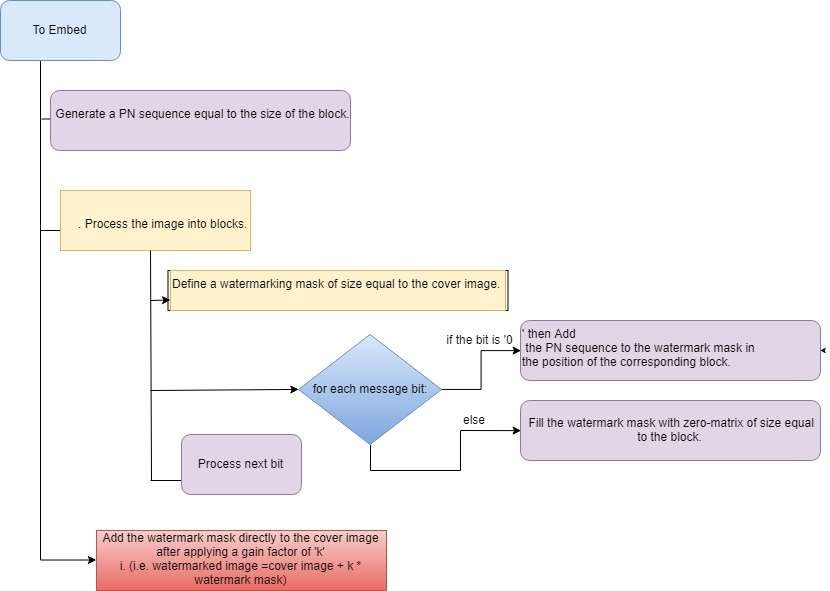
Add the PN sequence to the watermark mask in the position of the corresponding block.

* + - * 1. Else

Fill the watermark mask with zero-matrix of size equal to the

block.

* + - 1. Process next bit.
    1. Add the watermark mask directly to the cover image after applying a gain factor of ‘k’.
       1. (i.e. watermarked image = cover image + k \* watermark mask)



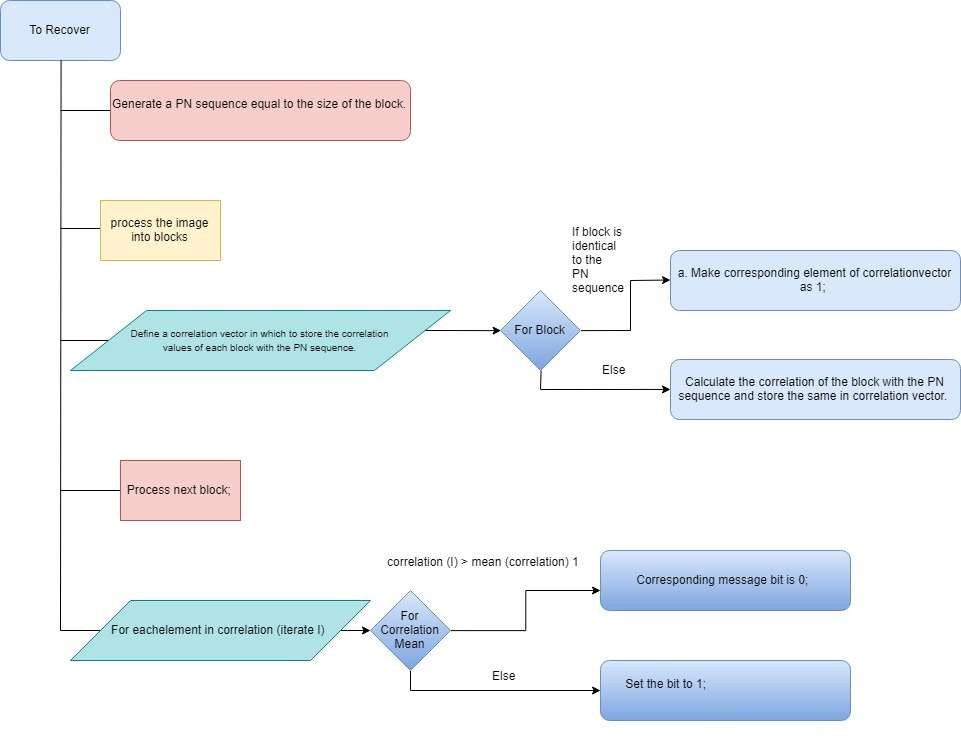
### Figure 4.1: To embed digital watermarking based on threshold correlation

**To Recover:**

1. Generate a PN sequence equal to the size of the block.
2. Process the image into blocks.
3. Define a correlation vector in which to store the correlation values of each block with the PN sequence.
   1. Now for each block
      1. If block is identical to the PN sequence a. Make corresponding element of correlation vector as 1;
      2. Else

a. Calculate the correlation of the block with the PN sequence and store the same in correlation vector.

1. Process next block;
2. For each element in correlation (iterate I)
   1. If correlation (I) > mean (correlation)
      1. Corresponding message bit is 0;
   2. Else
      1. Set the bit to 1;



### Figure 4.2: To recover digital watermarked image based on threshold correlation

* 1. **DCT based watermarking:**

The frequency of image which is used in watermarking is generally complex and to make it easy, the technology used for this frequency into different frequency range. This technology is known as DCT based watermarking scheme. This technology is related to the Fourier Transform in which the data is working in spatial mode of operation.

### DCT encoding:

The basic operation of DCT is given by:

1. The input image is N by M.
2. F (x, y) is the intensity of the pixel in row x and column y.
3. C (u, v) is the DCT coefficient in row u1 and column u2 of the DCT matrix.
4. For most images, much of the signal energy lies at lower frequencies; these appear in the upper left corner of the DCT.
5. Compression is achieved since the lower right values represent higher frequencies and are often small enough to be neglected with little visible distortion.
6. The input is an N x M matrix (image) and the output is the DCT matrix of same dimension.

### Computing the 2D DCT

The 2D DCT is computed by using the direct matlab function “dct2”.A pseudo code is as follows: dct\_image = dct2 (input\_image);

Comparison of mid-band DCT coefficients:

The DCT image technique based on mid band coefficients is one of the type of watermarking in which the conversion is made about 0 or 1 for particular watermarking scheme. Then different type of images is to be divided into some blocks and then each block is choosing for watermarking scheme with definite pixels of embedding. This data in the form of digitally as 0 or 1 remains constant for whole process of embedding. The robustness of technology is achieved by changing the pixels of data of watermarking scheme. This is constraint that no visualise of images is present in this technology.

The algorithm of the above method is given below:

### To embed the watermark:

1. Process the image in blocks.
2. For each block
   1. Transform block using DCT.
   2. if message\_bit is 0.

1. if dct\_block (5,2) < (4,3) .

* + 1. Swap them.
  1. Else

1. If (5,2) > (4,3)

* + 1. Swap them. iv. If (5,2) - (4,3) < k

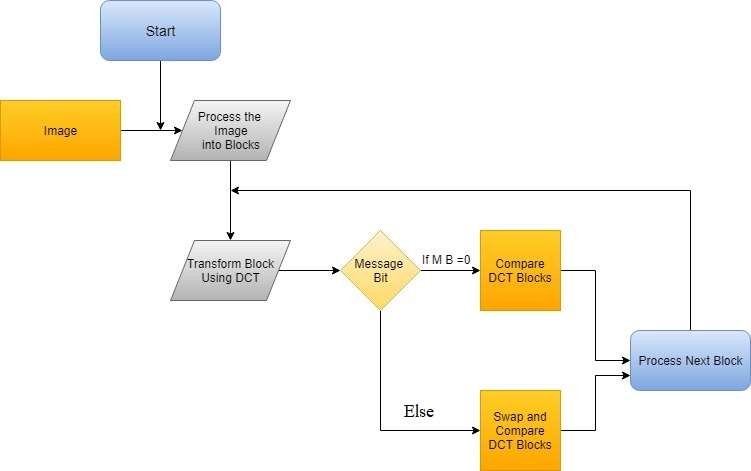
1. (5,2) = (5,2) + k/2;

2. (4,3) = (4,3) – k/2;

v. Else

1. (5,2) = (5,2) - k/2;

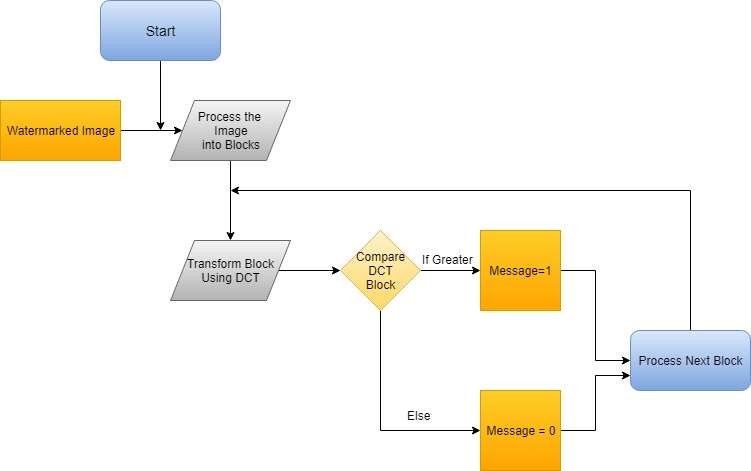
2. (4,3) = (4,3) + k/2;

1. Move to next block.

### Figure 4.3: To embed DCT based digital watermarking

**To recover the watermark:**

1. Process the image in blocks.
2. For each block
   1. Transform block using DCT. ii. If (5,2) > (4,3)
      1. Message = 1;
3. Else
   1. Message=0;
4. Process next block.



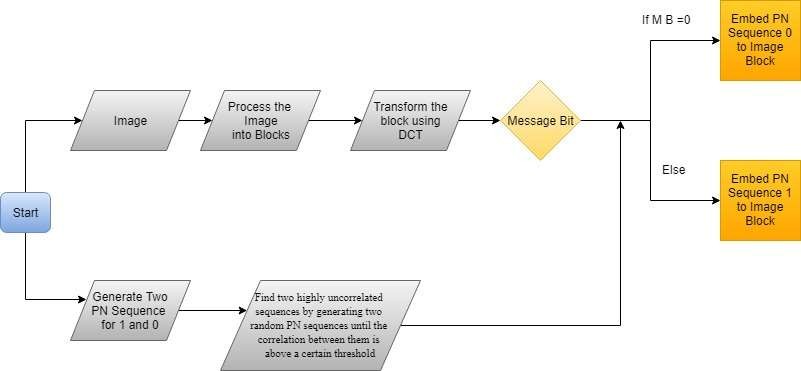
### Figure 4.4: To recover DCT based digital watermarked image

* 1. **Correlation based DCT watermarking:**

To enable the middle range frequency of embedded system of a PN sequence, this technology is used for particular block. In this technology, two uncorrelated data of different PN sequence is exist in the watermarking scheme as embedded into the images. This process is completed by the divide the images into many blocks and then it precede for each block working. The size of block is so that the entire messages can be built into this block and store respective image of embedded in watermarking scheme. Then it is proceeding for different computational techniques and different messages in form of 0 or 1 are generated. Then it is compared with PN sequence and other PN sequence for improvement the correlation of watermarking technology. The algorithm for the above method is given below:

### To embed:

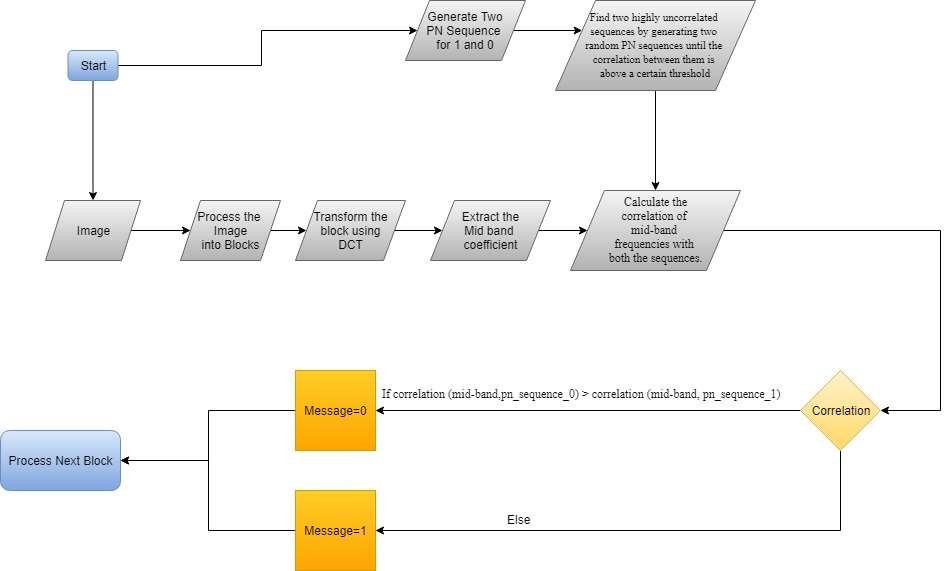
* + 1. Generate two “PN” sequences for 1 and 0.
    2. Find two highly uncorrelated sequences by generating two random PN sequences until the correlation between them is above a certain threshold.
    3. For each image block
       1. Transform the block using DCT.
       2. If message\_bit is 0 1. Embed pn\_sequence\_0 to the image block.
       3. Else1. Embed pn\_sequence\_1 to the image block.
       4. Take the inverse DCT
    4. Move to next block.



### Figure 4.5: To embed correlation based DCT digital watermarking

**To recover:**

1. Generate two “PN” sequences for 1 and 0.
2. Find two highly uncorrelated sequences
3. Process the image in blocks.
4. For each block
   1. Transform block using DCT.
   2. Extract the mid-band coefficients.
   3. Calculate the correlation of mid-band frequencies with both the sequences.
      1. If correlation (mid-band, pn\_sequence\_0) > correlation (mid-band, pn\_sequence\_1)
         1. Message=0;
      2. Else
         1. Message =1;
   4. Process next block.



### Figure 4.6: To recover correlation based DCT digital watermarked image

* 1. **Conclusions**

In this methodology of image processing, MATLAB 7.1 is used for coding which consists of many computational programming with data embedded in watermarking scheme.

The threshold correlation technique of watermarking scheme consists of embedded system and many properties related to this. In these two techniques of watermarking, working in spatial mode is easy and less robust. In this mode of operation decoding and encoding of data and messages are selected with PN block sequence and then prepare a watermark stage with embedded system. The watermark sequence is to be checked by bit of message as 0 or 1. The procedure is to be repeated and expanded for all stages and then contributes with image of watermarking done.

## CHAPTER 5

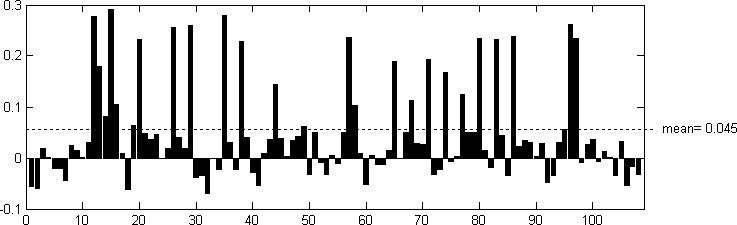
**WATERMARK EMBEDDING AND EXTRACTION**

## Threshold Based Correlation Watermarking

The threshold correlation technique of watermarking scheme consists of embedded system and many properties related to this. In these two techniques of watermarking, working in spatial mode is easy and less robust. In this mode of operation decoding and encoding of data and messages are selected with PN block sequence and then prepare a watermark stage with embedded system. The watermark sequence is to be checked by bit of message as 0 or 1. The procedure is to be repeated and expanded for all stages and then contributes with image of watermarking done.

Then the algorithm related to pseudo-random noise is applied and correlation between noise and watermark is done with computer technique. No check the correlation for threshold value and detection of watermark is available in the exceeding stage. This method is repeated again and again for obtains accuracy of watermark. This is used for multiple bit checking and technology also. Now the correlation factors at mean values of particular block of watermarking scheme with the PN sequence is applied for detection of watermarking.

The size of watermark is depends on the blocks are to be used for embedding system. This technology is used as size of block either it is small or larger. The size of block declare the robustness and other positive attributes of correlation procedure as well as watermarking technology. By this methodology, the errors can be minimized and recovery is done in easily process.



**Figure 5.1:** Choice of Threshold by Mean Value

## DCT Based Watermarking

The frequency of image which is used in watermarking is generally complex and to make it easy, the technology used for this frequency into different frequency range. This technology is known as DCT based watermarking scheme. This technology is related to the Fourier Transform in which the data is working in spatial mode of operation.

## Correlation Based DCT Watermarking

To enable the middle range frequency of embedded system of a PN sequence, this technology is used for particular block. In this technology, two uncorrelated data of different PN sequence is exist in the watermarking scheme as embedded into the images. This process is completed by the divide the images into many blocks and then it precede for each block working. The size of block is so that the entire messages can be built into this block and store respective image of embedded in watermarking scheme. Then it is proceeding for different computational techniques and

different messages in form of 0 or 1 are generated. Then it is compared with PN sequence and other PN sequence for improvement the correlation of watermarking technology.

## Conclusions

The embedded design is used for reliable purpose and completed the whole process of watermark. The watermark has some basic features such as recoverable in different disturbances conditions and changeable situations, it must be secure without any unwanted information and data even not accessible different messages, it must be non removable. After that it must be assured that watermark is secure for a given embedded system and necessary codes for every place and entity. Accept this; it is also ensure that digital watermarking is not assurance for any undisturbed data and authentication and resist messages of unwanted with a scientific and significantly proof or evidence.

Thus, DCT based watermarking technique gives better results for normal watermark embedding and extraction as indicated by lower bit error rates and higher peak signal to noise ratio.

# CHAPTER 6 EXPERIMENTAL RESULTS AND ANALYSIS

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | K=20 | | | K=40 | | | K=60 | | |
| PSN R | BE R (%) | Correlation Coefficient | PSNR | BE R (%) | Coeffi cient of Correl ation | PSNR | BE R (%) | Coefficient of Correlation |
| Threshold based watermarking | 80.36 | 1.2 | .9410 | 58.47 | .6 | .9693 | 37.3 | .3 | .9799 |
| DCT based watermarking | 81.34 | 0 | 1 | 72.41 | 0 | 1 | 64.31 | 0 | 1 |
| Correlation based DCT watermarking | 60.37 | 0 | 1 | 48.63 | 0 | 1 | 35.44 | 0 | 1 |

**Table 6.1: Performance analysis of watermarking techniques for normal watermark embedding and extraction**

# CHAPTER - 7

**SUMMARY, RECOMMENDATIONS AND FUTURE SCOPE**

The advanced signal processing is very useful in digital watermarking concerns of theft of copyright and multimedia information. The research is going on digital watermarking in many institutes as applications.

The method of disguising the plaintext in such a way as to hide its information is encryption and the encrypted text is known as cipher text. The process of reverting cipher text back to its original text is decryption.

To protect digital information at large scale against illegal manipulation, need a suitable technology that facilitate to avoid threats of intellectual property theft and unlawful tampering without any negotiation. The original messages in digital form arises because of information in digitally stored is easily copied rather than analogy.

The form of embedded system is to be selected so as it is secret and understanding for the owner and respond ate of the original data such as in the image form, data form, text form or any other form. But there are some constraints to represent in this method for the person or any owning person. So it is necessary to robustness and secure for further processing.

The threshold correlation technique of watermarking scheme consists of embedded system and many properties related to this. In these two techniques of watermarking, working in spatial mode is easy and less robust. In this mode of operation decoding and encoding of data and messages are selected with PN block sequence and then prepare a watermark stage with embedded system. The watermark sequence is to be checked by bit of message as 0 or 1. The procedure is to be repeated and expanded for all stages and then contributes with image of watermarking done.

The DCT image technique based on mid band coefficients is one of the type of watermarking in which the conversion is made about 0 or 1 for particular watermarking scheme. Then different type of images is to be divided into some blocks and then each block is choosing for watermarking scheme with definite pixels of embedding. This data in the form of digitally as 0 or 1 remains constant for whole process of embedding. The robustness of technology is achieved by changing the pixels of data of watermarking scheme. This is constraint that no visualise of images is present in this technology.

## REFERENCES

1. W. Stallings, “Cryptography and Network Security: Principles and Practice”, ISBN 0131115022, 9780131115026, Prentice-Hall, New Jersey, 2003.
2. Juergen Seitz, “Digital watermarking for Digital Media”,ISBN 1-59140-518-1,Information Science Publishing,London,2005.
3. Second Lieutenant J. Caldwell, “Steganography”, United States Air Force, Crosstalk-Journals of Defense Software Engineering, ,vol.-16,no.-6,pp.25-27, June 2003.
4. F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, “Information Hiding - A Survey”, Proceedings of the IEEE, vol. 87, no. 7, pp. 1062-1078, July 1999.
5. Jia-Shiang Chen, Yu-Bin Chen,Pei-feng Hsu,Nghia Nguyen-Huu and Yu-Lung Lo, “ Cryptographic scheme using genetic algorithm and optical responses of periodic structures”, OPTICS EXPRESS, vol. 19, no. 9, April 2011.
6. J. O. Ruanaidh,H.Peterson,A.Herrigel,S.Pereira and T.Pun, “Cryptographic Copyright Protection for Digital Images based on Watermarking Techniques”,Elsevier Science Publication, SPP Program(Grant 5003-45334), 1998.
7. Harsh K Verma,Abhishek Narain Singh,Raman Kumar“ Robustness of the Digital Image Watermarking Techniques against Brightness and Rotation Attack”, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 5, No. 1, 2009.
8. S. Battiato, D. Catalano, G:Gallo and R.Gennaro ," A Color Opponency Watermarking Scheme for Digital Images ", IST/SPIE International Symposium - Electronic Imaging 2000 -

Science & Technology, Security and Watermarking of Multimedia Contents II - San Jos,3971 : 510-515,2000 .

1. Maha Sharkas, Dahlia ElShafie, and Nadder Hamdy Senior Member IEEE, “A Dual Digital- Image Watermarking Technique”, World Academy of Science, Engineering and Technology, 5 2005.
2. Xinge You, Senior Member, IEEE, Liang Du, Member, IEEE, Yiu-ming Cheung, Senior Member, IEEE, and Qiuhui Chen, “A BlindWatermarking Scheme Using New Nontensor Product Wavelet Filter Banks”, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 19, NO. 12, DECEMBER 2010.
3. Nima Khademi Kalantari, Student Member, IEEE, and Seyed Mohammad Ahadi, Senior Member, IEEE, “A Logarithmic Quantization Index Modulation for Perceptually Better Data Hiding”, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 19, NO. 6, JUNE 2010.
4. Giulia Boato, Associate Member, IEEE, Valentina Conotter, Francesco G. B. De Natale, Senior Member, IEEE, and Claudio Fontanari, Member, IEEE, “Watermarking Robustness Evaluation Based on Perceptual Quality via Genetic Algorithms,” IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 4, NO. 2, JUNE 2009.
5. Jen-Sheng Tsai, Win-Bin Huang, and Yau-Hwang Kuo, “On the Selection of Optimal Feature Region Set for Robust Digital Image Watermarking,” IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 20, NO. 3, MARCH 2011.
6. Chip-Hong Chang, Senior Member, IEEE, and Aijiao Cui, Student Member, IEEE, “Synthesis-for-Testability Watermarking for Field Authentication of VLSI Intellectual Property,” IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS, VOL. 57,

NO. 7, JULY 2010

1. Kwangtaek Kim, Member, IEEE, Mauro Barni, Senior Member, IEEE, and Hong Z. Tan, Senior Member, IEEE, “Roughness-Adaptive 3-D Watermarking Based on Masking Effect of Surface Roughness”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 4, DECEMBER 2010.
2. A. V. Subramanyam, Sabu Emmanuel, Member, IEEE, and Mohan S. Kankanhalli, Senior Member, IEEE. “Robust Watermarking of Compressed and Encrypted JPEG2000 Images”, IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 14, NO. 3, JUNE 2012.
3. Yu-Ping Wang and Shi-Min Hu, Member, IEEE, “A New Watermarking Method for 3D Models Based on Integral Invariants”, IEEE TRANSACTIONS ON VISUALIZATION AND COMPUTER GRAPHICS, VOL. 15, NO. 2, MARCH/APRIL 2009.
4. Chuntao Wang, Member, IEEE, Jiangqun Ni, Member, IEEE, and Jiwu Huang, Senior Member, IEEE, “An Informed Watermarking Scheme Using Hidden Markov Model in the Wavelet Domain”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 3, JUNE 2012.
5. R. Reyes, C. Cruz, M. Nakano-Miyatake, Member IEEE and H. Pérez-Meana, Senior Member IEEE, “Digital Video Watermarking in DWT Domain Using Chaotic Mixtures”, IEEE LATIN AMERICA TRANSACTIONS, VOL. 8, NO. 3, JUNE 2010.
6. Pik Wah Chan, Student Member, IEEE, Michael R. Lyu, Fellow, IEEE, and Roland T. Chin, “A Novel Scheme for Hybrid Digital Video Watermarking:Approach, Evaluation and Experimentation”, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 15, NO. 12, DECEMBER 2005.
7. Nima Khademi Kalantari, Student Member, IEEE, Mohammad Ali Akhaee, Student Member, IEEE, Seyed Mohammad Ahadi, Senior Member, IEEE, and Hamidreza Amindavar, Member, IEEE “Robust Multiplicative Patchwork Method for Audio Watermarking”, IEEE TRANSACTIONS ON AUDIO, SPEECH, AND LANGUAGE PROCESSING, VOL. 17, NO. 6, AUGUST 2009.
8. Federica Battisti, Student Member, IEEE, Giulia Boato, Member, IEEE, Marco Carli, Senior Member, IEEE, and Alessandro Neri, Member, IEEE “Teaching Multimedia Data Protection Through an International Online Competition”IEEE TRANSACTIONS ON EDUCATION, VOL. 54, NO. 3, AUGUST 2011.
9. Hui-Yu Huang, Member, IEEE, Cheng-Han Yang, and Wen-Hsing Hsu, “A Video Watermarking Technique Based on Pseudo-3-D DCT and Quantization Index ModulationIEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 4, DECEMBER 2010.
10. Saraju P. Mohanty, Member, IEEE, Nagarajan Ranganathan, Fellow, IEEE, and Ravi K. Namballa, “A VLSI Architecture for Visible Watermarking in a Secure Still Digital Camera (S2DC) Design (Corrected)”, IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 13, NO. 8, AUGUST 2005.
11. Yu-Hsun Lin and Ja-Ling Wu, Fellow, IEEE, “A Digital Blind Watermarking for Depth- Image-Based

Rendering 3D Images”, IEEE TRANSACTIONS ON BROADCASTING, VOL. 57, NO. 2, JUNE 2011.

1. Chih-Chin Lai, Member, IEEE, and Cheng-Chih Tsai, “Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition”, IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL. 59, NO. 11, NOVEMBER 2010.
2. Luiz Octavio Massato Kobayashi, Sergio Shiguemi Furuie, and Paulo Sergio Licciardi Messeder Barreto, “Providing Integrity and Authenticity in DICOM Images: A Novel Approach”, IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE, VOL. 13, NO. 4, JULY 2009.
3. Min-Jeong Lee, Kyung-Su Kim, and Heung-Kyu Lee, “Digital Cinema Watermarking for Estimating

the Position of the Pirate”, IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 12, NO. 7, NOVEMBER 2010..

1. Xiang-Yang Wang, Pan-Pan Niu, and Hong-Ying Yang Liaoning Normal University, “A Robust, Digital-Audio Watermarking Method”, Article-IEEE Computer Society- 1070- 986X,2009.
2. Pei-Ju Chiang, Jan P. Allebach, Fellow, IEEE, and George T.-C. Chiu, “Extrinsic Signature Embedding and Detection in Electrophotographic Halftoned Images Through Exposure Modulation”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 3, SEPTEMBER 2011.
3. Pei-Yu Lin, Jung-San Lee, and Chin-Chen Chang, Fellow, IEEE, “Dual Digital Watermarking for Internet Media Based on Hybrid Strategies”, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 19, NO. 8, AUGUST 2009.
4. Fabrizio Guerrini, Masahiro Okuda, Nicola Adami, and Riccardo Leonardi “High Dynamic Range Image Watermarking Robust Against Tone-Mapping Operators”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 2, JUNE 2011.
5. Xiaoyu Feng, Hongting Zhang, Hsiao-Chun Wu, Senior Member, IEEE, and YiyanWu, Fellow, IEEE, “A New Approach for Optimal Multiple Watermarks Injection”, IEEE SIGNAL PROCESSING LETTERS, VOL. 18, NO. 10, OCTOBER 2011.
6. Kanchan H. Wagh, Pravin K. Dakhole, Vinod G. Adhau, “ Design & Implementation of JPEG2000 Encoder using VHDL”, Proceedings of the World Congress on Engineering 2008 Vol I, pp670-675, July 2 - 4, 2008.
7. Xiaotian Xu, Student Member, IEEE, Yong Liang Guan, Member, IEEE, and Kah Chan Teh, Member, IEEE, “Performance Analysis of Binned Orthogonal/Bi-Orthogonal Block Code as Dirty-Paper Code for Digital Watermarking Application”, IEEE SIGNAL PROCESSING LETTERS, VOL. 16, NO. 3, MARCH 2009.

## APPENDIX

**Program and Coding:-**

library IEEE;

use IEEE.STD\_LOGIC\_1164.ALL; use IEEE.STD\_LOGIC\_ARITH.ALL;

use IEEE.STD\_LOGIC\_UNSIGNED.ALL;

-- Uncomment the following lines to use the declarations that are

-- provided for instantiating Xilinx primitive components.

--library UNISIM;

--use UNISIM.VComponents.all;

entity random is

generic ( wd : integer := 8 );

port (

clk : in std\_logic;

random\_num : out std\_logic\_vector (wd-1 downto 0) --output vector

);

end random;

architecture Behavioral of random is begin

process(clk)

variable rand\_temp : std\_logic\_vector(wd-1 downto 0):="10000000";-- && others => '0'); variable temp : std\_logic := '0';

begin if(rising\_edge(clk)) then

temp := rand\_temp(wd-1) xor rand\_temp(wd-2); rand\_temp(wd-1 downto 1) := rand\_temp(wd-2 downto 0); rand\_temp(0) := temp;

end if;

random\_num <= rand\_temp; end process;

end Behavioral;