Copyright Protection Of Multimedia

Capstone Project Report

MID SEMESTER EVALUATION

Submitted by:

(102083013) Sehaj Kapoor

(101903270) Pratham Kapoor

(101903275) Vaibhav

(101903276) Yash Aggarwal

BE Third Year, COE

CPG No: 234

Under the Mentorship of

Dr. Ashima Anand

Assistant Professor

Computer Science and Engineering Department
Thapar Institute of Engineering and Technology, Patiala
July 2022

ABSTRACT

Watermarking performs a genuinely essential function inside the subject of network safety and authentication of records. But the main hassle is to secure the data from duplication and unauthorized use. Consequently, digital watermarking is employed. With this technology, we tend to implant the secret information into the real information for protecting it from unauthorized use. The need and requirement of online transaction of records is growing daily on the internet consequently we would like authentication and safety of our facts and virtual watermarking is the decision of that drawback. Digital watermarking illustrates techniques and technology that cover the records inside the form of text, images, audio and video.

For security purposes we take input as an image which you want to watermark, then we will generate any random key with our logic. By using RSA encryption, we generate public and private keys to encrypt randomly generated keys. After key generation we encrypt the watermark image by using RSA keys. After that we stored these data into our database. Then this newly formed image will be read and embedded into the original image. Then we have to detect the image for that we retrieve all the information regarding the image from the database. Then we decrypt the RSA private key to read that watermarked image, after decryption the image and hidden watermark will be displayed.

For any who envisions building an application, uploading images is a major component they have to take into account. It is an essential requirement while creating a complete application. File uploading means a user from a client machine wants to upload files to the server. For example, users can upload images, videos, etc. on Facebook, Instagram. As with any programming problem, there are many ways to achieve this outcome. This article explains a simple way to implement the approach to upload a single file with React.
The process of uploading an image can be broadly divided into two steps:

•Select a File (user input): To enable the user to pick a file, the first step is to add the tag to our App component. This tag should have the type attribute set as “file”. Now, we need an event handler to listen to any changes made to the file. This event handler will be triggered whenever the user selects a new file and will update the state.
•Send a request to the server: After storing the selected file (in the state), we are now required to send it to a server
•File encryption is one of the most effective security solutions. Combined with advanced security controls, it gives your business comprehensive data protection. AES Crypt is a file encryption software available on several operating systems that uses the industry standard Advanced Encryption Standard (AES) to easily and securely encrypt files.

•The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order.

Keywords: RSA, Watermark, Private Key, Public Key, Secure data, database, encryption, decryption

DECLARATION

We hereby declare that the design principles and working prototype model of the project entitled Copyright protection of multimedia is an authentic record of our own work carried out in the Computer Science and Engineering Department, TIET, Patiala, under the guidance of Dr Ashima Anand and during 7th semester (2022).

Date: 26/08/2022

Roll No.	Name	Signature
102083013	Sehaj Kapoor	S Kapoor
101903270	Pratham Kapoor	Pratham
101903275	Vaibhav	Vaibhav
101903276	Yash Aggarwal	Yash

Counter Signed By: Ashima 26/08/22

Faculty Mentor: Dr Ashima Anand

Designation: Assistant professor

CSED

TIET, Patiala

ACKNOWLEDGEMENT

We would like to express our thanks to our mentor Dr Ashima Anand. She has been of great help in our venture, and an indispensable resource of technical knowledge. She is truly an amazing mentor to have.

We are also thankful to Dr Shalini Batra, Head, Computer Science and Engineering Department, entire faculty and staff of Computer Science and Engineering Department, and also our friends who devoted their valuable time and helped us in all possible ways towards successful completion of this project. We thank all those who have contributed either directly or indirectly towards this project.

Lastly, we would also like to thank our families for their unyielding love and encouragement. They always wanted the best for us and we admire their determination and sacrifice.

Date: 26/08/2022

Roll No.	Name	Signature
102083013	Sehaj Kapoor	SKAPOOR
101903270	Pratham Kapoor	Pratham
101903275	Vaibhav	Vaibhav
101903276	Yash Aggarwal	Yash

Ashima
26/08/2022

TABLE OF CONTENTS

ABSTRACT…... i
DECLARATION….. ii
ACKNOWLEDGEMENT…... iii
LIST OF FIGURES..iv
LIST OF TABLES...v
LIST OF ABBREVIATIONS vi

CH APTER… ....Page No.
1. **Introduction** 1
1.1 Project Overview
1.2 Need Analysis
1.3 Research Gaps
1.4 Problem Definition and Scope
1.5 Assumptions and Constraints
1.6 Standards
1.7 Approved Objectives
1.8 Methodology
1.9 Project Outcomes and Deliverables
1.10 Novelty of Work
2. **Requirement Analysis**
2.1 Literature Survey
2.1.1 Theory Associated With Problem Area
2.1.2 Existing Systems and Solutions
2.1.3 Research Findings for Existing Literature
2.1.4 Problem Identified
2.1.5 Survey of Tools and Technologies Used
2.2 Software Requirement Specification
2.2.1 Introduction
2.2.1.1 Purpose
2.2.1.2 Intended Audience and Reading Suggestions
2.2.1.3 Project Scope
2.2.2 Overall Description
2.2.2.1 Product Perspective
2.2.2.2 Product Features
2.2.3 External Interface Requirements
2.2.3.1 User Interfaces

2.2.3.2 Hardware Interfaces

2.2.3.3 Software Interfaces

2.2.4 Other Non-functional Requirements

2.2.4.1 Performance Requirements

2.2.4.2 Safety Requirements

2.2.4.3 Security Requirements

2.3 Cost Analysis

2.4 Risk Analysis

3. Methodology Adopted

3.1 Investigative Techniques

3.2 Proposed Solution

3.3 Work Breakdown Structure

3.4 Tools and Technology

4. Design Specifications

4.1 System Architecture

4.2 Design Level Diagrams

4.3 User Interface Diagrams

4.4 Snapshots of Working Prototype

5. Conclusions and Future Scope

5.1 Work Accomplished

5.2 Conclusions

5.3 Environmental Benefits

5.4 Future Work Plan

INTRODUCTION

1.1 Project Overview

Digital watermarking is that technology that provides protection, appropriate data and copyright protection of the digital data. Security of digital data has become a popular matter due to the fast development of the multimedia technology.

Digital watermarking is the process of inserting secret digital data, signal into the digital media such as image, video, audio and text. Digital Image Watermarking technology has many applications for protection of digital data. The basic idea of digital watermarking is to embed the information i.e., watermark into a host image. Then that watermarked image will be transmitted over the internet and at the receiver side information is taking out. We can use steganography to hide text, video, images, or even audio data. It's a helpful bit of knowledge, limited only by the type of medium and the author's imagination. The second type of steganography is image steganography, which entails concealing data by using an image of a different object as a cover. Pixel intensities are the key to data concealment in image steganography. Unique picture that can conceal data. Stego-Image is an image with a hidden message. Digital media has many advantages over analogy media; however, the possibility of unlicensed duplication and dissemination of copyrighted material poses a hazard to traditional business models. Two complementary techniques have been applied to address this problem: encryption and watermarking. Encryption techniques can be used to protect the data when it is being delivered from the sender to the receiver. The receiver decrypts the data and obtain the original copy.

Complementary to encryption, invisible watermarking can embed a secret (possible imperceptible) signal, called watermark, such that it cannot be (easily) extracted but that can be easily read and employed in many different applications. Each watermark signal is application-specific; nevertheless, general requirements for a watermark can be specified as it is described in. A key feature of watermarking is the perceptual transparency. It refers to the fact that the embedding of a signal should not be perceptible to humans and not affect the quality of the underlying data. In this work, we describe most common watermarking application scenarios to illustrate that watermark algorithms are in the eye of the storm of most of the Internet security and Copyright problems. Then, we summarize the most common and well-known watermark methods giving a readable description and explaining their main advantages and drawbacks. Additionally, we provide a description of many possible attacks against watermarks.Data security is essential in today's world of internet and networking. In any organization information is critical. In today’s world people are ready to spend thousands and lack money in order to ensure a high level of information security.

In spite of spending such a huge amount, still the objective of securing the information is not achieved as the data somehow gets in the hands of hackers. As the technology for securing the data is advancing, hackers are also keeping pace with this technology .Hackers now make use of certain algorithms or other techniques to decode the data encoded by the senders. One of the ways to ensure security is to ensure that data is not visible to the hacker. This can be done by hiding the message itself behind some other objects.

1.2 Need Analysis

Files are the foremost basic secure storage units. information is usually keep and shared as files and folders. Therefore, file security could be a set of information security that focuses on the safe use of files. Data security protects information in use, in transit and at rest. Infrastructure and software system controls are accustomed implement strict information security methods. File security, on the opposite hand, protects sensitive files like client personal data and different business files.

Personally identifiable data, electronic personal health data confidentiality agreements, and alternative essential business information should be keep firmly. Careless transfer or use of such files may lead to a breach of privacy, subjecting the organization to significant fines. Files transmitted through insecure channels are often exploited by insiders or hackers for malicious activities. Comprehensive information escape interference software will facilitate stop the unauthorized movement of crucial business information outside of a company.In our system, we have to secure file after the user upload it and while sharing. For that we used the various encryption algorithm in it like AES, RSA and different watermarking techniques.

Here we are achieving this data security concept through the technique of Steganography. Being able to upload files is an essential requirement while creating an application. Uploading files means a user from a client side should be able to upload files to the server. There are many ways to achieve this, as each file system has its own implementation. In this article, we’ll look at file uploads in React with React Upload by building a file uploads system. React-Upload is a lightweight library that enables developers to build client-side, file-upload features with just a few lines of code. Essentially, it’s a library that focuses on modern file upload components and hooks for React applications. It’s also an all-in-one shop for all things file uploads, such as file upload progress, upload buttons, and enhancers for uploads. It's a method to conceal the fact that communication is taking place. Maintain communication security. Optional, but increases security when utilized. Once hidden information is decoded, the data can be used by anyone. Does not modify the data's general structure. Steganography is a method that makes it easy to conceal a message within another to keep it secret. Steghide is an application that hides data in different audio and image files, including JPEG, BMP, AU, and WAV.

Motivation

We need to maintain an optimal balance between imperceptibility, robustness and embedding capacity while embedding secret data into biomedical signals. Security of the significant information and computational cost is equally important for any practical application.

Different optimization techniques and Fuzzy logic concepts can be added with watermarking technique for getting better embedding locations. However, it will increase the time complexity as well. While developing the watermarking scheme, different types of attacks should be considered.

The embedding methods need to be chosen in such a way that it should be independent of the number of samples present in the cover signal to maximize the overall capacity. To control the access and confidentiality of the data cryptographic techniques as well as key management and distribution model can be added with data hiding methods. However, it should enhance the cost as well. To enhance the security of data in spatial domain, different error correcting codes can be applied at receiver side to increase robustness and to achieve reversibility.

Scrambling operations can be added with the existing methods to increase the imperceptibility and confidentiality of the cover signal. However, the integrity of the data should not be altered. Along with the data hiding method, different encryption and compression scheme can also be merged to increase the overall security and imperceptibility of the system. However, the overall complexity of the system will increase.

1.3 Research Gap

Different fields of computer systems require a higher degree of focus on specific quality factors such as privacy, integrity, flexibility, usability, etc. Moreover, some quality factors help each other in existence, while others strongly contradict each other. Usability of software applications is one factor that reduces security and privacy to a substantial level. This article explores the differences between usability factors and aspects related to security and privacy. A clear understanding of the gaps between these two opposing factors has been presented in this article. In addition, a description of the efforts made to bridge these gaps was also presented. We have categorized these efforts into guidelines, frameworks, and technology use. In the previously used system, they only used the watermark algorithm, while we used both AES and RSA algorithms. Algo AES is used for image encryption and RSA for text encryption.

1.4 Problem Definition and Scope

The current digital watermarking methods are facing the problems in maintaining invisibleness, robustness, capacity and security. In this article, authors are analysing the various popular algorithms used in digital watermark of copyright protection and propose a novel approach by combining three such algorithms aiming to increase the invisibleness and robustness of the watermarked image. The experimental results, exemplifies much increase in invisibleness and a nominal increase in robustness.

The multimedia products are easily to download and reproduce for the commercial profit. That is the so-called intelligent property privacy. with the fast adoption of the powerful multimedia manipulation tools, multimedia data such as pictures, video or audio clips have been decreased the credibility.it raises the awareness of the copyright problems in the e-commerce age.

Need to enforce secure digital watermarking strategies for e-governance applications and medical applications. Two completely distinct watermarks are embedded inside the cover page to boost the strength and protection. Moreover it reduces the distance for storing, transmission data bandwidth and transmission time time for clinical services. This will be for providing more secure algorithm and approach so as to protect from the Hackers and market competitors. With each implementation, there was considerable effort to enhance extensibility. As a result, the product had high maintainability, modifiability, and scalability. Deployment and maintenance will be done in the upcoming future and is outside of the scope of this paper.

1.5 Assumptions and Constraints

One of the factors influencing the analyst's choice as to whether a domain is relevant to the security of the system and should therefore be included in the context is the analyst's set of confidence assumptions. Trust assumptions are explicit or implicit choices about how to trust certain characteristics of domains. These assumptions can have a significant impact on system security. For example, most analysts implicitly assume that the compiler is not a security risk; they would never have thought to include it in the analysis. Thompson showed that this assumption is not necessarily justified by showing how the compiler could introduce a trapdoor into applications. Some examples illustrate how the requirements engineer's implicit trust in some domains in the environment can introduce unknown amounts of risk into the system. it went so far that without recognizing all the entities and their trust relationships in the software system during the requirements phase of the project, the project is doomed from the start.

Security requirements are often defined as "restrictions or limitations" placed on system services. Let's rephrase this definition slightly: security requirements express constraints on system behavior that are sufficient to meet security goals. Constraints are intended to limit undesirable system behaviour as much as possible while still satisfying system requirements. For example, the purpose of an ATM may be to provide cash to customers. This goal is clearly too broad from a security perspective. Providing restrictions, such as only if the customer physically owns the ATM card associated with the account and only if the customer provides the correct PIN (two security requirements), will limit the circumstances under which cash is to be provided.

1.6 Standards

When working on a project, standards are essential because they set quality levels and overall expectations. It also helps to make your project adaptable and easy to integrate. If other companies or teams want to integrate our project, we can do it easily. Adapts to our standard industry protocols.

IEEE 802.4 IEEE 802.4 describes the Marker Bus LAN standard. When using the token passing method, stations connected to the bus are organized into logical rings. With this method, only the station holding the token (the owner of the token) can send frames.

ISO/IEC/IEEE 23026:2015: Defines the systems management and engineering requirements for a website lifecycle, including strategy, design, design, testing and validation, and management and maintenance of intranet and extranet environments.

1.7 Approved Objectives

The main objectives of the project are:

The main objective for developing this application is that it can provide the user with security of data it will also provide the transfer of data from one machine to another in from of files only the authorized user and administrator can access the application.
1) Data embedding even as now no longer distorts the image.
2) Minimum perceptual degradation.
3) Information extraction without any loss.
4) This could in the long run be the reason for shielding medical images with watermarking.
5) Digital watermarking is presently a drastically focused technique aimed towards imparting a dependable manner to defend images or certify copyrights safety.
6) In the present mode-like spatial domain, the watermark isn't always nicely embedded and extracted and it finally ends up in the fallacious safety of secret info.
7) The prevailing spatial area is remodeled into frequency area mistreatment separate ripple rework.
8) In our projected paintings the watermark is from time to time embedded invisibly in the images to keep away from attracting the attention of malicious attackers.

9) We use color image watermarking, which has excessive efficiency in comparison to the ordinary gray scale picture watermarking.

1.8 Methodology

Following algorithms will be applied on features obtained above.

Image encoding:

The actual image is in AN encompassed sample which the pixel values are inside [0, 255], and intend the degrees of rows and columns as N1 and N2 and consequently the pixel wide variety as (N=N1 X N2). The watermark is embedded into the preliminary input image.

Encrypted Image Encoding:

The secret information became entered in textual content layout into the watermarked picture. If the key-word became matched, then best its movements to successive step. i.e., reconstruction, in any other case if the key-word doesn't match it ends in the error.

Image Watermark Extraction:

With the watermark embedded image and consequently the secret key (key-word), a receiver will regenerate the primary information of the preliminary image, and consequently the decision of the reconstructed image is based on the quantity of stage of watermark.

Frequency Domain Watermarking:

In frequency domain the watermark is embedded inside the spectral consistent of the image. The generally used algorithms in frequency domain are the discrete cosine transform (DCT), discrete Fourier transform (DFT), and discrete wavelet transform (DWT). The reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients.

Discrete cosine transforms (DCT):

DCT form of a Fourier rework, it represents data in phrases of frequency area rather than an amplitude area. this will be useful due to that corresponds extra to the technique people recognize light, so the 1/2 of that do not appear to be perceived may be regarded and thrown away. DCT based watermarking strategies are robust as compared to spatial area strategies. Such algorithms are robust in opposition to straightforward image technique operations like low pass filtering, brightness and difference adjustment, blurring etc. However, {they're} difficult to put in force and are computationally dearer. At steady time they may be susceptible in opposition to geometric attacks like rotation, scaling, cropping etc. DCT domain watermarking can be labelled into global DCT watermarking and Block based DCT watermarking. Embedding in the perceptually great slice of the image has its very own blessings due to maximum compression schemes cast off the perceptually insignificant part of the image. Steps in DCT Block based Watermarking algorithmic rule

1) Segment the image into non-overlapping blocks of 8x8.
2) Apply ahead DCT to each of these blocks
3) Apply a few block preference criteria (e.g., HVS).
4) Apply steady preference criteria (e.g., highest)
5) Embed watermark with the aid of using editing the selected coefficients.
6) Apply inverse DCT remodel on each block.

Discrete wavelet transforms (DWT):

Wavelet transform can be a contemporary-day approach frequently hired in digital image process, compression, watermarking etc. The transforms are supported little waves, called wavelet, of various frequency and limited period. The wavelet transform decomposes the image into three spatial directions, i.e., horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic residences of HVS loads of exactly. Magnitude of DWT coefficients is bigger inside the lowest bands (LL) at each stage of decomposition and is smaller for opportunity bands (HH, LH, and HL). The discrete wavelet transform (DWT) is currently employed in a terrific shape of sign manner programs, like in audio and video compression, elimination of noise in audio, and consequently the simulation of Wi-Fi antenna distribution. Wavelets have their power centred in time and are well matched for the evaluation of transient, time-various alerts. Since maximum of the actual lifestyles alerts encountered are time various in nature, the wavelet rework fits numerous programs alright. One among the maximum demanding situations of the watermarking disadvantage is to reap a better alternate among power and sensibility. Power is frequently accomplished via way of means of growing the power of the embedded watermark, but the seen distortion could be gathered also. However, DWT is manner favoured because of it gives a coincident spatial localization and a frequency spread of the watermark a few of the host image. The essential plan of wonderful wavelet rework in picture technique is to multi-differentiated decompose the image into sub-picture of numerous spatial domain and freelance frequencies.

RSA Algorithm:

RSA algorithmic program is asymmetric cryptography algorithmic program. Asymmetric without a doubt means that it really works on 2 completely unique keys i.e., Public Key and Private Key. Due to the fact the name describes that the overall public key's given to each person private key's saved private. An instance of asymmetric cryptography:

1) A customer (as an instance browser) sends its public key to the server and requests for some records.
2) The server encrypts the records the usage of client’s public key and sends the encrypted data.
3) Customer gets this records and decrypts it.

Since that is frequently asymmetric, no one else besides browser will decrypt the information despite the fact that a third party has public key of browser. The idea of RSA is based at the real truth that it is hard to clear up an outsized variety. The overall public key includes 2 numbers anywhere one variety is multiplication of two massive prime numbers and private key are conjointly derived from same 2 prime numbers. Consequently, if a person will clear up the massive range, the private keys compromised. Consequently, coding strength altogether lies on the important thing length and if we tend to double or triple the important thing length, the strength of coding will boom exponentially. RSA keys might be commonly 1024 or 2048 bits long, but experts accept as true with that 1024-bit keys may be tame the near future. But till presently it seems to be an impracticable task.

AES Algorithm:

With the widespread internet communication and the vital need to send data securely, we started using ciphering & encryption. As our use of ciphering increased, so did the complexity of the algorithms used to start from the very basic substitution ciphering reaching today’s most secure cipher, the AES. AES has superior features which allowed it to replace DES & almost every other known cipher, especially when it comes to security as AES is currently computationally unbreakable and will probably remain unbreakable unless a future quantum computer manages to reach the required computational ability. The encryption process involves Substitution of the bytes, shifting rows, mixing columns & adding round keys. The decryption process on the other hand involves adding round keys, inverse shifting rows, inverse byte substitution & inverse mixing columns. Current attacks have managed to target incomplete implementations of the algorithm without even coming close to breaking a Full-AES algorithm implemented correctly. In addition to security, the algorithm’s efficiency, sustainability & simplicity leads to a high evaluation allowing it to be in such supreme position among all other ciphers.

1.9 Project Outcomes and Deliverables

1. Can provide (strict) data-integrity, authenticity, non-repudiation, etc., if used with hash functions Faster than Digital Signature Can be cryptographically secure Can be robust to content preserving manipulations, if a suitable image feature is used Tampering localisation and recovery, if encrypted image feature is used as a watermark.
2. Data-integrity (strict) Authenticity (strict) much faster than Digital Signature Based on block-cipher or cryptographic hash function can be cryptographically secure Tampering localisation.
3. Data-integrity (strict) Authenticity (strict) Time stamp Non-repudiation Enforceability Tampering localisation can be cryptographically secure.
4. Data-integrity (selective) Authenticity (selective) Robustness to content preserving manipulations tampering localisation. Data-integrity (selective) Authenticity (selective) enforceability? Non-repudiation? Tampering localisation Robustness to content preserving manipulations possibly faster than paired helical filaments.

1.10 Novelty of Work

After adding the watermark to the file, we used RSA encryption, generate a public key and a private key to encrypt the randomly generated AES key. After generating the key, we encrypt the watermark image using AES keys. We then stored this data in our database. Then the newly created image will be loaded and inserted into the original image. Then we need to detect the image to get all the information related to the image from the database. Then we decrypt the AES key to read the watermarked image, after decryption the image and hidden watermark will be displayed. The proposed watermarking technique was developed under the assumption that noise attacks occur in isolation and not simultaneously. The project can be extended in a scenario where noise attacks occur simultaneously. Future work may be extended to audio and video data. The proposed scheme is limited to software only.

REQUIREMENT ANALYSIS

2.1 Literature Survey

2.1.1 Theory Associated with Problem Area

Service replication is not a complete solution to availability in network file systems, as we would have to face consistency and integrity issues between servers, so we would be back at the beginning of our problem. We could replicate our network file system, but it would take extra effort to get it working properly, and we'd have to use all the security mechanisms we need in both. On the other hand, traffic filtering can help us avoid any attacks because network file systems are usually accessible to a well-known range of addresses (usually the LAN range), so any traffic from these services flowing from or to addresses outside that range is not allowed operation. In addition, other measures can be taken at the service layer, such as dropping connections from sources that have failed to connect too many times over a period of time.

2.1.2 Existing Systems and Solutions

- A completely unique image sweetening technique, named CLAHE-discrete wavelet transform (DWT), which mixes the CLAHE with DWT.
- The new technique includes 3 main steps: initial, the first image is rotten into low-frequency and high-frequency elements by DWT.
- Then, the authors enhance the low-frequency coefficients exploitation CLAHE and keep the high-frequency coefficients unchanged to limit noise sweetening.

- This is often as a result of the high-frequency part corresponds to the detail info and contains most noises of original image.
- Finally, reconstruct the image by taking inverse DWT of the new coefficients.

Disadvantages of Existing System:

- System was not much secure.
- Easy to implement.
- System is not précised.

2.1.3 Research Findings for Existing Literature

Vaidya and Mouli |[1] demonstrated a color image watermarking based on multiple translorm domain decompositions DWT-CT-Schur-SVD. In this approach he singular values of encryptcd and decomposed watemark are conccaled into a carrier image luminancc componcnt with multiple decompositions. Experimental results indicate the proposed technique is robust and impereeptible against image processing attacks. Furthemore, when compared to other watemarking approaches, the suggested method is more safe, robust, and cficient. However, the scheme is costly. Gong et al. [2] proposed a scheme based on the combination of CT-SVD and Canny-edge detection. Initially, the carrier image is decomposed using contourlet transfom, then the low frequency sub-band is divided into 4x4 non-intersecting blocks. Further, the precise blocks are obtained via Canny cdge detection and singular valuc decomposition is performed. Finally, the watermark is concealed into the 'U' coefficient blocks. Experimental results reveal that the suggested scheme is good against nomal attacks. However, less resist geometric attac ks. Singh introduced a secure watermarking method for color medical images in LWT and DCT domains [3]. The security is improved by encrypting the signature mark using MD5. Also. BCH encoded patient details improves the resistance for channel noise. The RGB color image is converted into the Y1Q model and the resultant Y component is altered using the gain factor to hide the pre-processed marks. Visual quality and embedding capacity of this work is better than the traditional marking techniques. In [4], the authors investigated the effectiveness of the watermarking scheme for COVID-19 images and explored its impact on different attacks. In their article, multiple-marks are embedded by using the different transfomed-domain scheme for various kinds of images. Although the robustness of the scheme has been greatly improved in this paper, the security of the image is still weak. In [5]. Zhu et al. suggested a robust watermarking, which uses Amold scheme to scrambled the binary watenark for better securty. The serambled watemmark is further encrypted using a key and then embedded within a block of cover. Authors also analyse imperceptibility and security of the developed algorithm. Singh elal has presented a DWT-DCT-SVD based robust watemarking approach in the Iransfom domain [6]. Initially, DWT is applicd to decompose the host image into sub-bands. Further, DC T and SVD have been applied on selected sub-band. The watermark image is decomposed with the help of DCT and SVD. Watemark is inserted into the uranstormed coefficient of the host image. This scheme provides a better robustness against several attacks. In Ref. [7], a dual watermarking scheme is implemented for providing the security of digital contents. In the preprocessing stage, image watermark is scrambled using Arnold transform and Page 6 of 12 text watemark is encoded by hamming code. In the embedding stage, it uses the second- level of DWT to decompose the host image into diflerent sub-bands. Further, the selec ted sub-band is trans fomed using SVD. The dual watermark is hidden into trans fonmed coefricients of the host image.

The watemarked image is compressed via SPIHT transform to reduce bandwidth demand. A multiple watemarking technique is proposed by Alshanbari [1]. This method combines robust and fragile watermarking for ownership identification and authentication. It embeds ownership information in the whole image to verify thc authenticity. Further, the recovery mark is generated by combining the region of interest (RO1) along with its SHA-256 hash values and compressed using LZW compression. The principal component of the compressed recovery mark is placed inside the DWT-SVD coefficients ofthe RONI region of the cover image. DWT based blind watermarking framework for protection of digital records is proposed by Kahlessenane et al. [2]. Initially, patients' details are combined with its 128-bit MD5 hash values to fom the final watemark. Further, DWT is applied on the cover image. The final mark is placed in the reorganized low frequency DWT coefficients to ensure better security with high robustness. Singh introduced a secure watemarking method for color images in LWT and DCT domains [3] The security is improved by encrypting the signature mark using MD5. Also, BCH encoded patient details improves the resistance for channel noise. The RGB color image is converted into the YIQ model and the resultant Y component is altered using the gain factor to hide the preprocessed marks. Visual quality and embedding capacity of this work is better than the traditional marking techniques. Nazari and Maneshi developed a reversible watermarking technique for secure transmission of digital records [4]. The authors ensured tamper detection by transfoming the cover image using IWT and hiding Integrity Check Code (ICC) and patient's details in the least significant bits of the resulting IWT coefficients. Also, watemarks are encrypted using logistie sine based chaotie encryption for better security and authentication. The authors of [5] proposed a blind and secure watemarking scheme for medical and non-medical images. Initially, the cover image is divided into ROI and RONI regions, which are ureated as watemark and carrier images respecively. Encrypted ROI segment along with the patient's infomation is placed in different level IWT Page 7 of 12 coellicients of the RONI scgment. Also, the authentication process is enhanced by hiding the doctor's signature in the third level IWT coeflicients, which provides better robustness. Liu et al. devised DTCWT-DCT and eneryption based watermarking methods supporting zero and blind extraction [6]. In the proposed work, the three marks are encrypted using a chaotic system and a henon map ensuring better security. The encrypted marks are hidden in low frequency DTCWT-DCT coefficients of the carrier image of size 128 x 128.

[1] H. S. Alshanbari, "Medical image watemarking for ownership & tamper detection," Multimed. Tools Appl., vol. 80, pp. 16549-16564, 2021, doi: 10.1007/s1 1042- 020-08814-9.

[2] R. B. Wolfgang and E. J. Delp, “A watermarking technique for digital imagery: Further studies,” in Proc. Int. Conf. Imaging Science, Las Vegas, NV, June/July 1997, pp. 279–287.

[3] A. K. Singh, "Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image," Multimed. Tools Appl., vol. 78, pp. 30523-30533, 2019, doi: 10.1007/s1 1042-018-7115-x.

[4] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” IEEE Trans. Image Processing, vol. 6, pp. 1673–1687, Dec. 1997

[5] M. Nazari and M. Mehrabian, "A novel chaotic IWT-LSB blind watermarking approach with flexible capacity for secure transmission of authenticated medical images," Multimed. Tools Appl, vol. 80, pp. 10615-10655, 2021, doi: 10.1007/s1 1042-020-10032 2.

[6] J. Liu, J. Li, J. Ma, N. Sadi , U. A. Bhatti, and Y. Ai, "A robust multiwatermarking algorithm for medical images based on DTCWT-DCT and henon map," Appl. Sci., vol. 9, no. 4, 2019, doi: 10.3390/app9040700.

2.1.4 Problem Identified

The current digital watermarking methods are facing the problems in maintaining invisibleness, robustness, capacity and security. In this article, authors are analysing the various popular algorithms used in digital watermark of copyright protection and propose a novel approach by combining three such algorithms aiming to increase the invisibleness and robustness of the watermarked image. The experimental results, exemplifies much increase in invisibleness and a nominal increase in robustness.

The multimedia products are easily to download and reproduce for the commercial profit. That is the so-called intelligent property privacy. With the fast adoption of the powerful multimedia manipulation tools, multimedia data such as pictures, video or audio clips have been decreased the credibility.it raises the awareness of the copyright problems in the e-commerce age.

2.2 Software Requirement Specification

Hardware:

1. Processor: Intel Core i3 or more.
2. RAM: 4GB or more.
3. Hard disk: 250 GB or more.

Software:

1. Operating System: Windows 10, 7, 8.
2. Python.
3. Anaconda.
4. Spyder, Jupiter notebook, Flask.
5. MYSQL.
6. React

Technologies Used: -

Python:

Python could likewise be a taken item organized basic level language with dynamic derivation its straightforward level in-created information structures got together with unique organization and dynamic restricting sort it outrageously interesting for speedy application advancement what's more on be utilized as a pre piece or glue language to relate existing components on pythons clear direct to be told accentuation highlights quality by then decreases the cost of program fixes python maintains modules and packs that moves program quality and code utilize the python go-between and what's more the escalated standard library are offered in give or combined sort to nothing of charge for each and every fundamental stage and wish to be uninhibitedly spread oft programmers fall stricken with python because of the misrepresented strength it gives since there is no aggregation step the special stepped area test-investigate cycle is unfathomably expedient work python programs is basic a bug or unfortunate information won't ever cause a division deformity taking everything into account once the interpreter discovers a blunder it raises an extraordinary case once the program doesn't get the exception the go-between prints a stack follow a stock level program licenses assessment of local and world elements examination of self-emphatic enunciations setting breakpoints wandering through the code a line at a rapidly on the program is written in python itself vouching for pythons smart power barring generally the quick in view of right a program is to incorporate a few print clarifications to the accessibility the quick modify test-explore cycle makes this simple philosophy dreadfully amazing.

FLASK:

A Flask is a Web Application Framework that is built with Flexibility and Speed In the Mind. Flask is Built in Python , which many data Scientists are familiar with . Flask takes care of the Environment and Project setup involved in web Applications Allowing the Developer to focus on their application rather than thinking about HTTP , routing , dataset etc. Flask allows Data Scientists to create simple Single page Applications and one should Help or look into if they want to create Products for Consumers Flask is a micro web framework written in Python. It is classified as a microframework because it doesn't require particular tools or libraries. it’s no database abstraction layer, form validation, or the other components where pre-existing third-party libraries provide common functions. However, Flask supports extensions which will add application features as if they were implemented in Flask itself. Extensions exist for object-relational mappers, form validation, upload handling, various open authentication technologies and a number of other common framework related tools Flask was created by Armin Conacher of Pocono, a world group of Python enthusiasts formed in 2004.According to Conacher, the thought was originally an April Fool’s joke that was popular enough to form into significant application. When Conacher and Georg Brandi created a bulletin board system written in Python, the Pocono projects Werke and Jinja were developed. Flask has become popular among Python enthusiasts. As of October 2020, its second most stars on GitHub among Python web-development frameworks, only slightly behind

Django, and was voted the foremost popular web framework within the Python Developers Survey 2018.

These are some Important features of the Flask:

1. it is a Development Server
2. Debugger
3. RESTful request dispatching
4. Unicode Based
5. Flask have google app engine Compatibility

ReactJS:

React (also known as **React.js** or **ReactJS**) is a free and open-source front-end JavaScript library for building user interfaces based on UI components. It is maintained by Meta (formerly Facebook) and a community of individual developers and companies. React can be used as a base in the development of single-page, mobile, or server-rendered applications with frameworks like Next.js. However, React is only concerned with state management and rendering that state to the DOM, so creating React applications usually requires the use of additional libraries for routing, as well as certain client-side functionality.

MySQL:

MySQL is prestigious as world's most by and large utilized ascii archive data back-end its most guarantee data for pup as MySQL is most habitually utilized ascii record prearranging data attempt workers offer for MySQL is ideal and diminishes our work to an outsized degree.

2.2.1 Introduction

2.2.1.1 Purpose

Purpose of digital watermark Watermarks added to digital content serve different purposes purposes. The following list details the six purposes digital watermark.

1. Claim of ownership: establish ownership of content.
2. Fingerprints: avoid unauthorized reproduction and public distribution available multimedia content.
3. Authentication and integrity authentication: the authenticator is inextricably bound to content where the author has a unique key associated with the content and can verify its integrity this content by extracting the watermark.

4. Content marking: embedded bits to data that provides additional information about content such as a graphic image with time and place information.
5. Usage control: added to restrictions the number of copies made while the watermarks are modified by hardware and at some point would do not make any further copies (i.e. DVDs).
6. Content protection: content sealed with a visible watermark that is very difficult to remove to be public and free distributed. Unfortunately, there is no universal a watermarking technique that satisfies all these requirements purposes Content in determines the environment that will be used digital watermarking technique.

2.2.1.3 Project Scope

Need to enforce secure digital watermarking strategies for e-governance applications and medical applications. Two completely distinct watermarks are embedded inside the cover page to boost the strength and protection. Moreover it reduces the distance for storing, transmission data bandwidth and transmission time time for clinical services. This will be for providing more secure algorithm and approach so as to protect from the Hackers and market competitors

With each implementation, there was considerable effort to enhance extensibility. As a result, the product had high maintainability, modifiability, and scalability. Deployment and maintenance will be done in the upcoming future and is outside of the scope of this paper.

2.2.2 Overall Description

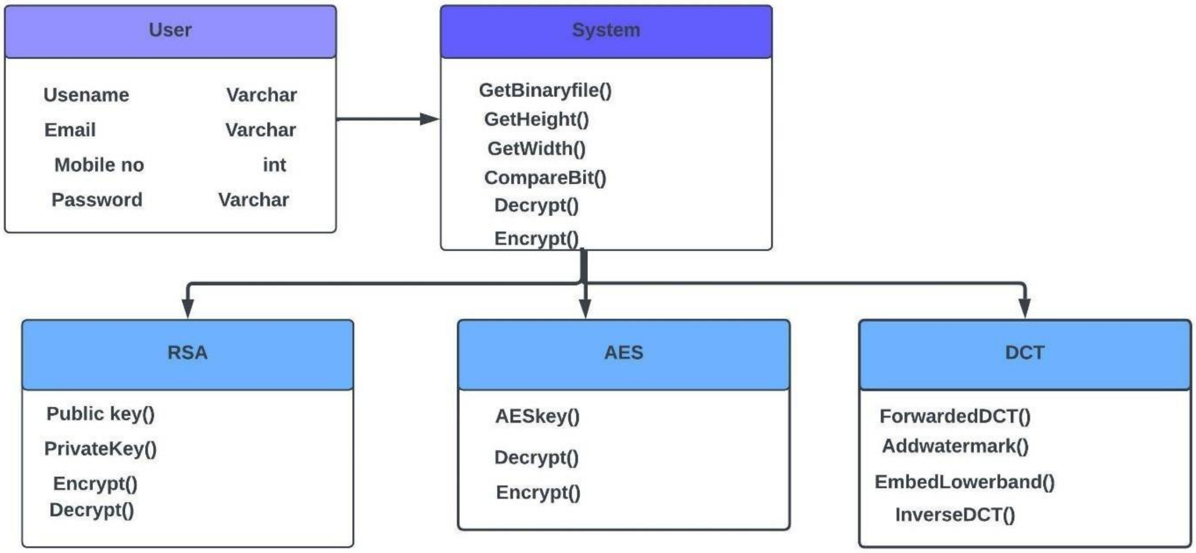
2.2.2.1 Product Perspective

For security purpose we take input as an image which you want to watermark, then we will generate any random key with our logic. By using RSA encryption, we generate public key and private key to encrypt randomly generated key. After key generation we encrypt the watermark image by using RSA keys. After that we stored these data into our database. Then this newly formed image will be read and embedding into the original image. Then we have to detect the image for that we retrieve all the information regarding image from database. Then we decrypt the RSA private key to read that watermarked image, after decryption image and hidden watermark will be display. The proposed watermarking technique have been developed under the assumption that the noise attacks are happening in isolation and not simultaneously. The project can be extended in scenario where the noise attacks happen simultaneously. The proposed scheme is limited to only image watermarking. The future work can be extended to audio and video data. The proposed scheme is limited to only software. The future work can be extended to the realization of the software implementation and the subsequent hardware implementation. The proposed method of watermarking has been implemented to make the process of watermarking both robust and imperceptible. The encrypted watermark file share with the other users and other users download that file after the acceptance of consent form.

2.2.2.2 Product Features

The system must to be capable of carrying out the following tasks:

- Data is more secure than existing system.
- It isn't robust to common signal technique operations thence watermarks are often simply depleted because of signal processing attacks
- Good compression and better imperceptibility.
- Easily shared encrypted data to any recipient.
- Very fast and simple encryption and verification.



2.2.3 External Interface Requirements

2.2.3.1 User Interfaces

Function 1	**Login/Signup**
Input	Name, email address, and password of the user
Processing	Validate the given details and record the information into the database.
Output	Redirect to user's home page

Function 2	**Upload file**
Input	It takes input by user as file and watermark in it.
Processing	Apply encryption algorithm and store metadata in database.
Output	Get encrypted file with watermark added in it.

Function 3	**Share file**
Input	It takes input as file and receiver name.
Processing	Shares all decryption info to the receiver.
Output	File shared

Function 4	**Download file**
Input	It take input as file and encryption key.
Processing	It decrypts the file and extract watermark from file.
Output	Display watermark.

1.2.3.2 Hardware Interfaces

- Processor: Intel Core i3 or more.
- RAM: 4GB or more.
- Hard disk: 250 GB or more.

1.2.3.3 Software Interfaces

- Operating System: Windows 10, 7, 8.
- Python.

- Anaconda.
- Spyder, Jupiter notebook, Flask.
- MYSQL.
- React

Functional Requirements:

1. In making mental demonstrations a purposeful premium describes a performance of an item group.

2. In its section a performance is depicted as a lot of information sources the lead and yields see together programming conscious prerequisites besides calculations, particular nuances data the board and cooperation.

3. Elective express rationale that format what a structure needs to make a few bucks' activity necessities depicting the entirety of the cases anyplace.

4. The system uses the deliberate prerequisites region unit found getting utilized cases deliberate prerequisites area unit maintained by non-utilitarian necessities similarly referenced as quality conditions.

5. Quality conditions that power necessities on the orchestrate or execution like execution prerequisites security or dependability by an enormous purposeful prerequisites' domain unit conveyed inside.

6. The sort structure should be constrained to attempt to however non-utilitarian prerequisites district unit systems are found for discipline.

7.purposeful necessities is elucidated inside the structure style they found for discipline non-utilitarian necessities is clarified inside the system organize as represented in prerequisites arranging.

8. Purposeful prerequisites show explicit delayed consequences of a system that may be separated from non-utilitarian prerequisites that affirm by and monstrous characteristics like cost and light-mindedness purposeful necessities.

9. drive the gear mastermind of a framework, though non-useful necessities drive the specialized plan of a framework.

2.2.4 Non-functional Requirements

1. In frameworks designing and wishes designing a non-utilitarian interest may be a necessity that determines models.

2. Which will be utilized to choose the activity of a framework as opposed to explicit practices that may be diverged from helpful requirements that layout explicit conduct or capacities the organization carrying out helpful requirements is intricate inside the framework style the mastermind executing non-practical.

3. Requirements are intricate inside the framework plan as a rule valuable necessities diagram.

4. What a framework should embrace and do though non-utilitarian requirements layout anyway a framework should be valuable requirements square measure commonly inside.

5. Such a framework will do though non-utilitarian necessities square measure framework will be non-utilitarian requirements.

6. Square measure generally alluded to as characteristics of a framework elective terms for non-useful necessities square measure imperatives quality ascribes quality objectives nature of administration prerequisites and non-social prerequisites

2.2.4.1 Performance Requirements

It can be seen that compared to traditional approaches, the performance of the proposed method is better in terms of robustness and PSNR according to the achieved simulation results. The performance of the proposed mechanism shows the maximum level of robustness and imperceptibility. Thus, compared to the existing approaches, the performance of the proposed approach is shown to be better. AES-192 was used to encrypt the critical information area to improve the security issue. It can be seen that in terms of security, insensitivity and robustness, the performance of the proposed mechanism is better. In various signal processing and geometric attacks, the proposed technique is applied to test the performance level and verify it. It can be seen that compared to the existing approaches, the performance of the proposed technique is better in terms of robustness and invisibility.

The performance is better, providing about 25% improvement for JPEG2000 compression and about 40% improvement for common filtering attacks. Greater robustness, high security and insensitivity. The reliability of this technique is better. It can be seen that according to the simulation results, the proposed approach achieves good invisibility, robustness, and capacity. This proposed approach also effectively resists commonly used image processing and combination attacks. For medical watermarking imaging, it is strongly recommended to provide a HCDH solution, as image quality is possibly preserved here by ensuring that CADx systems do not face distortion.

2.2.4.2 Safety Requirements

The watermarked multimedia data authentication of the proposed scheme (which is the main contribution of this thesis) is public; its safety depends on the robustness of the underlying RSA algorithm. The main advantages of this approach were demonstrated for some use cases. In order to ensure the overall safety of the communication, real-time authentication is employed during the transmission. Digital watermarking provides an alternative approach to ensure the safety of multimedia data during transmission in openly accessible channels. We can find that their security depends heavily on the safety of removable/non-removable smart cards issued by the telecommunication/mobile commerce providers The safety of static multimedia data can be inspected according to the
Following four aspects:

Storage: Is the data centrally stored, or dispersed?

Vulnerability: How robustness is the data against to theft or abuse?

Confidence/Authenticity: What constitutes authentic information? Can that information be tampered with?

Linking: Will the multimedia data be linked to other information, e.g., about originating and/or consuming party?

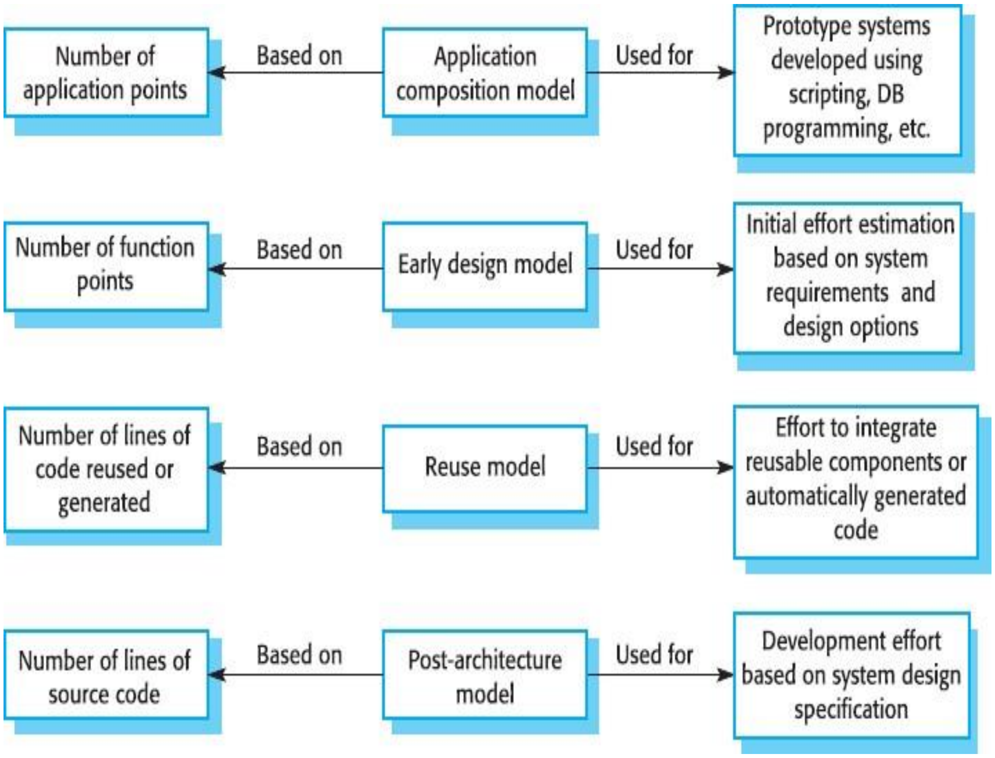
2.2.4.3 Security Requirements

In network environments, the security of multimedia data can be explored According to two points of view - static data security and dynamic data security Communication.

Fragile digital watermarking provides an alternative approach to ensuring security multimedia data during transmission on freely accessible channels. That is, digital watermarks can be generated by reference to originator, recipient, unique information serial number and time stamps. These watermarks are then embedded in multimedia data to ensure its integrity and source-of-origin authentication without degrading the overall level the quality of transmitted multimedia data.

In the real world, VoIP systems can suffer from many kinds of security threats. This is caused by the openness of VoIP implementations, as most VoIP is run in the public domain accessible networks. Hackers can attack the calling server, attack the operating system, inject a virus into VoIP phone endpoints and even perform DoS attacks on them signalling systems. In this work, we will focus only on the security of multimedia content data. RTP confidentiality can be implemented using encryption and encryption can be done at the application level or at the IP level. Perkins analysed advantages and disadvantages of both options in his recently published book [2.8]. RTP the standard does not provide integrity protection or source source authentication packetized data itself. So the creators of the RTP specification leave it blank on purpose different developers can implement security methods according to their needs. Most the authentication implementation is compliant with secure RTP or using IPsec.

2.3 Cost Analysis



Number of application points
Based on
Application composition model
Used for
Prototype systems developed using scripting, DB programming, etc.
Number of function points
Based on
Early design model
Used for
Initial effort estimation based on system requirements and design options
Number of lines of code reused or generated
Based on
Reuse model
Used for
Effort to integrate reusable components or automatically generated code
Number of lines of source code
Based on
Post-architecture model
Used for
Development effort based on system design specification

2.4 Risk Analysis

Notwithstanding the obstacle strategies utilized potential perils is in a position to which can arise inside or outside the affiliation ought to be assessed regardless of the established truth that the exact arrangement of expected catastrophes or their after results district unit delayed to outlined its valuable to play out an intensive risk investigation of all threats which can sensibly happen to the relationship in spite of the kind of peril the goals of business recuperating emerging with locale unit to validate the security of buyers workers and particular representatives eventually of and following a breakdown the overall probability of a failure happening should be settled things to appear at in urgent the probability of a particular breakdown should be constrained to represent in any case not be confined to field characteristic study of the planet closeness to indispensable wellsprings of power streams and air terminals level of receptiveness to workplaces inside the affiliation history of local service organizations in giving persistent kinds of help history of the spaces condition to standard risks neighbourhood to imperative turnpikes that vehicle bold waste and combustible item. Potential openings could even be delegated regular, specialized, or human dangers. Models include:

- Characteristic Threats: inner flooding, outer flooding, interior hearth, outside chimney, seismic movement, high breezes, snow and ice storms, emission, cyclone, typhoon, pandemic, torrent, hurricane.
- Specialized Threats: power disappointment/variance, warming, ventilation or air con disappointment, glitch or disappointment of hardware, disappointment of framework code, disappointment of use code, broadcast communications disappointment, gas spills, interchanges disappointment, atomic aftermath.
- Human Threats: robbery, bomb dangers, theft, blackmail, thievery, defacing, psychological warfare, common problem, synthetic spill, damage, blast, war, natural pollution, radiation tainting, perilous waste, vehicle crash, airdrome nearness, strike (Internal/External), PC wrongdoing.

All areas and offices should be encased inside the peril investigation maybe than attempting to sort out real prospects of every fiasco an overall relative game plan of high medium and low is utilized at first to distinguish the probability of the danger happening the possibility investigation also need to affirm the effect of such a likely danger on various capacities or offices inside the association a risk analysis type discovered here pdf format will work with the strategy the capacities or divisions can shift by kind of association the arranging strategy ought to set up and live the possibility of every single expected danger and in this way the effect on the association if that danger happened to attempt to this each division should be investigated severally in spite of the fact that the chief framework is furthermore the one most serious danger it isn't the solitary vital concern indeed even inside the first programmed associations a few offices will not be handled or programmed inside the smallest degree in totally programmed divisions essential records stay outside the framework as lawful records pc information programming bundle hang on diskettes or supporting documentation for data section the effect is evaluated as 0 no effect or break in tasks 1 noticeable effect break in activities for as long as eight hours 2 mischief to instrumentation and additionally offices break in tasks for eight 48 hours 3 major damage to the instrumentation or potentially offices break in tasks for every 48 hours all base camp or potentially pc focus capacities ought to be resettled bound suspicions is also important to consistently apply evaluations to every possible danger

Following are run of the mill suspicions which can be utilized all through the peril evaluation measure:

1. In spite of the fact that affect evaluations may fluctuate somewhere in the range of one and three for any office given a particular situation, appraisals applied should reflect expected, apparent or anticipated effect on each space.

2. each potential danger ought to be thought to be "confined" to the force being appraised.

3. Despite the fact that one potential danger could lead on to an uncommon likely danger (e.g., a typhoon may bring forth cyclones), no aftereffect ought to be expected.

4. On the off chance that the consequences of the danger wouldn't warrant development to a substitute site(s), the effect ought to be appraised no over a "2."

5. The threat evaluation should be performed by the force. to gauge the likely dangers, a weighted reason rating framework is utilized.

METHOLOGY ADOPTED

3.1 Investigative Techniques

Image encoding:

The actual image is in AN encompassed sample which the pixel values are inside [0, 255], and intend the degrees of rows and columns as N1 and N2 and consequently the pixel wide variety as (N=N1 X N2). The watermark is embedded into the preliminary input image.

Encrypted Image Encoding:

The secret information became entered in textual content layout into the watermarked picture. If the key-word became matched, then best its movements to successive step. i.e., reconstruction, in any other case if the key-word doesn't match it ends in the error.

Image Watermark Extraction:

With the watermark embedded image and consequently the secret key (key-word), a receiver will regenerate the primary information of the preliminary image, and consequently the decision of the reconstructed image is based on the quantity of stage of watermark.

Frequency Domain Watermarking:

In frequency domain the watermark is embedded inside the spectral consistent of the image. The generally used algorithms in frequency domain are the discrete cosine transform (DCT), discrete Fourier transform (DFT), and discrete wavelet transform (DWT). The reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients.

Discrete cosine transforms (DCT):

DCT form of a Fourier rework, it represents data in phrases of frequency area rather than an amplitude area. this will be useful due to that corresponds extra to the technique people recognize light, so the 1/2 of that do not appear to be perceived may be regarded and thrown away. DCT based watermarking strategies are robust as compared to spatial area strategies. Such algorithms are robust in opposition to straightforward image technique operations like low pass filtering, brightness and difference adjustment, blurring etc. However, {they're} difficult to put in force and are computationally dearer. At steady time they may be susceptible in opposition to geometric attacks like rotation, scaling, cropping etc. DCT domain watermarking can be labelled into global DCT watermarking and Block based DCT watermarking. Embedding in the perceptually great slice of the image has its very own blessings due to maximum compression schemes cast off the perceptually insignificant part of the image. Steps in DCT Block based Watermarking algorithmic rule

1) Segment the image into non-overlapping blocks of 8x8.
2) Apply ahead DCT to each of these blocks
3) Apply a few block preference criteria (e.g., HVS).
4) Apply steady preference criteria (e.g., highest)
5) Embed watermark with the aid of using editing the selected coefficients.
6) Apply inverse DCT remodel on each block.

Discrete wavelet transforms (DWT):

Wavelet transform can be a contemporary-day approach frequently hired in digital image process, compression, watermarking etc. The transforms are supported little waves, called wavelet, of various frequency and limited period. The wavelet transform decomposes the image into three spatial directions, i.e., horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic residences of HVS loads of exactly. Magnitude of DWT coefficients is bigger inside the lowest bands (LL) at each stage of decomposition and is smaller for opportunity bands (HH, LH, and HL). The discrete wavelet transform (DWT) is currently employed in a terrific shape of sign manner programs, like in audio and video compression, elimination of noise in audio, and consequently the simulation of Wi-Fi antenna distribution. Wavelets have their power centred in time and are well matched for the evaluation of transient, time-various alerts. Since maximum of the actual lifestyles alerts encountered are time various in nature, the wavelet rework fits numerous programs alright. One among the maximum demanding situations of the watermarking disadvantage is to reap a better alternate among power and sensibility. Power is frequently accomplished via way of means of growing the power of the embedded watermark, but the seen distortion could be gathered also. However, DWT is manner favoured because of it gives a coincident spatial localization and a frequency spread of the watermark a few of the host image. The essential plan of wonderful wavelet rework in picture technique is to multi-differentiated decompose the image into sub-picture of numerous spatial domain and freelance frequencies.

3.2 Proposed System: -

•For security purpose we take input as an image which you want to watermark, then we will generate any random key with our logic.

•By using RSA encryption, we generate public key and private key to encrypt randomly generated key.

•After key generation we encrypt the watermark image by using RSA keys. After that we stored these data into our database.

•Then this newly formed image will be read and embedding into the original image. Then we have to detect the image for that we retrieve all the information regarding image from database.

•Then we decrypt the RSA private key to read that watermarked image, after decryption image and hidden watermark will be display.

•The proposed watermarking technique have been developed under the assumption that the noise attacks are happening in isolation and not simultaneously. The project can be extended in scenario where the noise attacks happen simultaneously

•The proposed scheme is limited to only image watermarking. The future work can be extended to audio and video data.

•The proposed scheme is limited to only software. The future work can be extended to the realization of the software implementation and the subsequent hardware implementation.

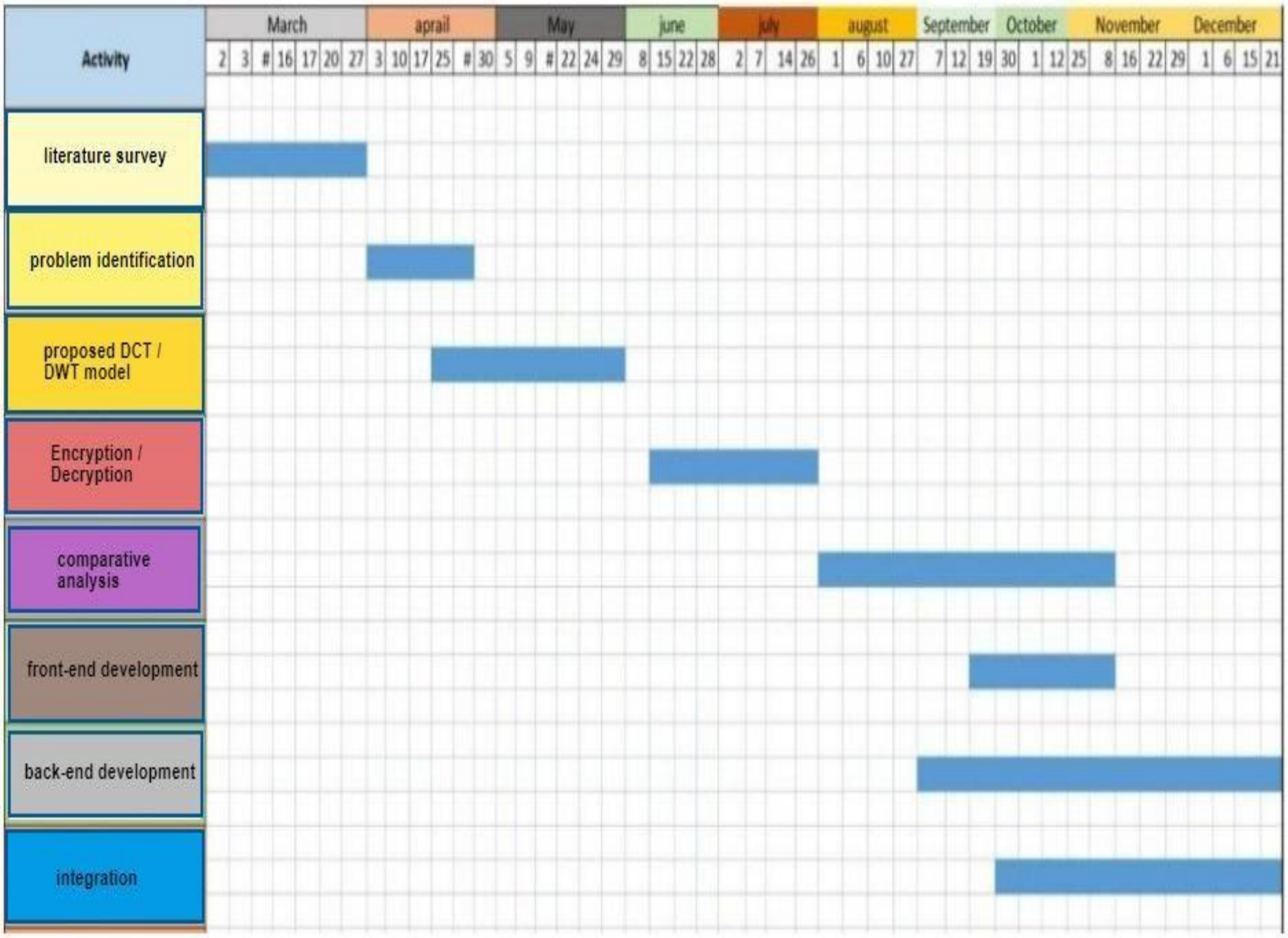
•The proposed method of watermarking has been implemented to make the process of watermarking both robust and imperceptible.

•The encrypted watermark file share with the other users and other users download that file after the acceptance of consent form.

Advantages of Proposed System:

1. Data is more secure than existing system.
2. It isn't robust to common signal technique operations thence watermarks are often simply depleted because of signal processing attacks
3. Good compression and better imperceptibility.
4. Easily shared encrypted data to any recipient.
5. Very fast and simple encryption and verification.

3.3 Work Breakdown Structure



3.4 Tools and Technology

1. Processor: Intel Core i3 or more.
2. RAM: 4GB or more.
3. Hard disk: 250 GB or more.
4. Operating System: Windows 10, 7, 8.
5. Python.
6. Anaconda.
7. Spyder, Jupiter notebook, Flask.
8. MYSQL.
9. React

DESIGN SPECIFICATIONS

4.1 System Architecture

System flowchart:

A stream diagram could even be a spread of characterize that addresses a standard or strategy showing the proposes that as boxes of shifted types and their solicitation by interfacing them with bolts this depict outline shows a response for a given recoil procedure exercises territory unit depict in these compartments and bolts rather there calm by the sequencing of undertakings flowcharts region unit used in taking apart emerging with documenting or managing the lone way or program in a few fields

Arrows

Showing "stream of the board" partner bolt returning from one picture and finishing at another picture addresses that control passes to the picture the bolt focuses to. the street for the bolt is strong or broken. The significance of the bolt with broken line could differ from one stream diagram to an uncommon and ought to be laid out inside the legend.

Generic processing steps

Addressed as square shapes Examples: "Add one to X"; "supplant known part"; "save changes" or comparable.

Subroutines

Tended to as square shapes with twofold influenced vertical edges these are adjusted show tangled connection steps which may be included during an exceptionally particular language model live records one bundle may require various clear area centres or leave streams see co day by day follow forward therefore these are showed up as checked wells inside the quadrangle and subsequently the leaders bolt interface with these wells

Input/output

Tended to as a quadrilateral Examples: Get X from the customer; show X Prepare prohibitive drawn as a two-dimensional figure Shows exercises that don't have any outcome close to fitting a cost for a later unforeseen or elective development (see under).

Conditional or decision

Tended to as a gem rhombus showing wherever a decision is fundamental typically a certifiable request or genuine bogus check the prohibitive picture is whimsical during this its two bolts start of it to a great extent from total base explanation and right explanation one adore affirmed or valid and one love no or bogus the bolts had the opportunity to be named more than two bolts may moreover be utilized in any case this is regularly frequently regularly frequently generally a simple marker that a tangled choice is being taken inside that case its having the possibility to should be isolated any or replaced with the pre-portrayed live picture

Junction symbol

For the most part portrayed with a dark mass showing any place different administration streams meet during one leave stream an intersection picture can have very one bolt returning into it anyway only one going out in direct cases one may simply have partner bolt reason to an exceptional bolt all things being equal these are supportive to address partner monotonous strategy what in designing is named a circle a circle may for instance incorporate a connective any place the board first enters measure steps a contingent with one bolt leaving the circle and one returning to the connective for added clearness where 2 lines incidentally cross inside the drawing one through and through them could even be drawn with minimal plane figure over the other showing that no intersection is assumed

Labelled connectors

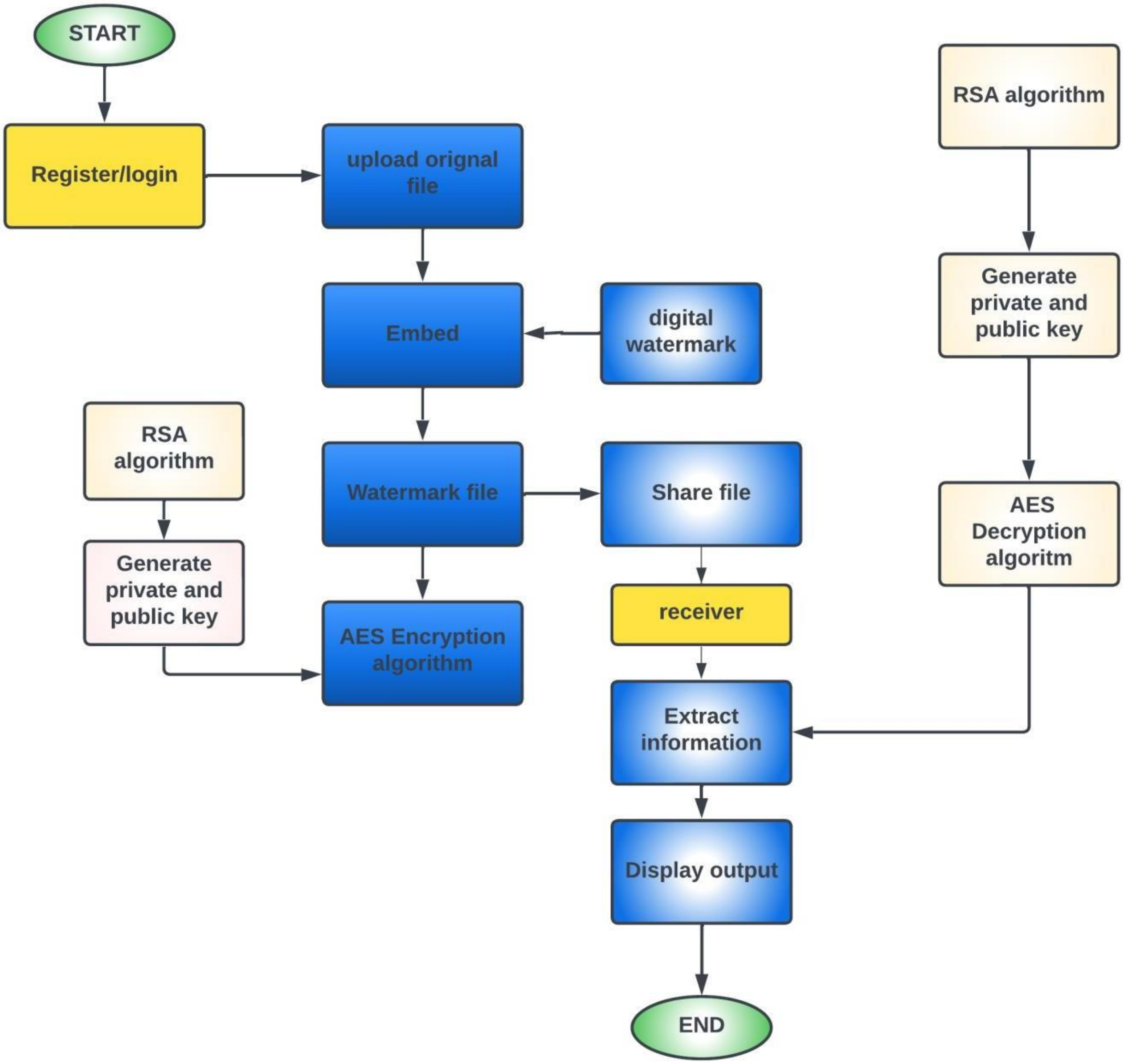
Addressed by A distinctive mark inside a circle. marked connectors are used in cutting edge or multi-sheet charts to fill in for bolts. for each name, the "surge" connective ought to be unmistakable, anyway there's additionally such a "inflow" connectors. During this case, an intersection up to the hustle stream is known.

Concurrency symbol

Addressed by a twofold cross-over line with any scope of section and leave bolts These images are utilized at whatever point 2 or extra administration streams ought to work at a comparable time. The leave streams are enacted at an identical time once the entirety of the passage streams have arrived at the simultaneousness picture. A simultaneous picture with one section stream could likewise be a fork; one with one live stream could likewise be a piece of. it is fundamental to make sure to stay these associations consistent so as. All cycles need to move from prime to base and left to right.

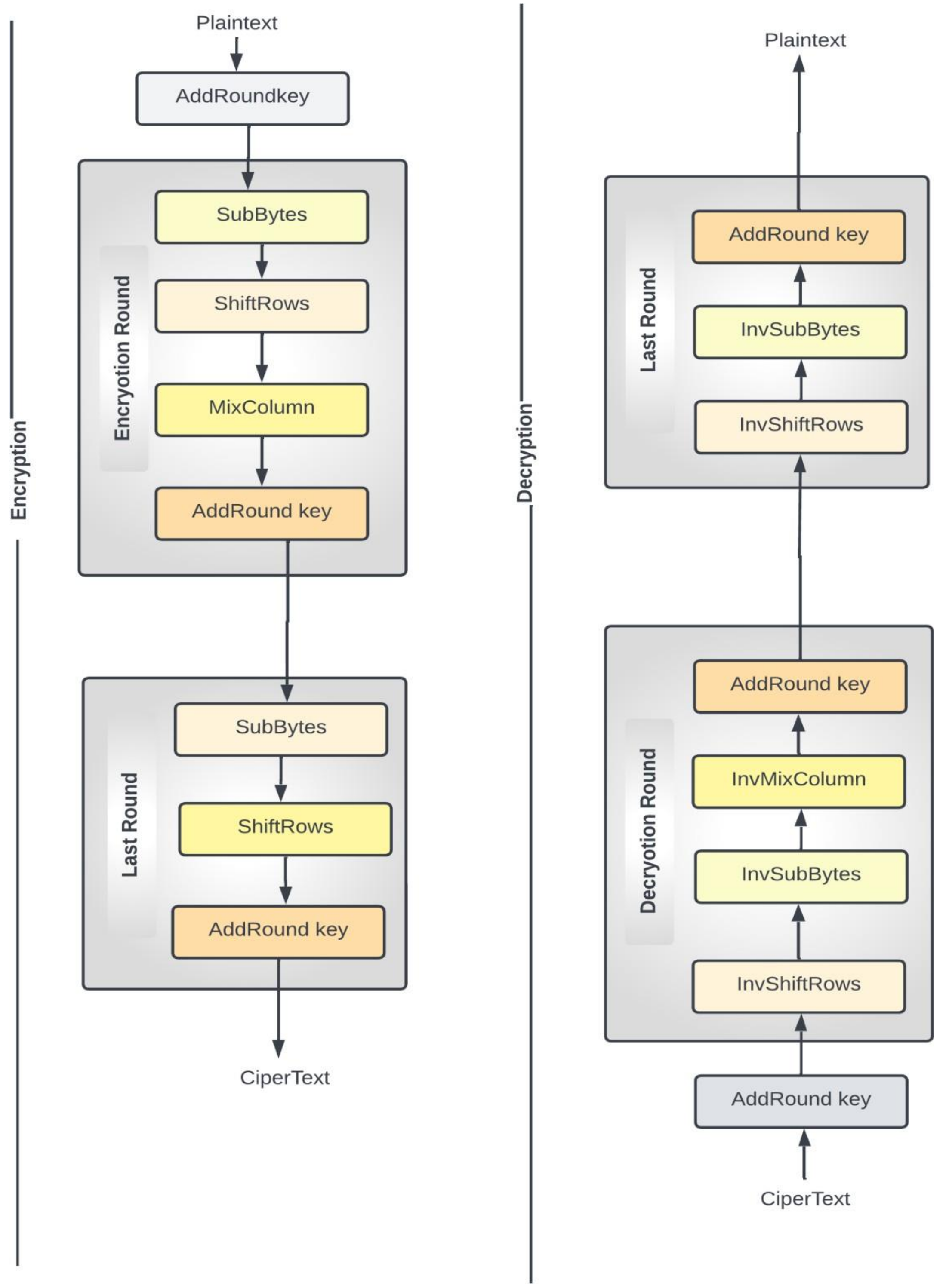
4.2 User Interface Diagrams

Flow chart



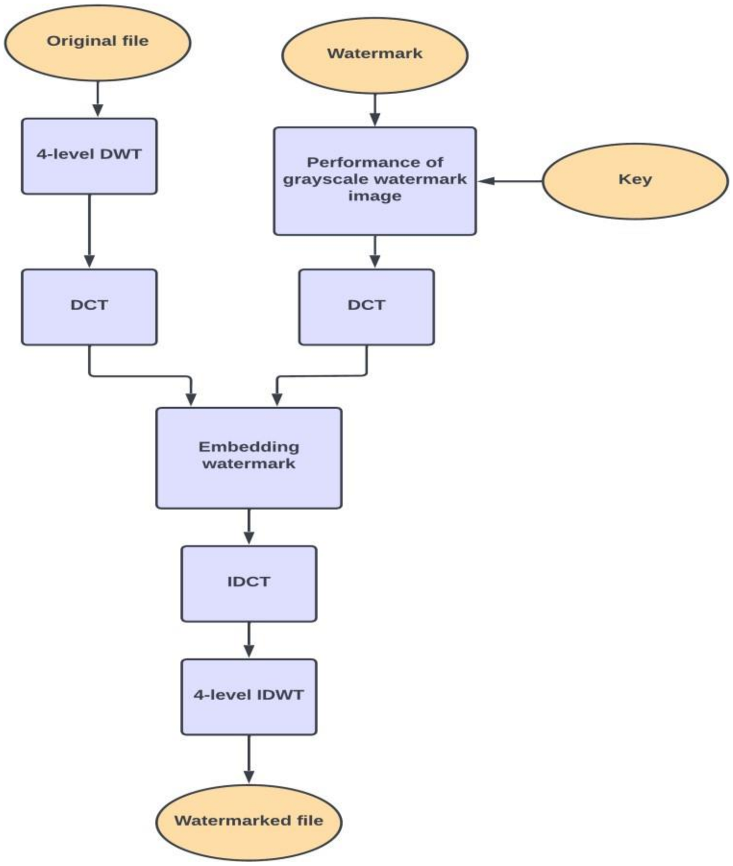
The above diagram, is brief description of the how the project flow from start to end. It has Login and registration to the user for authentication purpose. After successfully login User can upload file, share file, download file with all encryption algorithm. The shared file can download with proper authenticate details only.

AES Flow chart



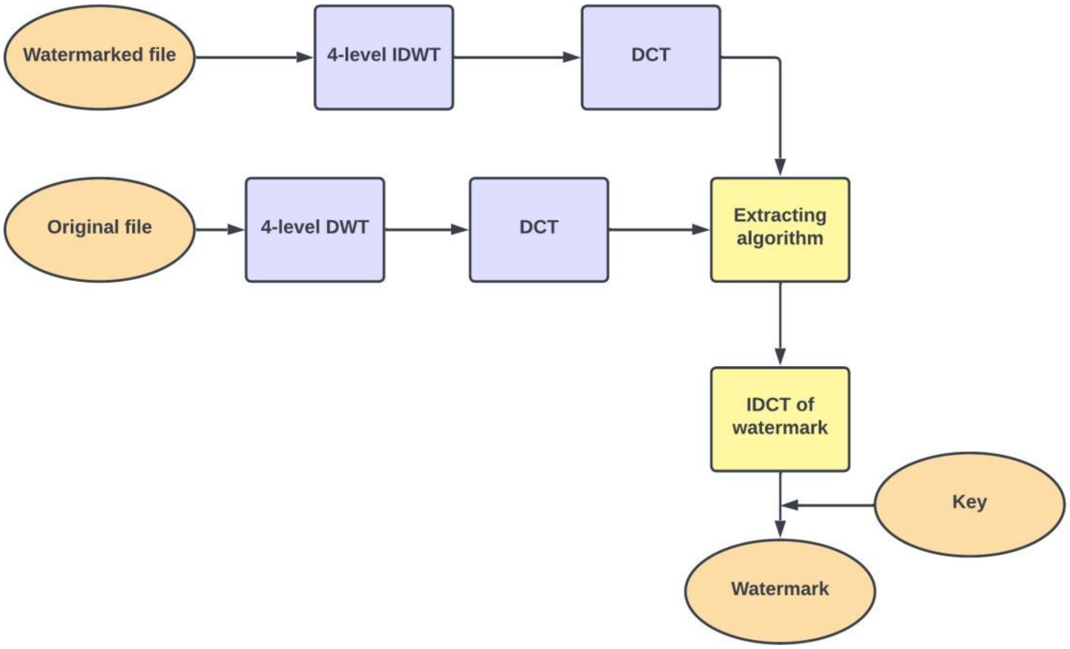
The above diagram, is brief description of the how the AES algorithm works. It has basically 2 rounds for encryption and same for decryption. It has 1 round i.e., encryption round and last round for converting plain text to cipher text and vies versa.

Watermark embedding Flow chart



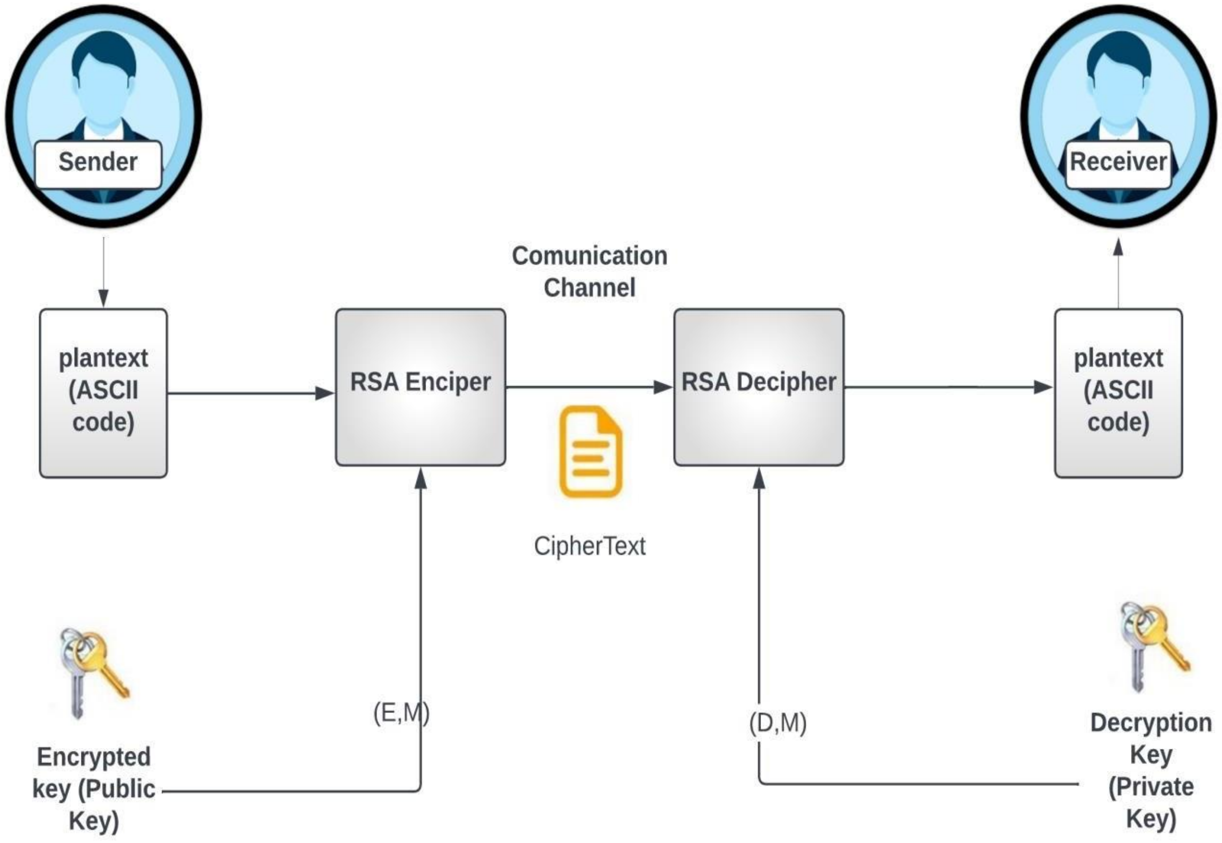
The above diagram, is brief description of watermark embedding technique. It converts original file to watermark file. It converts both file at the DCT level 4 and then embedding each other to get the one Watermark file.

Watermark extraction



The above diagram, is brief description of watermark extraction technique. It converts original file to watermark file. It converts both file at the 4 level of IDWT and then extract watermark from the file.

RSA



RSA algorithmic program is asymmetric cryptography algorithmic program. Asymmetric without a doubt means that it really works on 2 completely unique keys i.e., Public Key and Private Key. Due to the fact the name describes that the overall public key's given to each person private key's saved private. An instance of asymmetric cryptography:

1) A customer (as an instance browser) sends its public key to the server and requests for some records.

2) The server encrypts the records the usage of client’s public key and sends the encrypted data.

3) Customer gets these records and decrypts it.

4.3 Design Level Diagrams

SYSTEM IMPLEMENTATION

Execution incorporates each one of those exercises that end up changing over from the new framework to the new. The new framework comprises of manual tasks, that is worked terribly very surprising way from the arranged new framework. a precise execution is essential to supply a dependable framework to fulfil the prerequisites of the associations. partner inappropriate establishment could affect the achievement of the prepared framework.

IMPLEMENTATION METHODS:

There are a few different ways for taking care of the execution and furthermore the subsequent transformation from the past to the new prepared framework.

The chief secure method for transformation from the past framework to the new framework is to run the past and new framework in equal. During this methodology, a private may work inside the manual more seasoned cycle framework still as start employable the new prepared framework. This framework offers high security, as a consequence of in spite of the fact that there is a defect inside the handled framework, we'll rely upon the manual framework. Nonetheless, the value for keeping 2 frameworks in equal is unfathomably high. This exceeds its benefits.

Another unexpected procedure may be a prompt cut over from this manual framework to the prepared framework. The correction is moreover at stretches each week or at spans on an everyday basis. There aren't any equal exercises. Notwithstanding, there is no cure only in the event of a drag. This procedure needs cautious emerging with.

A working rendition of the framework can even be upheld in one neighbourhood of the association and furthermore the faculty are having the opportunity to steer the framework and changes are made as and once required. anyway, this framework might be a more modest sum liked because of the deficiency of the entireness of the framework.

IMPLEMENTATION PLAN:

The execution orchestrate incorporates an outline of the relative multitude of exercises that must happen to carry out the new framework and to place it into activity. It recognizes the staff answerable for the exercises and readies a period outline for executing the framework. The execution orchestrates the subsequent stages.

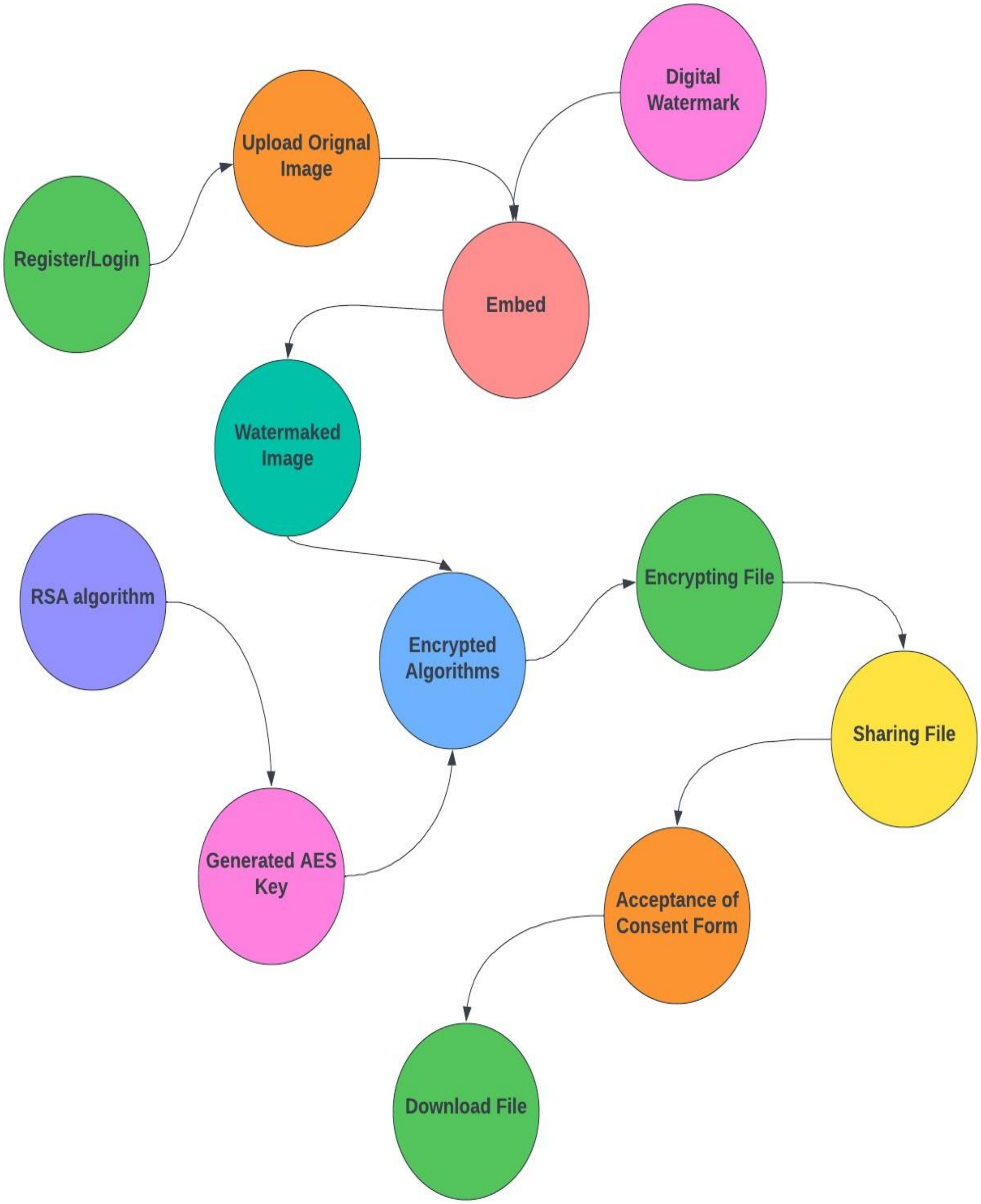
- Rundown all records required for execution.
- Recognize all data expected to make new documents all through the execution.
- Rundown every single new report and strategies that enter the new framework.

The execution orchestrate ought to expect achievable issues and will be prepared to manage them. the quality issues could even be missing records; blended data designs among current and documents, blunders in data interpretation, missing data and so forth

DFD (Data Flow Diagram)

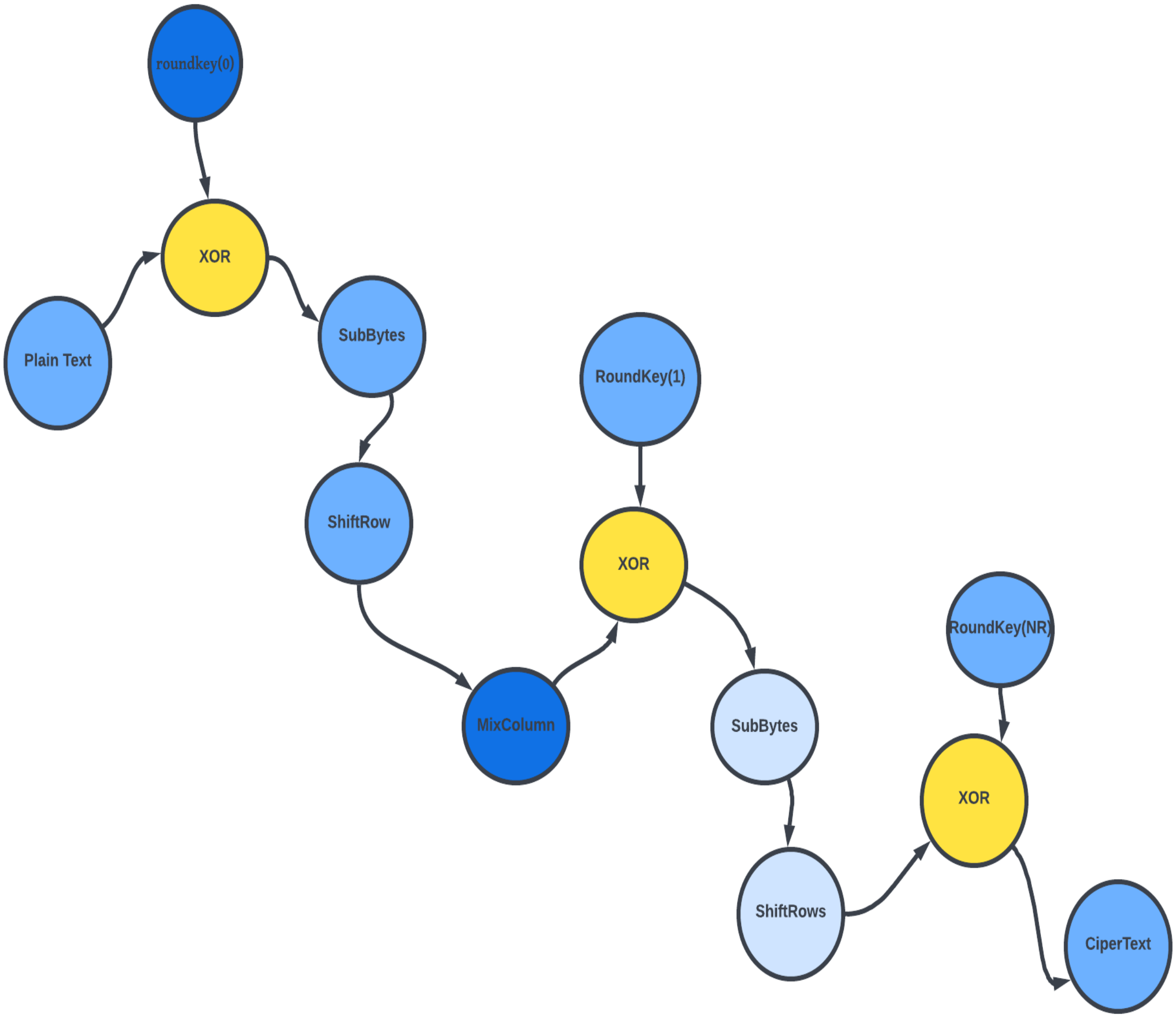
An information programming language did may be a graphical outline of the progression of information through associate in nursing framework an information programming language can likewise be utilized for the visual picture of information measure organized plan its ordinary apply for an architect to draw a setting level did first that shows the collaboration between the framework and out of entryways substances this setting level did is then detonated to implies extra detail of the framework being sculpturesque.

DFD level 0:



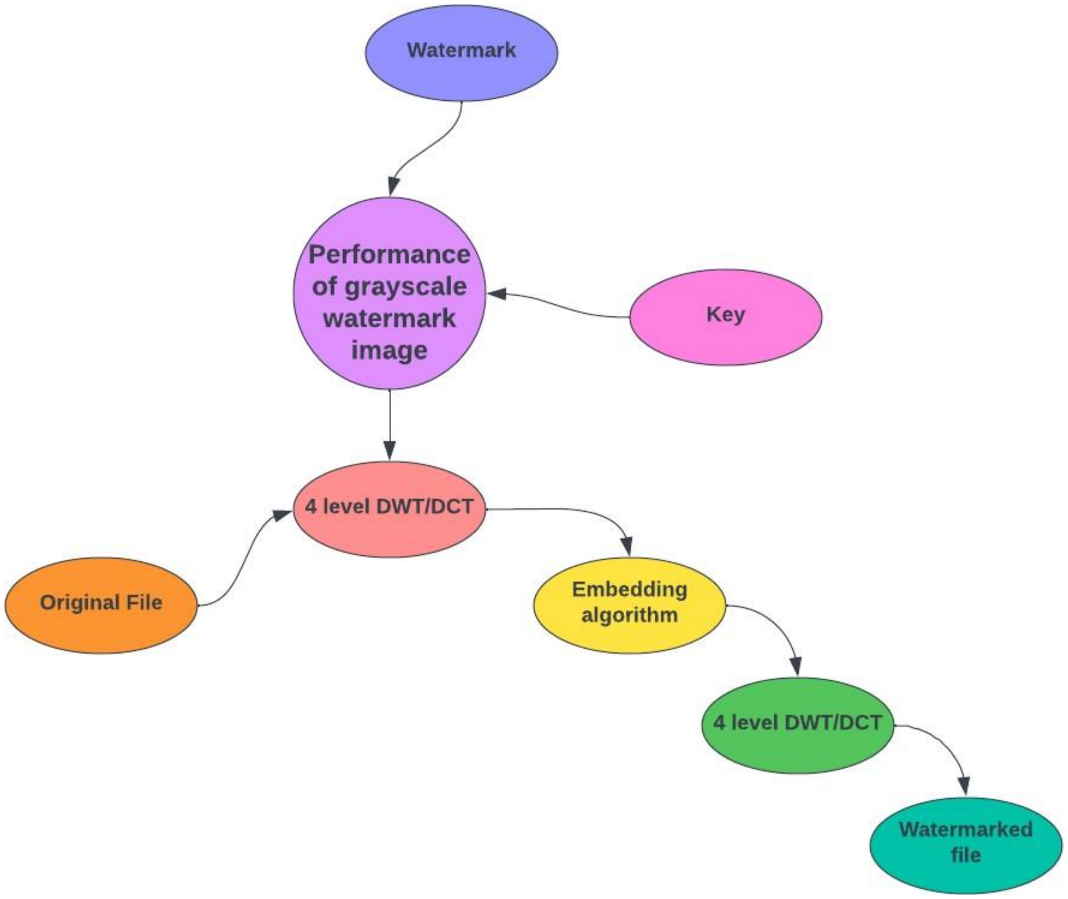
It’s first level of data flow diagram. It’s defined the data flow of project. After the file uploading the file first watermarked with DCT-DWT algorithm and watermark file gets encrypted with the AES algorithm and AES key encrypted with the RSA Public key and vice versa.

DFD level 1:



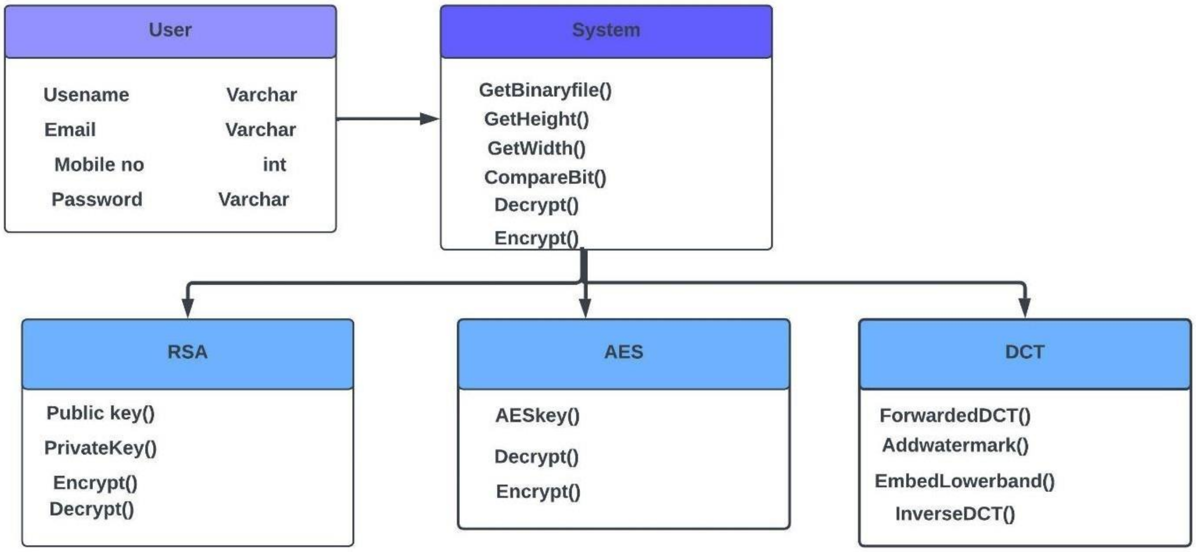
It’s second level of data flow diagram. It defined the data flow of AES algorithm.

DFD level 1:



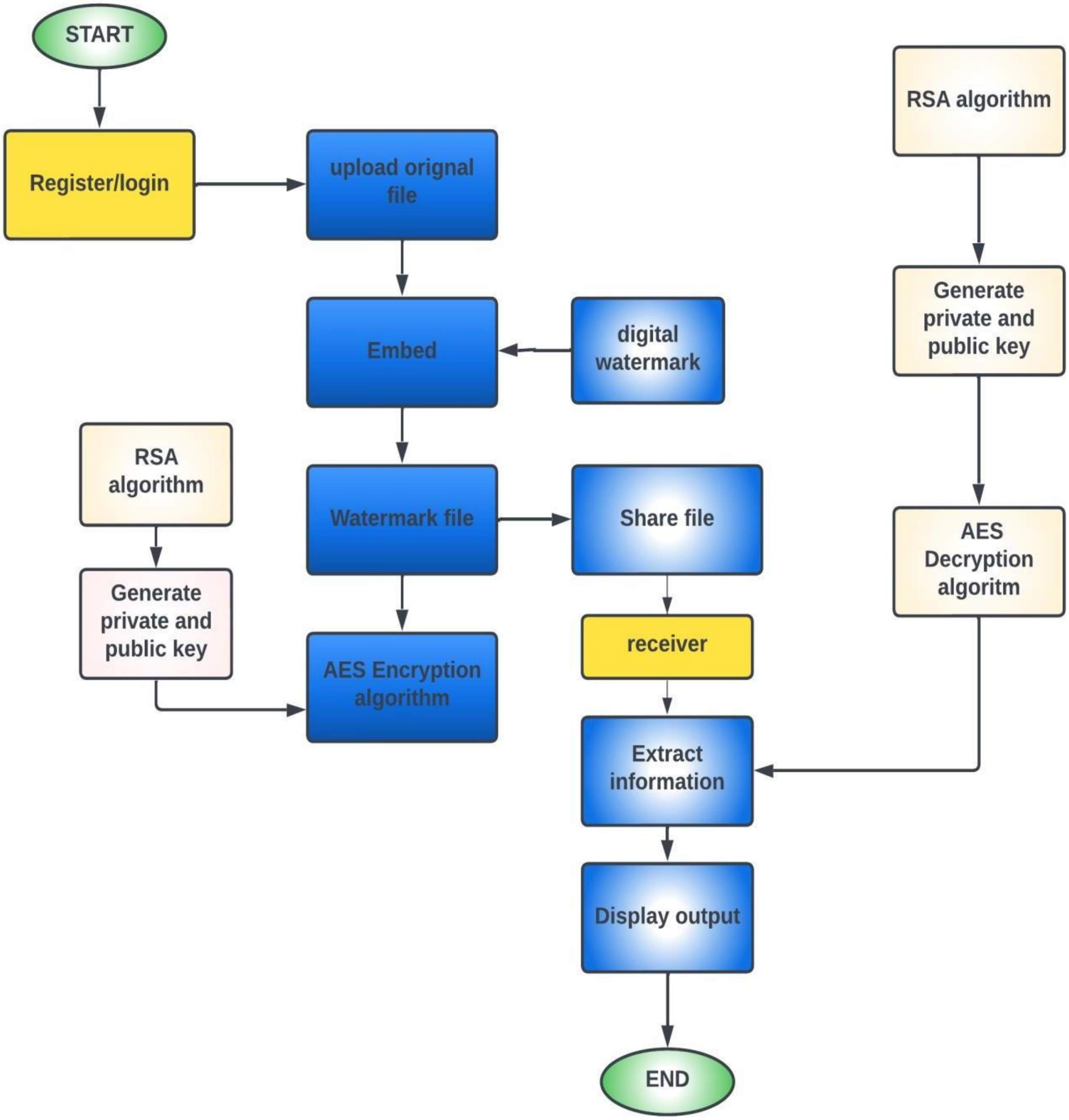
It’s last level of data flow diagram. It defines the data flow of DCT-DWT algorithm.

Class Diagram:



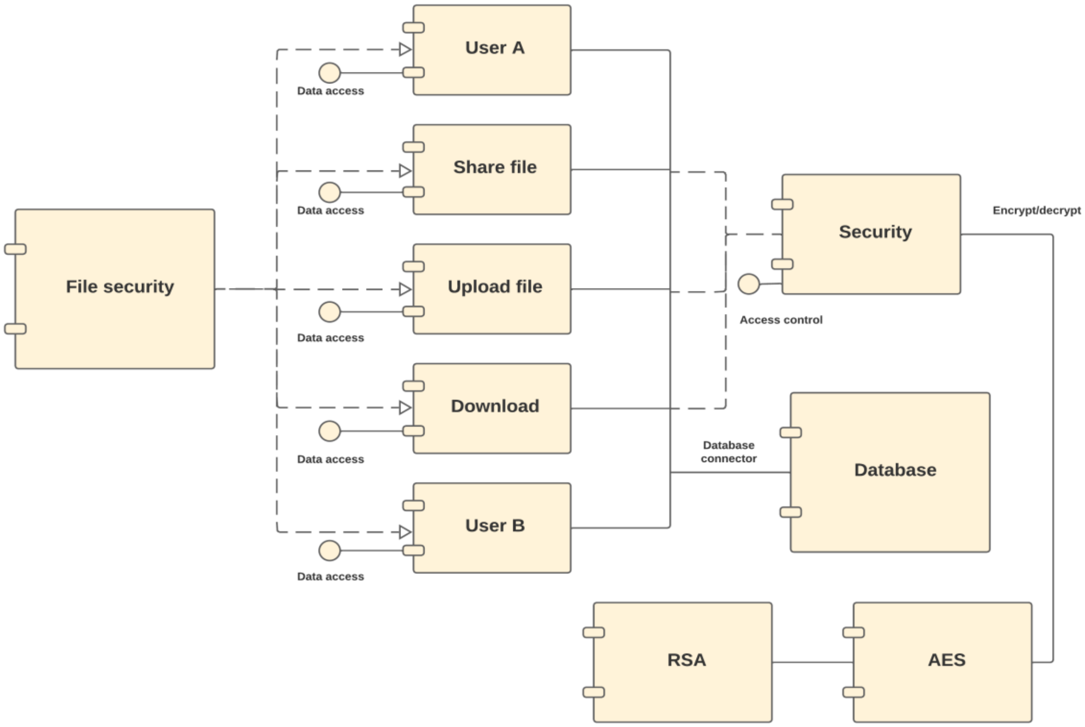
The above diagram, is brief description of the class of the project. It has the many classes like User, system and all algorithm. This all classes are interconnected with the system to perform the operations.

Activity Diagram:



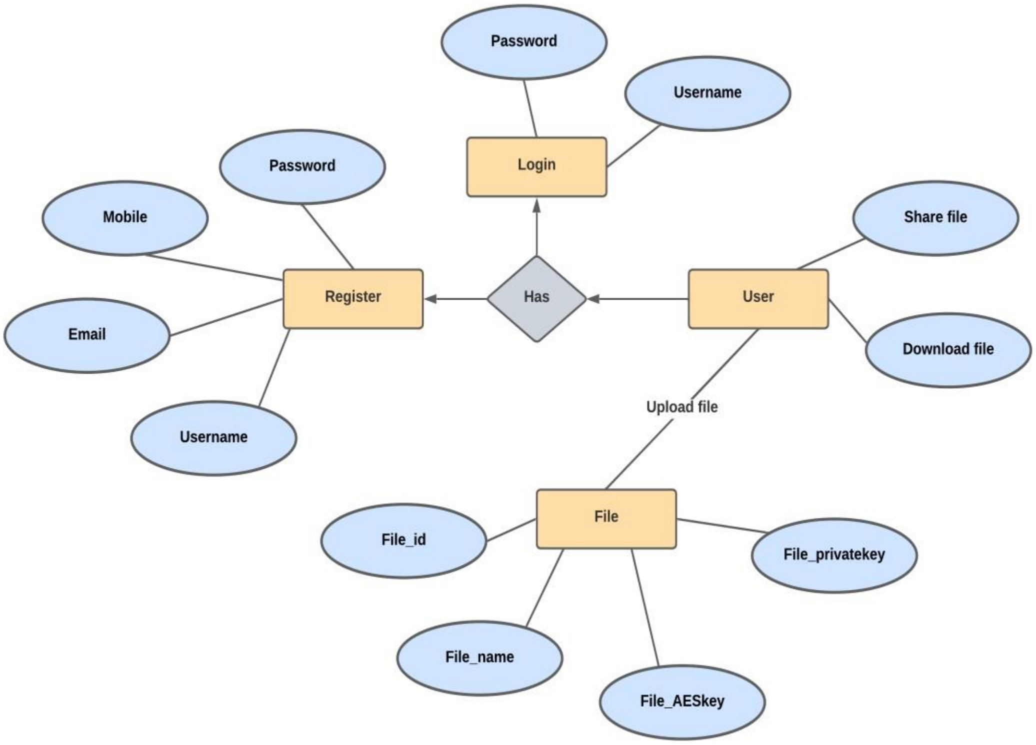
The above diagram, is brief description of the activities which performed in project. It has Login and registration to the user for authentication purpose. After successfully login User can upload file, share file, download file with all encryption algorithm. The shared file can download with proper authenticate details only.

Component diagram:



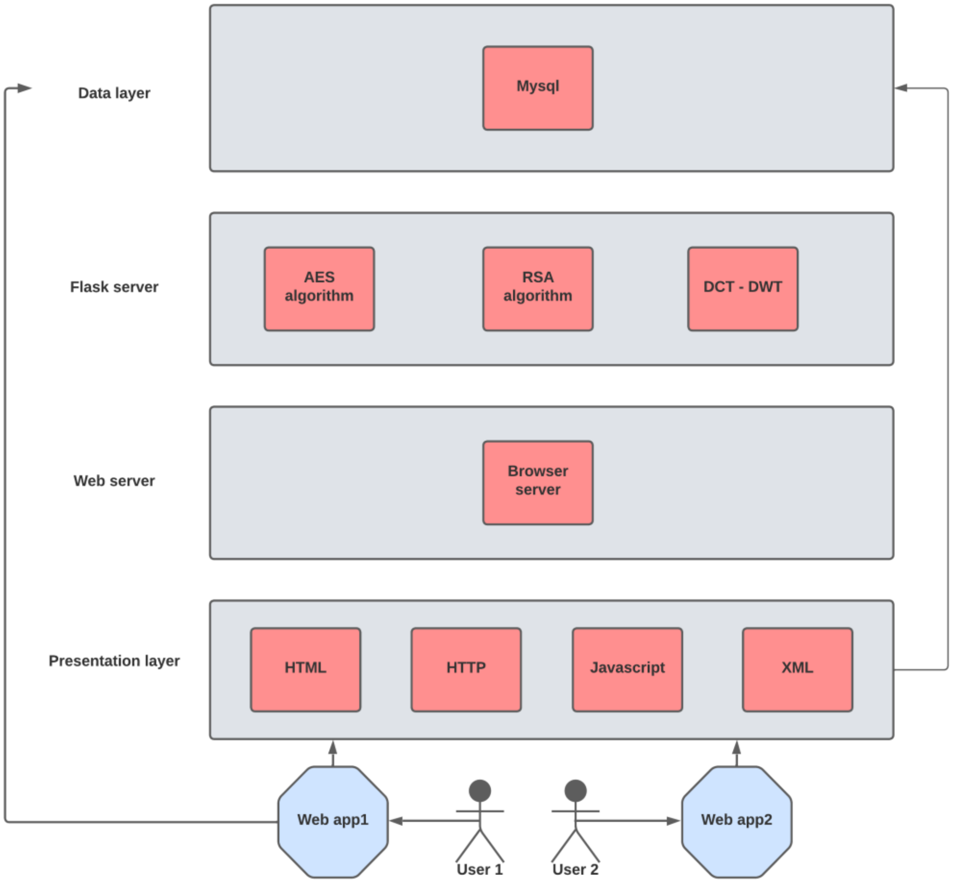
The above diagram, is brief description of the components which used in project. It has Login and registration component to the user for authentication purpose. Then we have database, AES and RSA components for encryption/decryption and storing purpose.

ER diagram:



The above diagram, is brief description of the Database management system. We have totally 3 tables for storing data for user details, uploading file and sharing file details. User has many entities like username password email and mobile number and also file has the entities like id file name, private key, AES key.

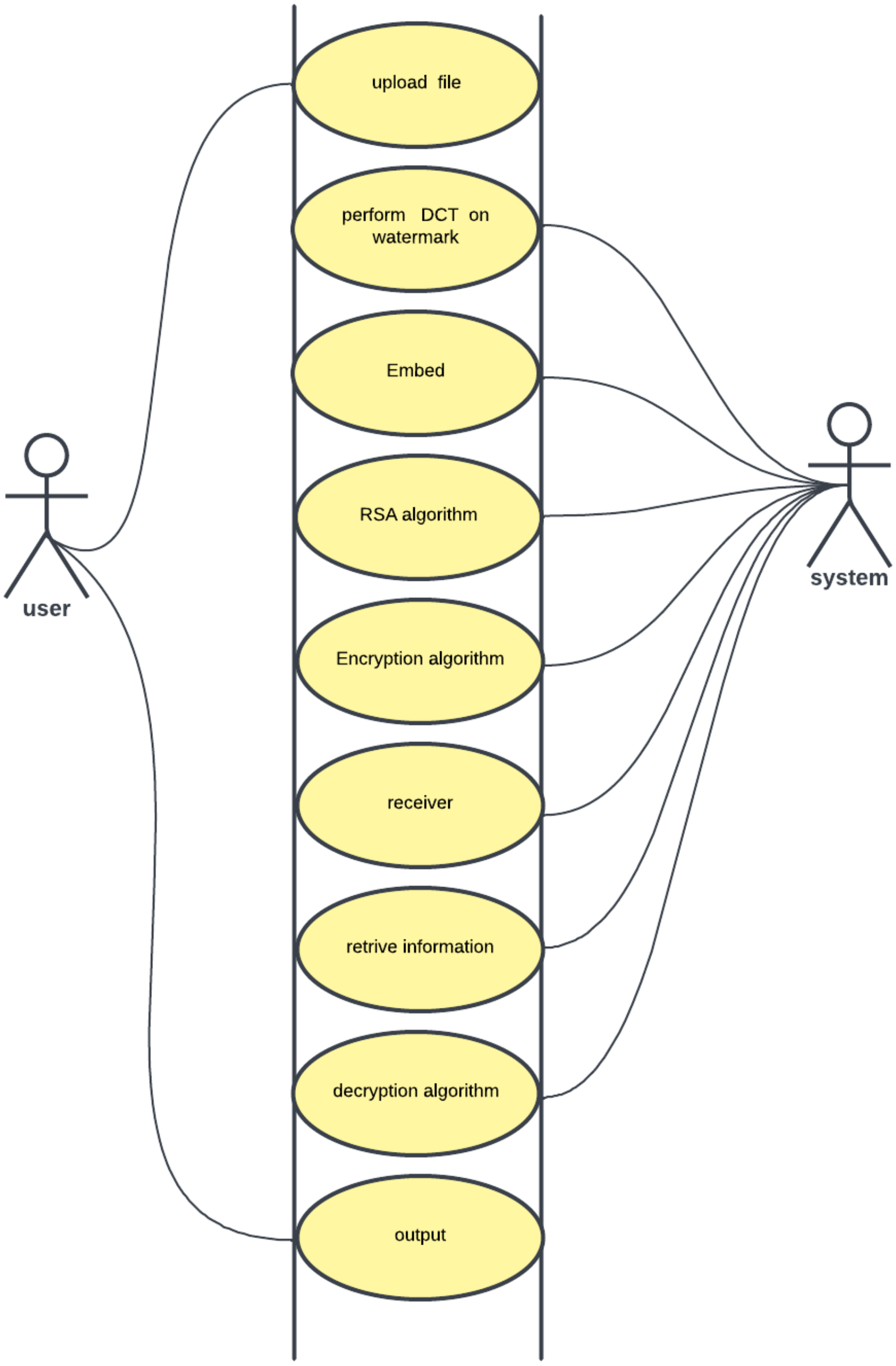
Architecture diagram:



The above diagram, is brief description of the Architecture which used in project. We totally have 4 architecture level vies. Each architecture has its own functions.

Use Case Diagram: -

The architecture for detecting the drowsiness of the driver is shown in the above figure. When the web camera is activated, the model that we trained using neural networks for this project loads the classifier, which reads the video stream of the driver using the web camera. This will continuously capture images of the facial characteristics of the driver from the video stream. Every image that is taken has a classifier applied at the backend that determines whether the driver's eyes were open or closed. The score starts rising as soon as the system recognises that the user has closed eyes. If the score rises above a predetermined threshold, it indicates that the person is sleepy since their eyes are closed, and the system sounds an alert to wake them up. This alarm continuously rings until the driver does not wake up and the system recognizes the eyes of the driver to be open. When the system captures the open eyes, the score decreases and alarm stops ringing.


upload file
perform DCT on watermark
Embed
RSA algorithm
Encryption algorithm
receiver
retrive information
decryption algorithm
output
user
system

CONCLUSION AND FUTURE SCOPE

5.1 Work Accomplished

1. Sehaj Kapoor [Team Leader]:

- Working on various encryption algorithm for secured transfer of data.
- Work on Web Development
- Use-case diagram, Activity diagram, Architecture diagram
- Worked on consent management form.

2. Yash Aggarwal:

- Working on various encryption algorithm for secured transfer of data.
- Work on Web Development
- Worked on research papers.
- Deploy a web app for the model.

3. Pratham Kapoor:

- Working over various digital watermarking algorithms including both visible & invisible watermarking.
- Work on Web Development
- Class diagram, DFD diagrams.
- Worked on consent management form.

4. Vaibhav:

- Prepare the Ghantt chart as per the work plan.
- Component Diagram, ER diagrams.
- Set the outcomes for the project.
- Work on web development.

5.2 Conclusions:

Digital watermarks that employ convolutional coding prove to be more robust to additive noise and JPEG compression when compared to the non-coding method. Surprisingly, the coding method appeared more vulnerable to image resizing. Perhaps more sophisticated method of image restoration are needed to improve detection. Even though the coding method improved the watermark detection under compression and additive noise, there is a significant gain in computation due to the complexity of the Viterbi Algorithm. If detection time is an important factor, then sub-optimal methods may be used to reduce computation with a trade-off of more errors. Nevertheless, under certain conditions, the watermarking methods that use convolutional coding have the potential to outperform their non-coding counterparts.

As we've mentioned that aside from information protection Digital Watermarking is presently used for Digital marketing, promotional Services health care and military data. A Static Promotional media is presently is created extremely efficient Dynamic Promotional medium with the aid of using exploitation Digital watermarking. Consequently, for developing it safer, actual and copyright a Blind digital watermarking the use of RSA approach for colour images may be deliberate for future work and hence for the safety of digital watermark a few extra researches must be done.

5.3 Environmental Benefits

1. Data is more secure than existing system.
2. It isn't robust to common signal technique operations thence watermarks are often simply depleted because of signal processing attacks
3. Good compression and better imperceptibility.
4. Easily shared encrypted data to any recipient.
5. Very fast and simple encryption and verification.

5.4 Future Work Plan-

Need to enforce secure digital watermarking strategies for e-governance applications and medical applications. Two completely distinct watermarks are embedded inside the cover page to boost the strength and protection moreover it reduces the distance for storing, transmission data bandwidth and transmission time for clinical services. This will be for providing more secure algorithm and approach so as to protect from the Hackers and market competitors. Every application has its own merits and demerits. Further enhancements can be made to the application, so that the web site functions very attractive and useful manner than the present one.

APPENDIX A: References

[1] P.Tay and J.P. Havlicek, Image Watermarking Using Wavelets,Copyright@IEEE,2002.

Link: https://ieeexplore.ieee.org/document/1187021

[2] J.J.K. O Ruanaidh,W.J. Dowling, F.M. Boland,Watermarking Digital Images for Copyright Protection, IEEE, 1995.

Link: https://ieeexplore.ieee.org/document/465537

[3] JUAN R. HERNANDEZ, AND FERNANDO PEREZ-GONZA LEZ, Statistical Analysis of Watermarking Schemes for Copyright Protection of Images, PROCEEDINGS OF THE IEEE, VOL. 87, NO. 7, JULY 1999 .

Link: https://ieeexplore.ieee.org/document/771069

[4]Chun-Shien Lu and Hong-Yuan Mark Liao, MultipurposeWatermarking for Image Authentication and Protection, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 10, NO. 10, p.1579-1592, OCTOBER 2001.

Link: https://ieeexplore.ieee.org/document/951542

[5] JUAN R. HERNANDEZ, AND FERNANDO PEREZ-GONZA LEZ, Statistical Analysis of Watermarking Schemes for Copyright Protection of Images, PROCEEDINGS OF THE IEEE, VOL. 87, NO. 7, JULY 1999.

Link: https://ieeexplore.ieee.org/document/771069

[6] V. M. Potdar, S. Han and E. Chang, “A Survey of Digital Image Watermarking Techniques”, 2005 3rd IEEE International Conference on Industrial Informatics (INDIN).

Link: https://ieeexplore.ieee.org/document/1560462

[7] N. Tiwari, M. k. Ramaiya and Monika Sharma, “Digital watermarking using DWT and DES”, IEEE (2013).

Link: https://ieeexplore.ieee.org/abstract/document/6514380

[8] S. S. Gonge and J. W. Bakal, "Robust Digital Watermarking Techniques by Using DCT and Spread Spectrum", International Journal of Electrical, Electronics and Data Communication, ISSN: 2320-2084, vol. 1, no. 2, (2013).

Link: https://ieeexplore.ieee.org/abstract/document/5579033

[9] R.G. Schyndel, A. Tirkel, and C.F Osborne,―A Digital Watermark, Proceedings of IEEE International conference on Image Processing, ICIP-1994, pp. 86-90, 1994.

Link: https://ieeexplore.ieee.org/abstract/document/413536

[10] Christine I. Podilchuk, Edward J. Delp,―Digital watermarking: Algorithms and applications, IEEE Signal processing Magazine, July 2001.

Link: https://ieeexplore.ieee.org/document/939835

[11] Jiang Xuehua,―Digital Watermarking and Its Application in Image Copyright Protection, 2010 International Conference on Intelligent Computation Technology and Automation.

Link: https://ieeexplore.ieee.org/document/5523112

[12] Bilge Gunsel, Umut Uludag, A. Murat Tekalp, Robust watermarking of "fingerprint images, 0031- 3203/02/$22.00 2002 Pattern Recognition Society. Published by Elsevier Science Ltd. All rights reserved. PII: S0031-3203(01)00250-3,2002.

Link: https://www.sciencedirect.com/science/article/abs/pii/S0031320301002503

REFERENCES

[1] P.Tay and J.P. Havlicek, Image Watermarking Using Wavelets,Copyright@IEEE,2002.

[2] J.J.K. O Ruanaidh,W.J. Dowling, F.M. Boland,Watermarking Digital Images for Copyright Protection, IEEE, 1995.

[3] JUAN R. HERNANDEZ, AND FERNANDO PEREZ-GONZA LEZ, Statistical Analysis of Watermarking Schemes for Copyright Protection of Images, PROCEEDINGS OF THE IEEE, VOL. 87, NO. 7, JULY 1999

[4] Chun-Shien Lu and Hong-Yuan Mark Liao, MultipurposeWatermarking for Image Authentication and Protection, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 10, NO. 10, p.1579-1592, OCTOBER 2001.

[5] JUAN R. HERNANDEZ, AND FERNANDO PEREZ-GONZA LEZ, Statistical Analysis of Watermarking Schemes for Copyright Protection of Images, PROCEEDINGS OF THE IEEE, VOL. 87, NO. 7, JULY 1999.

[6] V. M. Potdar, S. Han and E. Chang, “A Survey of Digital Image Watermarking Techniques”, 2005 3rd IEEE International Conference on Industrial Informatics (INDIN)

[7] N. Tiwari, M. k. Ramaiya and Monika Sharma, “Digital watermarking using DWT and DES”, IEEE (2013).

[8] S. S. Gonge and J. W. Bakal, “Robust Digital Watermarking Techniques by Using DCT and Spread Spectrum”, International Journal of Electrical, Electronics and Data Communication, ISSN: 2320-2084, vol. 1, no. 2, (2013).

[9] R.G. Schyndel, A. Tirkel, and C.F Osborne,―A Digital Watermark, Proceedings of IEEE International conference on Image Processing, ICIP-1994, pp. 86-90, 1994

[10] Christine I. Podilchuk, Edward J. Delp,―Digital watermarking: Algorithms and applications, IEEE Signal processing Magazine, July 2001.

[11] Jiang Xuehua,―Digital Watermarking and Its Application in Image Copyright Protection, 2010 International Conference on Intelligent Computation Technology and Automation.

[12] Bilge Gunsel, Umut Uludag, A. Murat Tekalp, Robust watermarking of "fingerprint images, 0031- 3203/02/$22.00 2002 Pattern Recognition Society. Published by Elsevier Science Ltd. All rights reserved. PII: S0031-3203(01)00250-3,2002

ss

ORIGINALITY REPORT

27%	20%	10%	10%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	tuprints.ulb.tu-darmstadt.de Internet Source	3%
2	Submitted to Symbiosis International University Student Paper	3%
3	Submitted to Thapar University, Patiala Student Paper	3%
4	B Swapna, M Kamalahasan, S Srinidhi, S Sowmiya, S Vasanth, P Sri Divyabharathi. "Digital picture watermarking technique for security applications", IOP Conference Series: Materials Science and Engineering, 2020 Publication	2%
5	docplayer.net Internet Source	2%
6	ijirset.com Internet Source	2%
7	Submitted to Shinas College of Technology Student Paper	2%

8	N. Sharma, A. Anand, A. K. Singh. "Bio-signal data sharing security through watermarking: a technical survey", Computing Internet Source	2%
9	global.oup.com Internet Source	2%
10	notesmarket.netlify.app Internet Source	2%
11	upcommons.upc.edu Internet Source	2%
12	link.springer.com Internet Source	2%
13	www.geeksforgeeks.org Internet Source	2%

Exclude quotes	On	Exclude matches	< 2%
Exclude bibliography	On		