IMAGE WATERMARKING USING

WALSH HADAMARD TRANSFORM AND SVD

A Project Submitted to

Jawaharlal Nehru Technological University, Kakinada

In the partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY
IN
ELECTRONICS AND COMMUNICATION ENGINEERING

Submitted by:

SANNEBOYINA LAVANYA	19491A04J6
SANNEBOYINA SURENDRA	19491A04J5
USURUPATI UDAYKIRAN	19491A04O1
VALETI AJAY	19491A04O4
RAGIPINDI NIRANJANLOKESH	19491A04I4

Under the Guidance of

Mr. V. JAIKUMAR M. Tech, (Ph. D),

ASSOCIATE PROFESSOR

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

QIS COLLEGE OF ENGINEERING AND TECHNOLOGY

(AUTONOMOUS)

Approved by AICTE | Permanent Affiliation: JNTU-Kakinada |

UGC-Recognized | NBA Accredited | Accredited by NAAC A+ |

An ISO 9001:2015 Certified InstitutionVENGAMUKKAPALEM,

ONGOLE – 523272, ANDHRA PRADESH

2019-2023

QIS COLLEGE OF ENGINEERING AND TECHNOLOGY (AUTONOMOUS)

Approved by AICTE | Permanent Affiliation: JNTU-Kakinada
|UGC-Recognized Accredited by NBA | Accredited by NAAC A+ | An ISO 9001:2015
Certified | VENGAMUKKAPALEM, ONGOLE-523272, A.P.

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that the project entitled

IMAGE WATERMARKING USING WALSH HADAMARD TRANSFORM AND SVD

Is a bonafide work of

SANNEBOYINA LAVANYA	19491A04J6
SANNEBOYINA SURENDRA	19491A04J5
USURUPATI UDAYKIRAN	19491A04O1
VALETI AJAY	19491A04O4
RAGIPINDI NIRANJANLOKESH	19491A04I4

in the partial fulfilment of the requirement for the award of the degree of Bachelor of Technology in **ELECTRONICS AND COMMUNICATION ENGINEERING** and for the academic year **2022- 2023.**

This work is done under my supervision and guidance.

Signature of the Guide	**Signature of the Head of the Department**
Mr. V. JAIKUMAR	**Dr. CH. HIMABINDU**
M. Tech, (Ph. D)	**M. Tech, Ph. D,**
Associate Professor, Department of ECE	**Professor & HOD, ECE**

Signature of External Examiner

ACKNOWLEDGEMENT

We thank the almighty for giving us the courage and perseverance in completing the project. It is an acknowledgement for all those people who have given us their heartfelt cooperation in making the major project a grand success.

We express our gratitude to the Honorable president **Sri. N. NAGESWARARAO GARU, B.E.,** QIS Group of Institutions, Ongole for his valuable suggestions and advices throughout the course.

We would like to place on record the deep sense of gratitude to the Honorable Secretary & Correspondent **Dr. N. SURYA KALYAN CHAKRAVARTHY GARU, M. Tech., Ph.D**., QIS Group of Institutions, Ongole for providing necessary facilities to carry the project work.

We express our gratitude to our respected principal **Dr. Y. V. HANUMANTHARAO GARU, B.E., M. TECH., Ph.D.,** QIS College of Engineering and Technology, Ongole for his valuable suggestions and advices throughout the course.

We express our gratitude to the Head of the Department of ECE, **Dr. CH. HIMA BINDU**, **M. Tech., Ph.D.,** QIS College of Engineering & Technology, Ongole for her constant supervision, guidance and co-operation throughout the project.

We express our gratitude to the Project Guide, **V. JAIKUMAR, M. Tech., Ph.D.,** QIS College of Engineering& Technology, Ongole for his constant supervision, guidance and co-operation throughout theproject.

We would like to express our thankfulness to our Project Co-ordinator, **Dr. PRASAD JONES**, **M.Tech., Ph.D.,** QIS College of Engineering & Technology, Ongole for his constant motivation and valuable help throughout the project work.

Finally, we would like to thank our Parents, Family and friends for their co-operation to complete this project.

TABLE OF CONTENTS

ABSTRACT

Digital image watermarking is a process of embedding a known data into an image. To include a watermark into a recognized cover picture, many methods have been proposed. Watermarking digital photos offers security features including copyright protection, proof of ownership, and image authentication. This study uses the FWHT-SVD transformation to present a new, robust picture watermarking and watermark extraction technique. Correlating the recovered watermark with the original watermark for different Walsh Hadamard transformation coefficients is a step in the extraction process. The digital image watermarking algorithms using Walsh Hadamard transform have been identified to be more prevalent as compared to those with the other watermarking algorithms. This is due to the transformation that converts the spatial domain of the host image to the transform domain. The WHT is a powerful tool that can transform an image into a set of coefficients that capture its energy distribution in different frequency component.

This work presents the robust multiple watermarking which combines Walsh Hadamard transform (WHT) and Singular Value Decomposition (SVD). The process of embedding a message into an image is known as digital image watermarking. The development of technologies with respect to computers, networks, and multimedia, the transmission of information in the form of images has become more and more convenient. Due to its rising popularity, the Walsh Hadamard Transform is commonly used in recent watermarking techniques. In this article, we present a combined WHT to decompose the cover digital image into a set of coefficients, we tend to apply the SVD to decomposed coefficient matrix, and insert the same watermark data by renovating the singular values. The simulation results show how strong and successful this suggested watermarking system is.

LIST OF FIGURES

LIST OF ABBREIVATIONS

WHT	Walsh Hadamard transform
FWHT	Fast Walsh Hadamard transform
SVD	Singular value decomposition
DCT	Discrete cosine transform
DWT	Discrete wavelet transform
FFT	Fast Fourier transform
DIW	Digital Image Watermarking
QIM	Quantization index modulation
PSNR	Peak signal to noise ratio
SSIM	Structural similarity index
TIFF	Tag image file format
PNG	Portable networks graphics
PCA	Principal component analysis
Lena Image	Host Image
Medical Images	Watermark

CHAPTER-1
INTRODUCTION

1.1 Introduction

Watermarking (data hiding) is the process in which we are going to embedding data into a multimedia element such as image, video or audio. For security reasons, this embedded data may subsequently be found in or retrieved from the multimedia. a watermarking algorithm composed of a detection or extraction algorithm, an embedding algorithm, and the watermark structure. Symbols that are typically placed on paper during production to identify the producer are called watermarks. The first watermark was discovered in Italy in the 13th century. in the recent past. The internet has grown to be a very popular instrument for information transfer. With the internet, data such as text, voice, photos, and videos are sent. Researchers have thus had to deal with a variety of problems, including secrecy, dependability, and availability. One appropriate solution to these problems is digital watermarking. The basic idea of digital watermarking is to insert 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 extracted.

The following characteristics of an efficient invisible digital watermarking approach should be present: it should be almost undetectable, and it should be resistant to operations on the pictures such cropping, rotation, scaling, filtering, collusion assaults, etc. Digital watermarking techniques may primarily be used in one of two ways: in the spatial domain or in the frequency domain. The spatial domain watermarking techniques have less computational overhead compared to the frequency domain watermarking techniques.

The main transforms are Walsh Hadamard Transform (WHT). There is a need for visible and invisible watermarks to verify documents for validity. When the user gets the watermarked image from other sources, can check the authenticity of the information in the image by comparing it with the original image. The user must be able to extract the valid watermark from the watermarked image the original image is essential. Digital image watermarking is imperceptible and hard to remove by unauthorized persons. Several methods have used the spatial and frequency domains to apply the concept, each with its own advantages and limitations.

1.2 History

Digital image watermarking is a technique in which watermark data is embedded into a multimedia products like images and, later, is extracted from or detected in the watermarked product. These methods ensure tamper-resistance, authentication, content verification, and integration of the image. In a noise-tolerant signal, such as audio, video, or picture data, a digital watermark is a type of marking that is discreetly included. It is often used to establish who owns the copyright to a certain signal. The method of "watermarking" involves concealing digital data inside a carrier signal; the concealed data may or may not be related to the carrier signal. The legitimacy or integrity of the carrier signal may be confirmed using digital watermarks, and their owners' identities may also be revealed. It is often used for banknote authentication and for tracking copyright violations. Digital watermarks, like conventional physical ones, are frequently only detectable under specific circumstances, for as after using an algorithm Depending on its intended use, a digital watermark may be deemed less effective if it modifies the carrier signal in a way that makes it obvious.

Traditional watermarks may be applied to visible media (like images or video), whereas, in digital watermarking, the signal may be audio, pictures, video, texts, or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal. The needed properties of a digital watermark depend on the use case in which it is applied. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied. Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals.

While steganography aims for imperceptibility to the human senses, digital watermarking tries to control robustness as a top priority. Since a digital copy of data is the same as the original, digital watermarking is a passive protection tool. It just marks data but does not degrade it or control access to the data. One application of digital watermarking is source tracking. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of especially image editing software such as Adobe Photoshop. Visible watermarks may lose their functions to show the copyright of the digital products due to malicious use of this software, Hence the need for the invisible watermark.

1.3 Scope of Project

Basically, there are two types of digital watermarking that have been mentioned. They are visible watermarking and invisible watermarking. This project will focus on invisible watermarking only because invisible watermarking has proved to be more useful compared to visible watermarking. The visible watermark can be removed easily by image processing programs such as Photoshop but the invisible watermark cannot be removed easily. Although digital watermarking may be applied to a variety of digital assets, including video, audio, and images, this project will concentrate on watermarking digital images, and the watermark will also be an image. Only images with a minimum dimension of 300 by 300 will be utilized as watermarks. The digital cover picture must be at least 300 by 300 pixels in size and be in grayscale. The program that will be utilized to carry out this project is Matlab.

Basically, this project will be divided into three stages, which are pre-processing stage which involves resizing the cover image and watermark image to appropriate dimensions. converting the images to greyscale if RGB. The second stage will be the processing stage, which involves applying the WHT transforms to the image. The third stage is the post-processing stage which involves extracting the embedded watermark. Possible attacks to the watermarked image may also be done here and the watermark extracted after the attacks to prove robustness.

1.4 Problem Statement

Digital photos provide a number of advantages, including quick and affordable processing costs, simple communication and storage, rapid quality evaluation, many copies while maintaining quality, quick and affordable reproduction, and adaptive modification.

A daily necessity is the use of digital photographs. Processing photos for use in medicine typically involves a computer. Image processing entails a wide range of methods and actions, including picture acquisition, archiving, display, and communication. The image is a function that represents features of an observed object, such as lighting or color. Digital photos offer several advantages, including quick and inexpensive processing costs, simple transmission and storage, rapid quality evaluation, and many copies while maintaining quality. Adaptable manipulation and quick and inexpensive replication. The disadvantages of digital images are exploitation of copyright, and the inability to resize with preserving the quality. the need for large-capacity memory. and the need for a faster processor for manipulation.

CHAPTER-2

LITERATURE REVIEW

MM. Abd-Eldayem, “**A proposed security method for digital communications and imaging in medicine that uses watermarking and encryption”**. Modern Hospital Data Management Systems (HDMSs) are now used in a computer network, and medical devices also create digital versions of medical images. To maintain image integrity and protect patient privacy, HDMS must store and exchange these images in a secure setting. To provide integrity and privacy, reversible watermarking techniques can be used. The use of a security method based on watermarking and encryption for digital imaging and communications in medicine is proposed in this paper (DICOM). Reversible watermarking is used to provide patient authentication, information confidentiality, and integrity. A hash value based on encrypted MD5 is extracted from the image to achieve integrity service at the sender side. R-S-Vector is calculated from the image in order to satisfy the reversible feature[1].

Benoraira, K. Benmahammed, N. Boucenna, “Blind image watermarking technique based on differential embedding in dwt and dct domains”. This study presents a novel discrete wavelet transform-based blind and reliable image watermarking method (DWT) together with discrete cosine transform (DCT). The bits of the watermark sequence are differentially embedded using two sub-vectors that have undergone DCT transformation. By subsampling the approximation, the original sub-vectors are obtained. coefficients of the host image's DWT transform. The embedded watermark sequence can be found during the extraction process by simply comparing the corresponding sub-vectors of the watermarked image. The proposed method successfully satisfies the requirement of imperceptibility, according to experimental findings, and offers high robustness against various image-processing attacks, including JPEG compression, noise addition, low-pass filtering, sharpening, and bit-plane removal. Our system also performs well to acceptably well against some geometrical attacks such as resizing and cropping[3].

R. Bamal, S.S. Kasana, **“Dual hybrid medical watermarking using walsh-slantlet transform”.** This study introduces a new, reliable, and blind image watermarking method based on discrete wavelet Transform (DWT). The Singular Value Decomposition (SVD) with Fast Walsh Transform (FWT) and Slantlet Transform (SLT) for image authentication are used in this paper to propose a hybrid robust lossless data hiding algorithm. These transforms have good energy compaction and distinct filtering, which results in higher embedding capacities of 1.8 to 7.5 bits per pixel (bpp). The proposed algorithm uses two different watermarks and an Artificial Neural Network (ANN) to detect regions of interest (ROI). After applying FWH, embedding is carried out by altering the highest coefficients of the SLT sub-bands as well as the SVD coefficients. The ROI is the first watermark in dual hybrid embedding, and another watermark consists of three parts, i.e., patients' personal details, unique biometric ID and the key for encryption [5].

N. Salem, S. Hussein, "Data dimensional reduction and principal components analysis". The development of computer algorithms that can handle massive amounts of data and then utilize e this data in an intellectual way to solve a variety of real-world problems is a key issue that is addressed by research in the fields of machine learning and intelligent systems. It is crucial to reduce the number of variables and interpret linear combinations of the data in many applications in order to interpret data with a lot of variables in a meaningful way. In order to decrease the dimensionality of large datasets, the unsupervised learning technique known as Principal Component Analysis (PCA) applies sophisticated mathematical concepts. The objective of this paper is to present a thorough understanding of the sophisticated PCA in the fields of machine learning and data dimensional reduction. It provides a mathematical explanation and describes its relationship with Singular Value Decomposition (SVD) when PCA is calculated using the covariance matrix. In addition, with the use of MATLAB, the paper shows the usefulness of PCA in representing and visualizing Iris dataset using a smaller number of variables [7].

T. Khanam, P.K. Dhar, S. Kowsar, J.-M. Kim, **"SVD-based image watermarking using the fast Walsh-Hadamard transform, key mapping, and coefficient ordering for ownership protection".** Users who require proof of ownership for multimedia data are exposed to serious risks because of the numerous transmission channel attacks that can occur when using distributed computing infrastructures. This paper proposes an effective blind symmetric image watermarking method for ownership protection using the fast Walsh-

Hadamard transform (FWHT) and singular value decomposition (SVD). The watermark image is initially scrambled using Gaussian mapping to protect the system from unauthorized detection. After that, the cover image is subjected to FWHT with coefficient ordering. Two distinct keys are generated from the singular values of the FWHT blocks of the cover image, which are kept by the owner alone, to make the embedding process robust and secure against serious attacks. The generated keys are then used to extract the watermark and verify the ownership. The simulation result demonstrates that our proposed scheme is highly robust against numerous attacks. Furthermore, comparative analysis corroborates its superiority among other state-of-the-art methods. The NC of the proposed method is numerically one, and the PSNR resides from 49.78 to 52.64. In contrast, the NC of the state-of-the-art methods varies from 0.7991 to 0.9999, while the PSNR exists in the range between 39.4428 and 54.2599 [8].

E.E. Abdallah, A.F. Otoom, A.E. Abdallah, M. Bsoul, S. Awwad,**"Ahybrid secure watermarking scheme using nonnegative matrix factorization and fast Walsh-Hadamard transform".** With the help of Fast Walsh-Hadamard Transform (FWHT) and Nonnegative Matrix Factorization (NMF), we present a reliable and undetectable secure image watermarking method (FWHT). The main concept of the suggested plan consists of four essential steps: Blocks of the original cover image are separated. Following the application of the NMF to each block separately, the FWHT is used to calculate the weight matrix. The watermark image's singular values are then distributed across the blocks that have been transformed. The experimental findings undoubtedly demonstrate improved visual imperceptibility and exceptional resistance to different types of attacks [9].

E.M. El Houby, N.I. Yassin, "Wavelet-hadamard based blind image watermarking using genetic algorithm and decision tree". The active use of Internet and multimedia technologies has recently increased copyright violations. In the area of multimedia copyright protection, digital watermarking is essential. This paper proposes an improved Hadamard transform and discrete wavelet transform (DWT) based image watermarking method. The Genetic Algorithm (GA) is an optimising method for balancing robustness and imperceptibility. Utilizing the Decision Tree's estimation capabilities, blind property is conducted (DT). Prior to applying the Hadamard transform to a few chosen DWT sub-bands, the host image is first transformed using second level DWT. Utilizing GA, adaptive multiple strength values are calculated. With the help of the trained DT, which calculates the initial coefficients required for the extraction process without the use of the original host image. The proposed technique is evaluated against several types of attacks: compression, median filtering, salt and pepper noise, histogram equalization, blurring, scaling, painting, and cropping. Experimental results show that the proposed watermarking technique is robust against these attacks while keeping good imperceptibility. The proposed technique outperforms the compared techniques according to robustness, imperceptibility, and capacity [10].

S. Thakur, A.K. Singh, S.P. Ghrera, M. Elhosen, "Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications." In this article, we present a reliable and secure watermarking method for tele-health applications using transform domain techniques. For the purposes of authentication, annotation, and identification, the patient report or identity is embedded into the host medical image. We apply a less complicated chaos-based encryption algorithm to watermarked images for increased confidentiality. The results of the experiments showed unequivocally that the suggested method is sufficiently secure against different types of attacks without introducing any significant distortions between the watermarked and cover images. Additionally, our method was found to perform better than the cutting-edge watermarking methods currently in use. Additionally, a subjective evaluation of the watermarked image's quality is conducted, which is advantageous in the quality-driven healthcare sector [13].

S. Thakur, A.K. Singh, S.P. Ghrera, A. Mohan, **"Chaotic based secure watermarking approach for medical images"**. In this paper, a secure watermarking method for medical images based on chaos is proposed. The method significantly improves imperceptibility and robustness using non-subsampled contourlet transform (NSCT), redundant discrete wavelet transform(RDWT), and singular value decomposition (SVD). Applying 2-D logistic map-based chaotic encryption to a watermarked medical image further ensures the approach's security. In our method, the cover image is first divided into smaller images, and NSCT is then applied to the sub-image with the highest level of entropy. The singular vector of the RDWT coefficient is then calculated after applying RDWT to the NSCT image. Both watermark images follow a similar process. Both watermarks' singular values are incorporated into the cover's singular matrix. Experimental analysis demonstrates when the approach is subjected to attacks, using combination of NSCT, RDWT, SVD and chaotic encryption it makes the approach robust, imperceptible, secure and suitable for medical applications [14].

CHAPTER - 3
WATERMARKING

3.1 Watermarking

Watermarking is the process of superimposing a logo or piece of text atop a document or image file, and it's an important process when it comes to both the copyright protection and marketing of digital works.

3.1.1 Digital Image Watermarking

Digital image watermarking is a technique in which watermark data is embedded into a multimedia products like images and, later, is extracted from or detected in the watermarked product. These methods ensure tamper-resistance, authentication, content verification, and integration of the image. The following fig. shows the block diagram of watermarking:

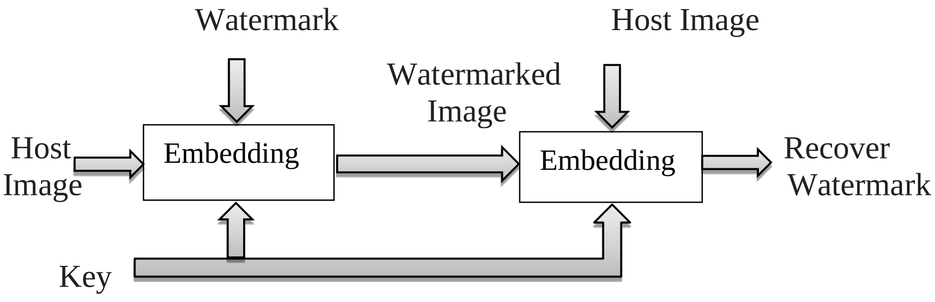


Fig 3.1 Basic Blocks of Image Watermarking

3.1.2 How it is done

The embedding and extraction steps of the watermarking process combine to create the watermarked digital image. The cover image is given watermarks during the embedding process in order to provide protection. The watermarked image is separated from the original image during the extraction procedure. Methods for digital watermarking can be used in the frequency domain or the spatial domain. However, it is important to note that digital watermarking in the frequency domain is more reliable than in the spatial domain.

3.1.3 Types of Watermarks

- Visible Watermarks- These watermarks are visible.
- Invisible Watermarks - These watermarks are embedded in the media and use steganography technique.
- Public Watermarks - These can be understood and modified by anyone using certain algorithms.
- Fragile Watermarks - A watermark is a logo, text, or pattern that is intentionally superimposed onto another.

3.1.4 Advantages of Watermarking

- Copyright protection
- Fingerprinting & Transaction tracking
- Medical applications
- Military applications
- Authentication & Tamper detection
- Broadcast monitoring
- Ownership identification
- Digital forensic
- Electronic voting system

3.1.5 Applications of Watermarking

Digital image watermarking is a highly focused research area, due to its potential use in media applications such as copyright protection, annotation, privacy control, data authentication, device control, media forensics, and medical reports (e.g., X-rays).

The following fig. shows the different applications of watermarking in digital image watermarking:

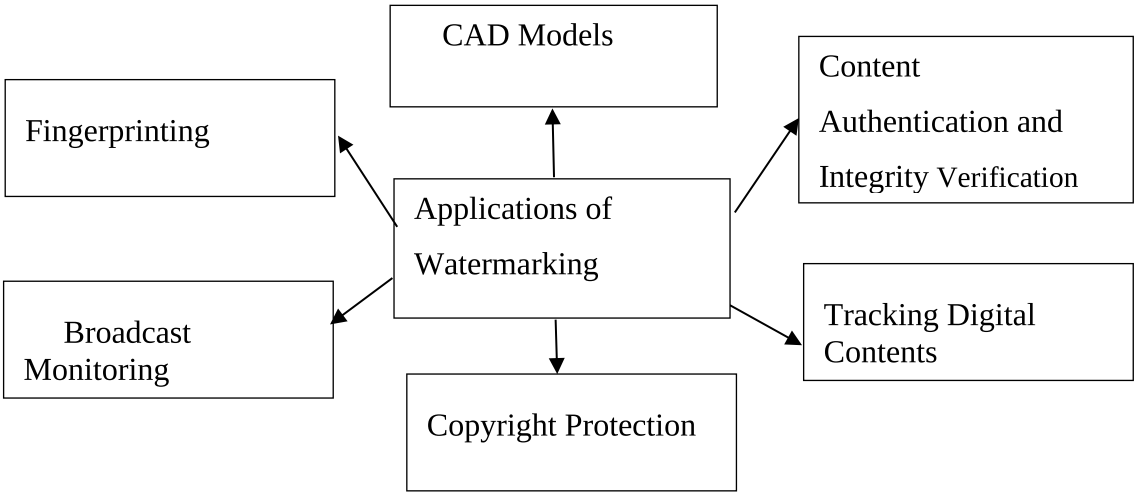

CAD Models
Content Authentication and Integrity Verification
Fingerprinting
Applications of Watermarking
Broadcast Monitoring
Tracking Digital Contents
Copyright Protection

Fig 3.2 Applications of Watermarking

3.1.6 Characteristics of Digital Image Watermarking

The chracteristics of Digital Image Watermarking are:

a. Robustness

The robustness of watermarking scheme refers to survival of embedded watermark against any image processing and geometric attacks. These attacks may include spatial filtering. copying, cropping, scaling, translation, compressing and rotation either intentionally or unintentionally**.**

b. Security

It is desired that watermark must remain a secret and is undetectable to unauthorized parties. Security of the watermark defines ability of watermark to be undetectable to unauthorized parties. Security of watermark also decides its resistance against attacks.

c. Imperceptibility

The term imperceptibility refers to amount of likeness between the message image and the image that is watermarked. Perceptual transparency is the main requirement of any watermarking system. In all applications of digital watermarking, watermark is inserted in the cover image, so the perceptual quality of host image gets affected. It is always desired that watermark is implanted in the message image in such a manner that the perceptual quality of message image doesn't get degraded after some extent.

d. Cost

The cost here refers to the computational cost involved in the entire watermarking process which includes embedding of watermark to host image and extraction of watermark.

3.2 Existing Methods

Hybrid watermarking is a popular approach to embedding watermarks in digital media, which combines multiple techniques to achieve better robustness and security. One such method for hybrid watermarking uses the Walsh-Hadamard transform (WHT) and Singular Value Decomposition (SVD). The fundamental idea behind this technique is to use WHT to modify the host picture by breaking it down into its frequency constituents. The most important characteristics are then extracted from these frequency components using the SVD. The watermark is then incorporated into the chosen features using an appropriate method, such as quantization index modulation or spread spectrum (QIM). The watermarked picture is then subjected to the inverse SVD and WHT to produce the finished watermarked image.

The benefit of employing WHT is that it offers an easy-to-use method of transforming the host picture, and it can be quickly reversed to retrieve the original image. Nonetheless, SVD is renowned for its capacity to extract an image's most important elements, making it a viable option for inserting the watermark.

This technique has several different implementations, and the particulars may change based on the application and the specifications. To get the final watermarked picture, inverse transformations are used after watermark embedding and WHT for frequency decomposition and SVD for feature extraction.

3.3 Proposed Method

The watermark in a weak watermarking system is very sensitive to changes made to the watermarked picture. A watermarked file's authenticity and integrity are guaranteed by this creative strategy. In most cases, robust watermarking is utilized to properly protect concealed data from potential attackers. The major objective of our adopted strategy is to ensure the veracity and consistency of a watermarked medical image while effectively including a watermark that is strong enough to withstand any attacks and stay recognizable.

Like any other watermarking method, the steps in our approach—watermark production, insertion, and successful extraction—are all broken down into three separate phases. While assessing whether watermarking systems are imperceptible, their proposed technique fared better. More masking strength leads to less quality loss in the watermarked picture, according to their experimental findings. The Proposed model flow chart for image watermarking using WHT-SVD is shown below:

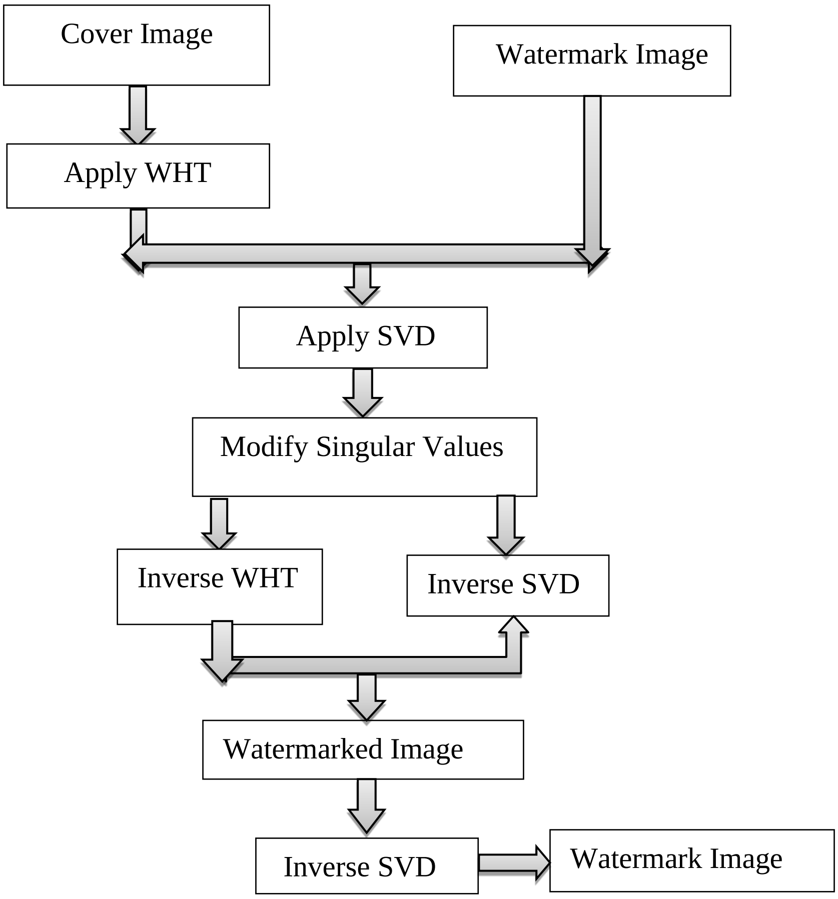


Fig 3.3 Proposed model flow chart using WHT-SVD

Several different watermarking methodologies and techniques are designed and opted for various applications for many years. The proposed scheme of Digital Watermarking comprises of both blind and non-blind Digital watermarking techniques within the process, this combined approach of digital watermarking can also be known as serial watermarking. Digital image watermarking can be used for proof of the authenticity of the object's originator. Additionally, digital counterfeiting, fraud, identity theft, secured electronic voting, and deployable remote education, among many others, are all possible applications of digital watermarking.

This technique inserts watermark information into the host image, as defined by the owner in the spatial or time domain, using different methods. These techniques work directly on the original image pixels. The watermark can be inserted by manipulating the pixel values, based on a logo or signature information provided by the author. In the most commonly used designs, pixel intensities at known points in space represent the image, where the lowest-order bit of certain pixels in a color or grayscale image is flipped. Depending on the pixel intensity, the resulting watermark may be visible or invisible. We review various approaches regarding spatial domain techniques that have attracted the attention of researchers due to their optimal balance among imperceptibility, robustness, and capacity, which are the most important requirements of any watermarking technique. These techniques have low complexity, improved efficiency, and faster execution. Furthermore, the watermarked image quality may be controlled. However, these techniques perform well only if the image is not exposed to any noise or human modification. Picture cropping can be used to exclude the watermark, which is a major weakness in spatial domain watermarking.

CHAPTER - 4

METHODOLOGY

4.1 Watermark Embedding

The proposed algorithm includes three steps: decomposing the cover image, embedding, and extraction. A binary watermark image will be used as the watermark for embedding. The trained PNN is used to extract the watermark during watermark recovery. This paper describes an algorithm concerned with digital image watermarking which is developed by the combination of the two: WHT and SVD. In this section, a brief introduction to WHT and SVD is given**.**

The cover image that will be protected will have watermarks added as part of the embedding process. A Lena image will be used as the watermark, and it will be embedded into the host image, also known as the cover image

4.1.1 Walsh Hadamard Transform:

Walsh Hadamard transform is referred to as a non-sinusoidal orthogonal transform technique that is capable to decompose a signal/image into a set of its basic functions. The basis for the Walsh Hadamard transform is the system of Walsh functions. These Walsh functions are orthogonal and have the values mainly +1 and -1. The general form of the Walsh transform can be generated by the Hadamard matrix shown as:

For 2x2 can be defined as:

$$\mathrm{H4} = \begin{bmatrix} \mathrm{H2} & \mathrm{H2} \\ \mathrm{H2} & -\mathrm{H2} \end{bmatrix}$$

for k=1, 2, 3, ...H1=1 for k=0

Further for k=2 the Hadamard matrix H2 for 2x2 can be defined as:

$$H2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Further for k=1 the Hadamard matrix H4 for 4x4 can be defined as:

$$H4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

The output array of the WHT coefficients contains only the integer values, as a result of this. the Hadamard transform is referred as the very fast transform and thus can be implemented in O(N log2 N) additions and subtractions. Further, it is proved in this paper, that Walsh Hadamard transform can be effectively used in the watermarking technique. Natural and Sequence ordered WHT: By the application of the above definition repeatedly we can construct an 8×8 natural ordered matrix as shown below:

Matrix Rows

$$H8 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} \quad \begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \end{array}$$

From the above natural ordered Hadamard matrix sequence matrix can be constructed by changing the row ordering of the above matrix, based on the number of sign changes in each of the rows. The steps involved in the process of conversion of natural order matrix to sequence order are as follows, finding the grey code of the binary index code and then reversing it. An example of such transformation is given below. This shows in the first step the conversion of binary code to the grey code and then the grey code bits get reversed thus the value of k is obtained based upon which 8×8sequencey ordered matrix is obtained. In the Walsh Hadamard transform, an image signal can be analyzed by converting the image into set of co-efficients.

The following fig. shows the conversion of data from natural order to sequence order:

S	0 1 2 3 4 5 6 7
Binary	000 001 010 011 100 101 110 111
Gray Code	000 001 011 010 110 111 101 100
Bit-reverse	000 100 110 010 011 111 10 01

Fig 4.1 Sample example to convert natural order matrix to sequence order

- Thus an 8x8 sequency order Hadamard matrix can be given as:

$$\mathrm{H8} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} \begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \end{array}$$

The sequence ordered Hadamard matrix organizes the transformed data in increasing order of frequency which makes the process of feature selection systematic and fast. The main application of the Walsh Hadamard transform is in speech processing, filtering, and power spectrum analysis. Walsh Hadamard transform has a fast version, Further it is declared from the methodology that, in all of the cases WHT transformation is used both in case of watermark Embedding and in watermark extraction process.

4.1.2 Singular Value Decomposition:

The context of digital watermarking, SVD (Singular Value Decomposition) is a technique used to embed a watermark into a host image. The basic idea behind watermarking is to add a hidden message or information (the watermark) to a digital image in a way that is imperceptible to human eyes but can be detected and extracted by authorized parties using appropriate tools.

SVD can be used in watermarking by decomposing the host image into three matrices, as described earlier. The watermark is then embedded by modifying the singular values of the decomposition matrix, which makes the watermark robust against various image processing operations such as compression, filtering, and cropping. To extract the watermark, the receiver must perform the same SVD decomposition on the watermarked image and compare the resulting singular values with those of the original image to detect the presence of the watermark.

Overall, SVD-based watermarking is a widely used technique for copyright protection, content authentication, and data hiding in digital. SVD (Singular Value Decomposition) can be used in digital watermarking to embed a watermark signal into a host signal, such as an image or audio file.

The basic idea is to use the SVD of the host signal to transform it into a lower-dimensional representation, while simultaneously embedding the watermark signal in the resulting transformed data. Here's a high-level overview of how SVD can be used in watermarking:

1. Take the host signal, such as an image, and perform SVD on it to decompose it into three matrices: U, S, and V.

2. Modify the singular values in the S matrix to embed the watermark signal. This can be done by adding or subtracting a small value to the singular values, depending on the value of the corresponding bit in the watermark signal.

3. Reconstruct the host signal using the modified U, S, and V matrices to obtain a watermarked version of the signal.

4. To extract the watermark from the watermarked signal, perform SVD on the watermarked signal to obtain its U, S, and V matrices.

5. Compare the modified singular values in the S matrix to the original singular values to determine the watermark bits.

SVD-based watermarking can be effective because it is robust to many types of signal processing and attacks, such as compression, filtering, and noise addition. However, it can also be vulnerable to some types of attacks, such as cropping or scaling of the watermarked signal. Therefore, various techniques have been proposed to enhance the robustness of SVD-based watermarking, such as using multiple watermarks and using a combination of SVD and other watermarking techniques.

4.1.2.1 TYPES OF SINGULAR VALUE DECOMPOSITION:

In digital watermarking, SVD (Singular Value Decomposition) is commonly used for embedding and detecting watermarks in multimedia content. There are different types of SVD-based watermarking techniques, including: There are five types of singular value decomposition:

1. Spatial domain SVD
2. Frequency domain SVD
3. Hybrid SVD
4. Block-based SVD
5. Robust SVD

1.Spatial domain SVD

In this technique, the watermark is embedded in the spatial domain of the multimedia content by modifying the pixel values. The SVD is applied to the modified image to obtain the singular values, which are used to embed and detect the watermark.

2.Frequency domain SVD

This technique applies the SVD to the frequency domain of the multimedia content, such as the Discrete Cosine Transform (DCT) coefficients in images or videos. The watermark is embedded by modifying the selected DCT coefficients, and the SVD is used to obtain the singular values for watermark detection.

3.Hybrid SVD

This technique combines both spatial and frequency domain SVD for watermarking. The watermark is embedded in the spatial domain of the multimedia content and then the SVD is applied to the modified image. The resulting singular values are modified using the DCT coefficients to further embed the watermark.

4.Block-based SVD

In this technique, the multimedia content is divided into blocks, and the SVD is applied to each block to obtain the singular values. The watermark is embedded by modifying the singular values, and the SVD is applied again to obtain the watermarked blocks.

5.Robust SVD

This technique is designed to withstand common signal processing attacks, such as compression or noise addition. The watermark is embedded by modifying the singular values, and a robust detection scheme is used to detect the watermark even in the presence of attacks. These are some of the common types of SVD-based watermarking techniques used in multimedia content protection.

The following fig. shows the Watermark embedding procedure flowchart using WHT-SVD:

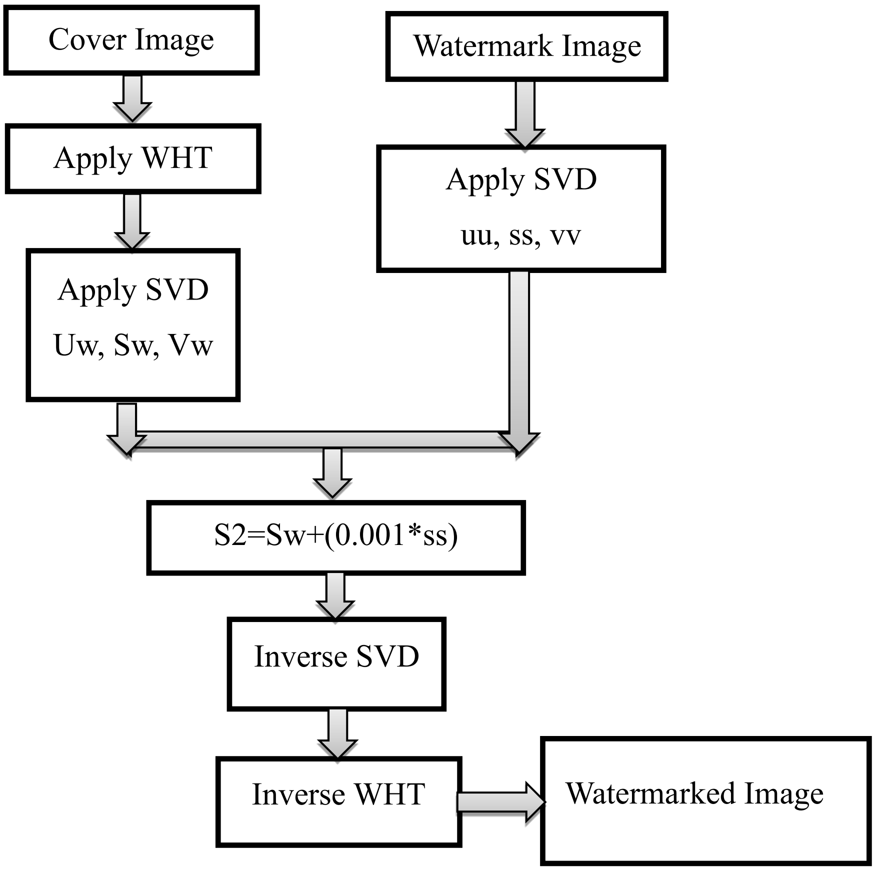


Fig 4.2 watermark embedding procedure flowchart

4.2 Watermark Embedding Algorithm

The watermark embedded algorithm is as follows:

Start

Step1: Read the cover image

Step2: Read the Watermark image

Step 3: Apply WHT Transform to decompose the cover image into a set of coefficients

Step 4: Apply SVD to the transformed image

Step 5: The applied SVD converts the matrix into three singular matrices(uu, ss, vv)

Step 6: Apply SVD on the watermark image to get three singular matrices as uw, sw, vw

Step 7: To Embed the Watermark into the host image add the obtained diagonal matrix of the host image with the diagonal matrix of watermark image.

Step 8: Apply inverse WHT on the WHT-transformed image including the modified singular values, to produce the watermarked cover image**.**

Step 9: Apply inverse SVD to get the watermarked image.

Stop.

In the algorithm process, the decomposition of the original cover image is done with the use of the Walsh Hadamard transform. The WHT is well known for its simplicity and robustness. In the WHT, the image is converted into a set of coefficients known as pixels. This process is called decomposition or analysis. The transformed image can be assembled back into the original image without loss of its robustness. This process is called reconstruction or synthesis.

For image watermarking, the fundamental idea behind the use of the Walsh transform is to embed the watermark into a set of pixels. According to the other transforms, the WHT approach is the easiest and most efficient technique for image watermarking. However, the most important aspect of WHT embedding is the selection of the coefficients to be used for embedding and the location in which to embed the watermark within the selected coefficients.

4.3 Watermark Extraction

The watermarked image is isolated from the original image during the extraction process. Fig. below shows the suggested method for extracting the watermark. As it uses and duplicates both the original image and the embedded watermark image, which are required for the extraction, this extraction method is a non-blind watermarking.

The following fig. shows the flowchart of watermark extraction procedure using WHT-SVD:

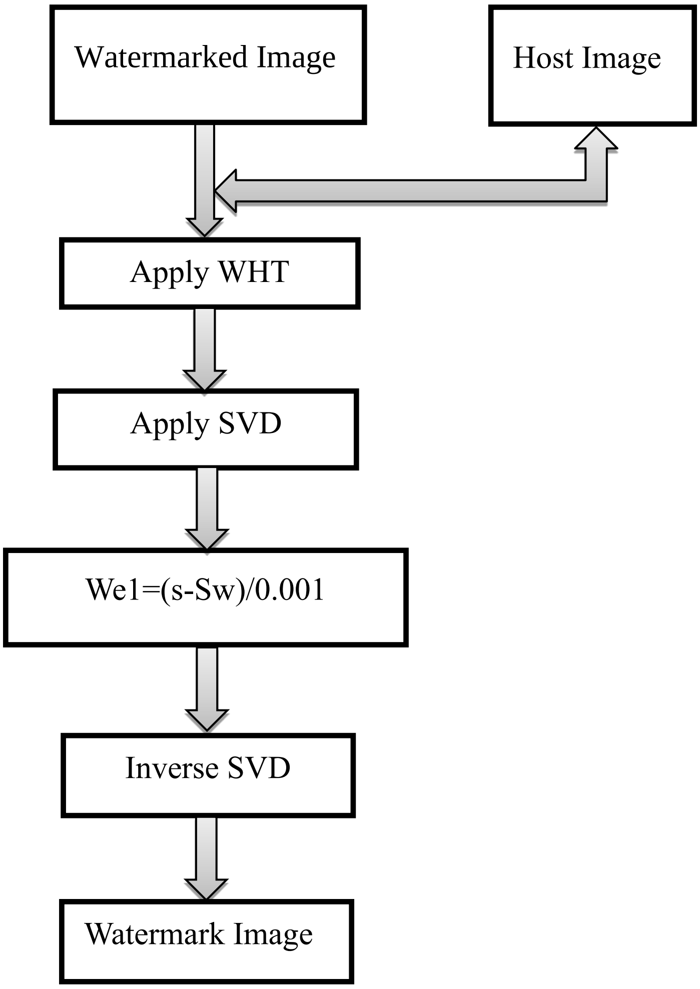


Fig 4.3 Watermark Extraction Procedure flowchart

4.4 Watermark Extraction Algorithm

The watermark extraction algorithm is as follows:

Start

Step 1: Read watermarked image

Step 2: Decompose the Watermarked image into set of coefficients using WHT**.**

Step 3: Apply SVD to the FWHT-transformed watermarked image.

Step 4: The applied SVD generates the three singular matrices, which are used for easy embedding and extraction**.**

Step 5: To get the original image from the transformed image subtract the diagonal matrix of the svd-based watermarked image from the host image and divide with the scalar factor.

Step 6: Reconstruct the watermark image by applying inverse SVD.

Stop.

The watermark extraction procedure is the direct reversal of the watermark embedding procedure. The watermarked encrypted image is decomposed using the same transform used in the embedding process, which means that the transformed co-efficients are processed to extract the frequency domain watermark. In this experiment, the author decomposed the image using two-dimensional WHT to obtain the coefficients of the Image, so that it can be easy for users to embed or extract the image from the selected set of pixels. The higher the DWT level, the better the concealing effect of embedding the watermark.

4.5 Proposed Methods

The proposed methods for watermark embedding and extraction using WHT-SVD is as follows:

4.5.1 Proposed Embedding Algorithm

The proposed watermarking scheme implement a hybridization of the (FWHT) and (SVD). The proposed algorithm for the watermark embedding process For a host image and a watermark image, each with a dimension of (512x512), the algorithm's procedures are as follows:

1. Partition the host image and so the watermark image into three channels or blocks: (red, green, blue).

2. Apply the (FWHT) on each channel of the host image and similar for the watermark image.

3. Apply the (SVD) on each channel and convert it into three U, S, and V matrices, each is with (512x512) dimensions.

4. Find the singular values of the host image and then modify them by the singular values of the watermark image using the following equation:

$$Snew = Shost + \alpha \text{ x } Swatermark$$

where α is set to a value of 0.10.

5. Apply the inverse (SVD) as follows:

$$Wnew = Uhost \text{ x } Swatermark \text{ x } VT$$

6. Find the inverse (FWHT) to acquire the watermarked image.

7. Combine the three channels: (red, green, blue).

8. Repeat all the above procedures for another watermark image.

4.5.2 Proposed Extraction Algorithm

The proposed process of the watermark extraction is a nonblind watermarking, given the fact that it uses and copies both the original image and the embedded watermark image that are necessary for the extraction. The process steps are as follows:

1. Apply the FWHT on the watermarked image and on the host image.
2. Apply the SVD on the FWHT transformed watermarked image.
3. Subtract the singular values of the host image from the singular values of the watermarked image, as follows:

$$Swnew = Swatermark - Shost$$

4. Apply the inverse SVD to acquire the extracted watermark image, as follows:

$$Wext = Uw*Swnew*VT$$

5. Apply the inverse FWHT.

4.6 Fast Walsh Hadamard Transform (FWHT)

In this paper, we present the WHT combined with SVD (FWHT-SVD) as a new approach in the digital image watermarking scheme based on Hadamard transform. The WHT is applied on the original watermark before it is embedded into the coefficients of the host image. The motivation to apply this transform is that it offers several advantages such as higher image fidelity. The initial experiment using FWHT-SVD has been performed, as in the further experiments and analysis is performed in this paper as an improvement of the initial project, which is organized as follows.

The proposed FWHT-SVD image watermarking scheme is described in provides the measures used to analyze the watermark performance. The Hadamard transform matrix is an orthogonal square matrix that only has 1 and -1 element values. This transform is also known as Walsh-Hadamard transform.

HI is the smallest Hadamard matrix and it is defined as Fast Walsh Hadamard Transform. The Walsh-Hadamard transform returns sequency values. Sequency is a more generalized notion of frequency and is defined as one half of the average number of zero-crossings per unit time interval. Each Walsh function has a unique sequency value.

The basic block diagram of FWHT is shown below:

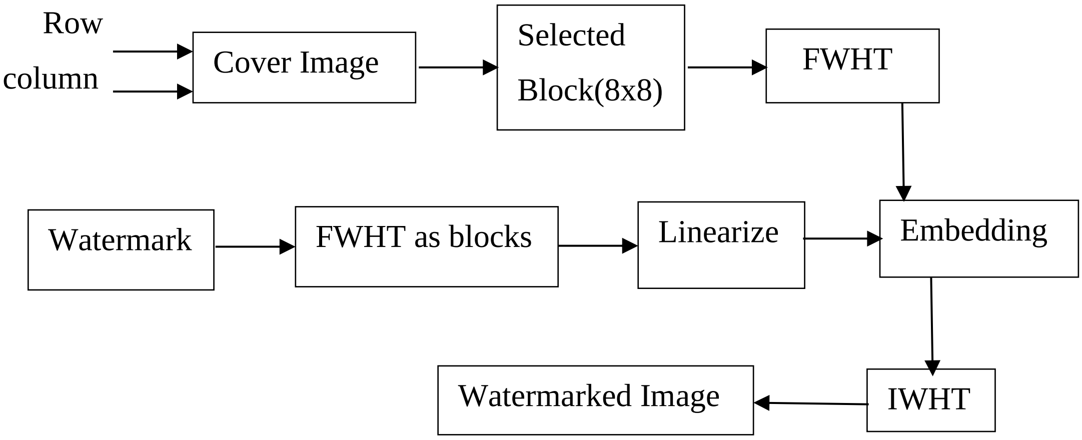


Fig 4.4 Basic blocks of FWHT

4.6.1 Advantages of WHT

The advantages of Walsh Hadamard Transform are:

- Low computational cost
- Robustness
- Security

4.7 Singular Value Decomposition

An image of the form C is factorized as a matrix in the singular value decomposition (SVD). It is divided into three matrices, U, S, and V, where U and V are mxm orthogonal matrices. In other words, V = 1 and U = I. The S, also known as S = dig(i), is a diagonal matrix with singular values 1, 2, ..., m. The (SVD) of C can be illustrated as shown below:

$$C = USV$$

4.8 Characteristics of Digital Image Watermarking Using MATLAB

The characteristics of digital image watermarking are shown below:

a) Inseparable

The embedded information can survive after compression, processing and format transformation.

b) Unchanging Data file size

The media of Data size cannot change before and after embedding operation because the embedded information is passed into the media.

c) Invisible/Inaudible

Without the use of digital content degradation, the information is embedded, because of the steps of embedding operation is small for human to identify the change**.**

d) Stages of Digital Image Watermarking Using MATLAB

Processing: How to modify original Data to embed watermark.

Location selection: where to embed watermark.

e) Types in Digital Image watermarking using MATLAB

Semi-private(semi-blind) watermarking.

Private (non-blind) watermarking
Public (blind) watermarking.

1.Semi-private(semi-blind) watermarking:

It tries for the question to answer. Evidence in court ownership is the major application of blind and semi-blind watermarking.

2.Private (non-blind) watermarking

The original cover Data are required for extraction/detection.

3.Extraction of watermarking

In market space, a simple watermarking system operates The process of map points in media space to plot points in other marking space original cover data not used for detection.

The extraction of the embedded watermark is the inverse procedure of watermark embedding and generation as shown in Fig. 4.3 After decomposing the to-be-checked image, the respective subbands are selected, where the watermark is embed-ded. The keys and the wavelet types used in the watermark generation and embedding process are supposed to be availableat the receiving end. The coefficients in the respective subbands are concatenated, permuted, and divide into groups in the similar way by using the same keys. The weighted mean of each group is calculated and the watermark bits are extracted by quantizing the weighted mean of each group

4.9 Applications of Digital image watermarking using MATLAB

- Broadcast monitoring
- Copyright protection
- Images and Document security
- Tracking digital content
- Tamper Detection
- Medical Applications

- Copy control
- Content Authentication
- Integrity Verification
- Finger printing
- Military

Some of the applications of Digital Image Watermarking using Matlab are:

1. Serialized Packaging

Digital watermarks can contain serialized data. When added to packaging, this allows for greater product traceability across the global supply chain. Consumer brands and food manufacturers can benefit from risk mitigation and real-time insight into product locations such as warehouses or distribution centers.

2. Brand Protection

Over or covert digital watermarks can be added to products, packaging, and labels, as well as product images. By using digital watermarks, brands can identify and take action against counterfeit products that are damaging their brand reputation and putting consumer safety at risk.

3. Digital Images & Documents

Digital image watermarking and document watermarking can help companies identify unauthorized use of digital assets. When digital watermarking is combined with other technologies, it is possible to track and trace sensitive images and document leaks to the source. Digital watermarks allow the brand to keep control over where digital brand assets are being used and stop unwanted distributions.

4. Audio

Digital audio watermarks can be integrated directly into audio files to identify and maintain important metadata and distinguish between individual versions of the same audio content.

When combined with blockchain technology, it can be a method for identifying music rights holders.

CHAPTER - 5
SOFTWARE INVOLVED

5.1 Software Used

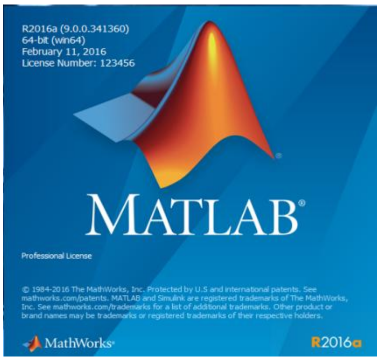
In this project we used Matlab R2016 a version software to obtain the simulation results visually. The following gives few information about Matlab software**.**

5.1.1 MATLAB

MATLAB is a numerical computing environment and programming language used for scientific and engineering computations. It is widely used in academia, industry, and research for tasks such as data analysis, signal processing, control systems design, image and video processing, and more.

With MATLAB, you can create, analyze, and visualize numerical data, as well as develop and run algorithms and applications. It provides a wide range of functions, tools, and libraries for numerical computation, data analysis, and visualization, and it has a user-friendly interface that makes it easy to use and learn. MATLAB also offers a variety of add-on toolboxes that extend its capabilities for specific areas of application, such as statistics, optimization, signal processing, and more.

Overall, MATLAB is a powerful and versatile tool for numerical computing and data analysis, used by a wide range of professionals and researchers in various fields. Here is the image of matlab software interface that is shown below:



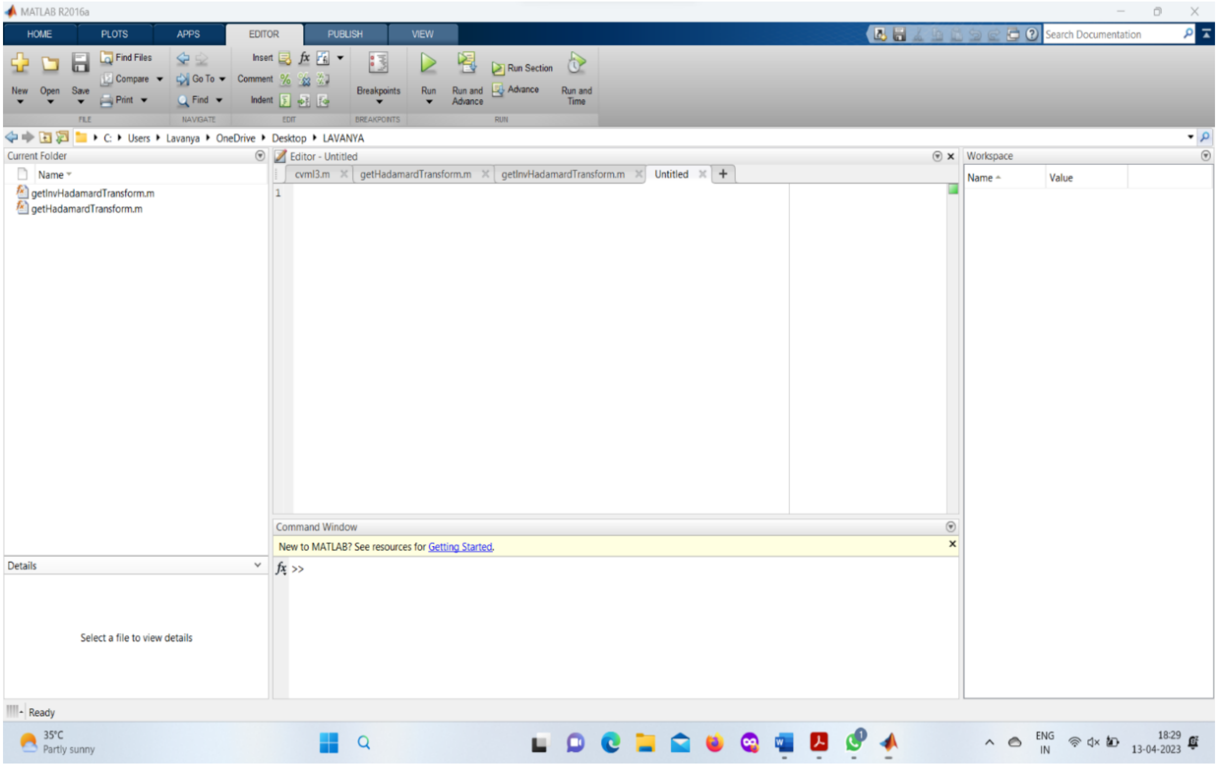
R2016a (9.0.0.341360)
64-bit (win64)
February 11, 2016
License Number: 123456

Professional License

© 1984-2016 The MathWorks, Inc. Protected by U.S and international patents. See mathworks.com/patents. MATLAB and Simulink are registered trademarks of The MathWorks, Inc. See mathworks.com/trademarks for a list of additional trademarks. Other product or brand names may be trademarks or registered trademarks of their respective holders.

Fig 5.1 desktop application of Matlab

The following fig. shows the internal view of matlab software:



New to MATLAB? See resources for Getting Started.

Select a file to view details

Fig 5.2 Matlab software Interface

5.1.2 Matlab Tools

MATLAB provides a wide range of built-in tools and functions for numerical computation, data analysis, and visualization. Some of the main tools in MATLAB include:

1. **MATLAB Editor**

   This is the primary interface for writing, executing, and debugging MATLAB code.

2. **Command Window**

   This is where you can enter and execute commands interactively.

3. **Plotting and Visualization**

   MATLAB provides tools for creating 2D and 3D plots, as well as visualizing data in various ways, such as histograms, scatter plots, and more.

4. **Workspace Window**

   This displays information about the variables currently in the workspace, including their names, sizes, and values.

5. **Current Folder Window**

   This displays the files and folders in the current working directory.

6. **Figure Window**

   This is where MATLAB plots and visualizations are displayed. You can create multiple figures and customize their properties.

7. **MATLAB Compiler**

   This allows you to compile MATLAB code into standalone applications or shared libraries for deployment.

Overall, MATLAB provides a rich set of tools and functions for numerical computation, data analysis, and visualization, making it a powerful and versatile tool for a wide range of applications.

5.1.3 Uses of Matlab

Matlab is a powerful software platform that is widely used in the scientific, engineering, and financial fields. Here are some common uses of Matlab:

1.Numerical computation

Matlab is an excellent tool for performing complex numerical computations. It offers a range of built-in functions and libraries that allow users to perform tasks such as matrix operations, solving differential equations, and optimization.

2.Data analysis

Matlab is also useful for analyzing and visualizing data. It has built-in functions for statistical analysis, curve fitting, and signal processing.

3.Image and signal processing

Matlab is widely used in the field of image and signal processing. It has built-in functions for image filtering, enhancement, and segmentation.

4.Machine learning and deep learning

With its powerful libraries for machine learning and deep learning, Matlab is becoming increasingly popular in the field of artificial intelligence.

5.Financial analysis

Matlab is also used in finance for tasks such as portfolio optimization, risk management, and options pricing.

Overall, Matlab is a versatile software platform that can be used for a wide range of tasks in various fields

CHAPTER - 6
EXPERIMENTAL RESULTS

6.1 Experimental Results

The Experimental results of robust hybridized watermarking using Walsh Hadamard Transform and Singular Value Decomposition are as follows.

6.1.1 Inputs

In this project we took a cover image i.e., host image and a watermark image as inputs. The cover image is the image to which a watermark image is inserted by the process called “Embedding”. This process is used to protect the valuable data or information that is presented inside the watermark image itself. For this we used an image transformation technique i.e., Walsh Hadamard Transform and Singular Value Decomposition to embed the watermark into the cover image by converting the image into set of coefficients. After all these the obtained watermark inserted cover image is known as “Watermarked Image”

Here, we also used a process to remove the watermark image from the watermarked image known as “Extraction”. With this the user can extract the information that is hidden inside the cover image.

The images we used as inputs in this project are given below:

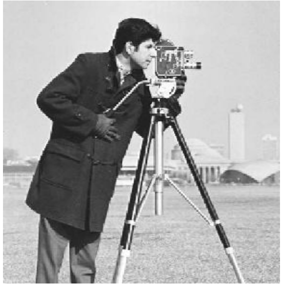


Fig 6.1 Cover Image

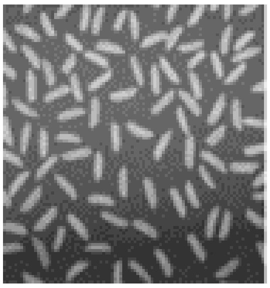
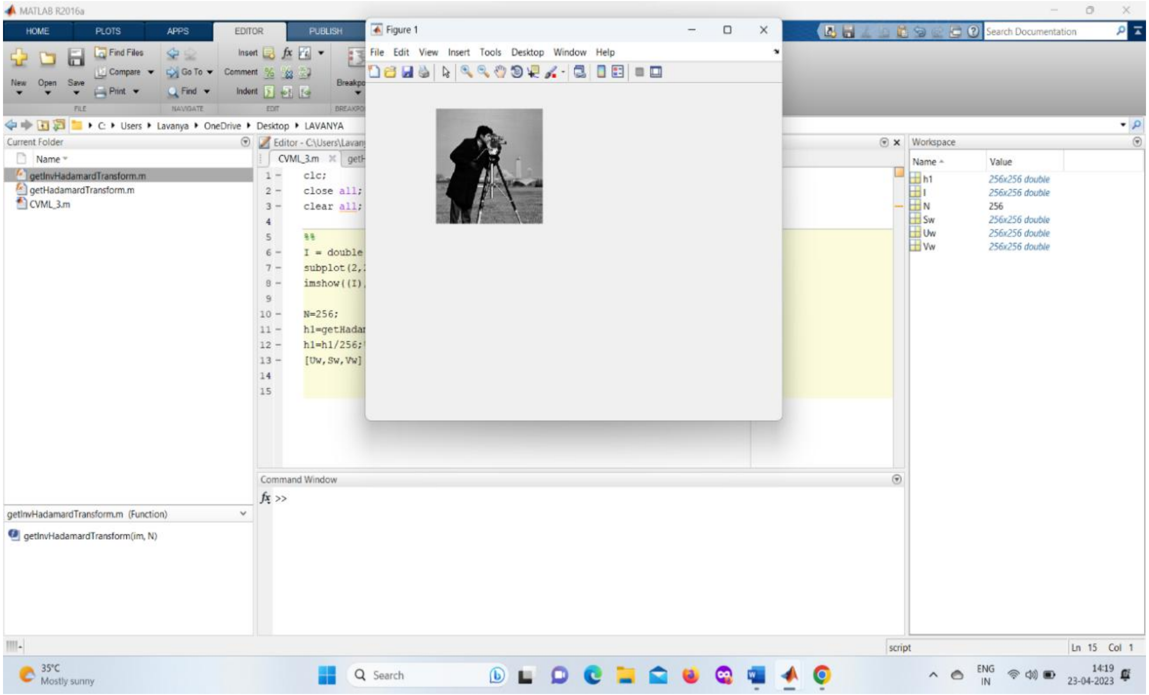


Fig 6.2 Watermark Image

6.1.2 Output Screens

❖ Cover Image

In this work we took a grayscale image i.e., cover image as input which is visible to the user when a watermark image is inserted into it.



getInvHadamardTransform.m
getHadamardTransform.m
CVML_3.m

getInvHadamardTransform.m (Function)
getInvHadamardTransform(im, N)

```
clc;
close all;
clear all;

%%
I = double
subplot(2,
imshow((I)

N=256;
h1=getHadar
h1=h1/256;
[Uw,Sw,Vw]
```

Name	Value
h1	256x256 double
I	256x256 double
N	256
Sw	256x256 double
Uw	256x256 double
Vw	256x256 double

```
>>
```

script   Ln 15   Col 1

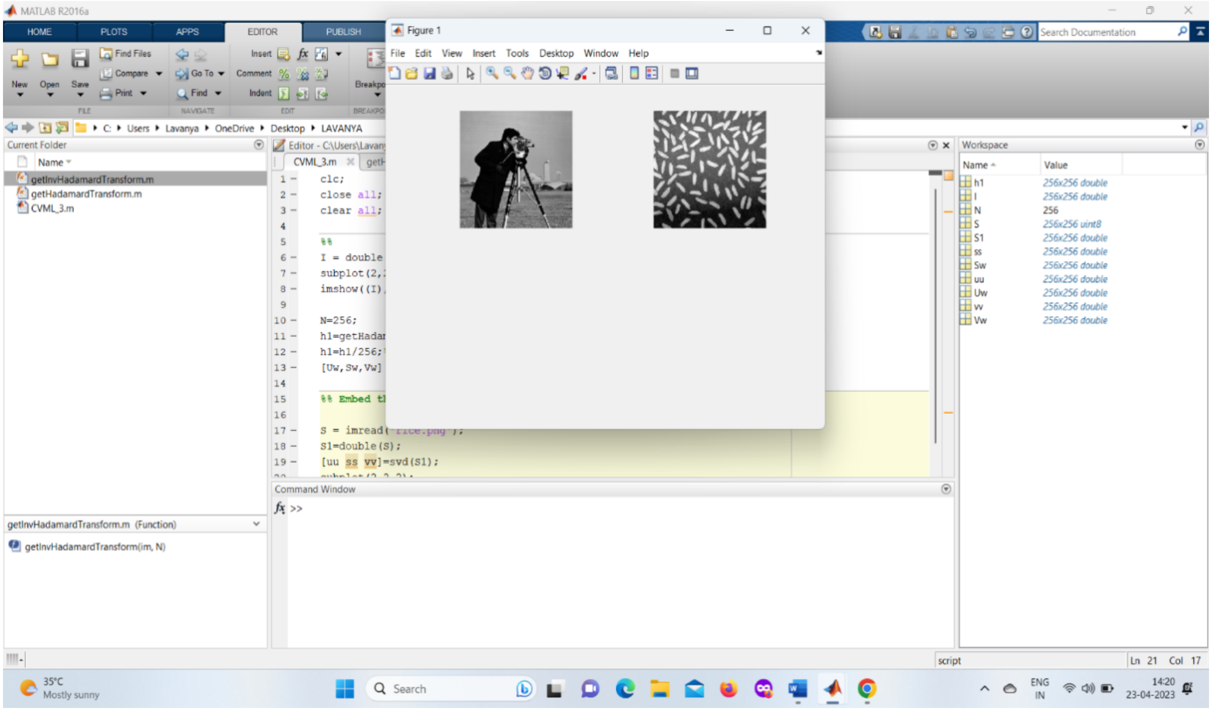
Fig 6.3 Reading and displaying cover image

from the above fig. we can observe that the cover image is displayed on the output screen of matlab software. First we have to read the input cover image and its size by using the “imread()” function. As the range of grayscale image is between 0-256, if the size of the input image is more than the actual size then we can use “double()” function to read the size of the image. After that by using “subplot(m,n)” and “imshow()” we can plot the image and display the input cover image.

Further, the Walsh Hadamard transform is applied using “getHadamardTransform()” function that converts the image into transformed image(set of coefficients) and singular value decomposition is applied to the transformed image to convert the image into three singular matrices(UU SS VV), that can be helpful for further use.

❖ Watermark Image

A watermark image is the image or text or signal that consists of valuable information that is prone to attacks. To protect from attacks Watermark image can be made invisible by inserting it into a cover image. Later, the user can use the information present in that cover image by removing the watermarks with the keys available.



```
clc;
close all;
clear all;

%%
I = double
subplot(2,
imshow((I)

N=256;
h1=getHadar
h1=h1/256;
[Uw,Sw,Vw]

%% Embed tl

S = imread('rice.png');
S1=double(S);
[uu ss vv]=svd(S1);
```

```
>>
```

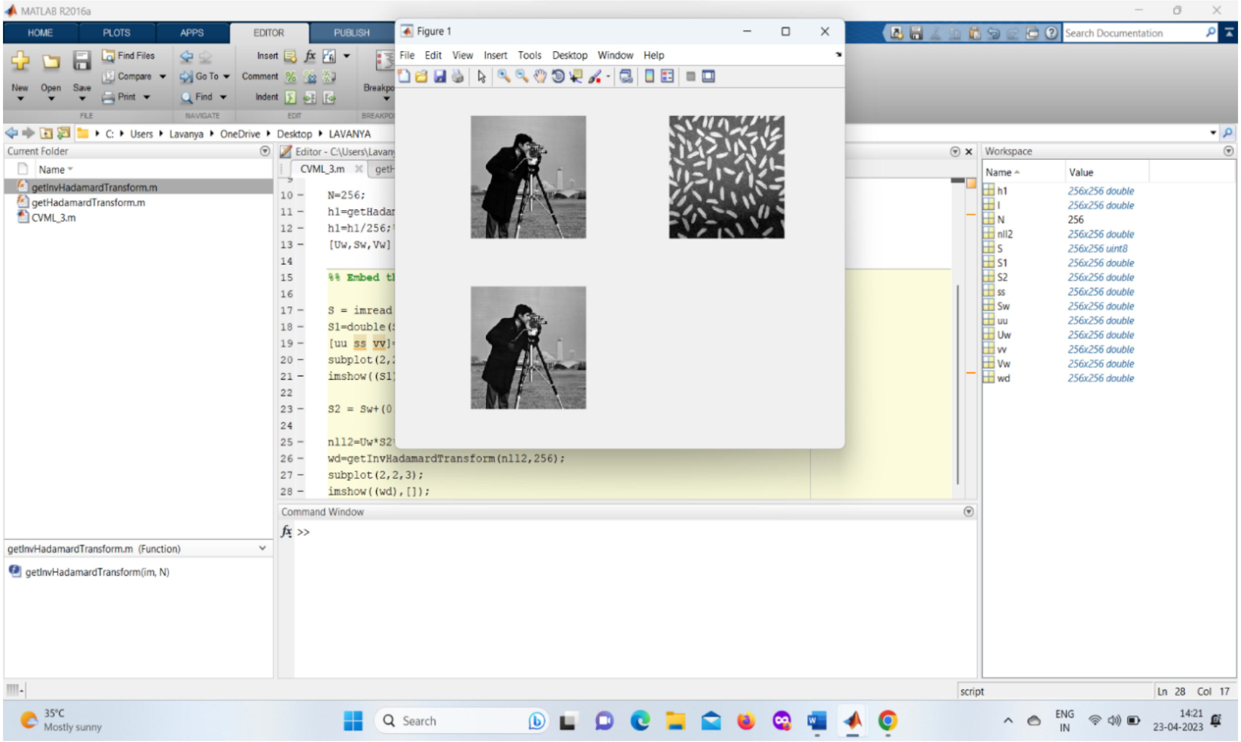
Name	Value
h1	256x256 double
I	256x256 double
N	256
S	256x256 uint8
S1	256x256 double
ss	256x256 double
Sw	256x256 double
uu	256x256 double
Uw	256x256 double
vv	256x256 double
Vw	256x256 double

Fig 6.4 Cover Image and Watermark Image

from the above fig. we can say that the watermark image is first read and then it can be plot and displayed using certain functions same as that of cover image. Further, the singular value decomposition can be applied to the watermark image to convert the image into three singular matrices(u s v) that can be helpful for further use.

❖ Watermarked Image

A watermarked image is the image that can be obtained by embedding the watermark image into the cover image. We cannot Embed the watermark directly into the cover image. For this we have to add the singular matrices of both the host image and watermark image and multiply with a singular matrix i.e.,0.001. The watermarked image can be obtained by using "getInvHadamardTransform()" function.



```
N=256;
h1=getHadar
h1=h1/256;
[Uw,Sw,Vw]

%% Embed tl

S = imread
S1=double(
[uu ss vv]
subplot(2,
imshow((S1)

S2 = Sw+(0

nl12=Uw*S2
wd=getInvHadamardTransform(nl12,256);
subplot(2,2,3);
imshow((wd),[]);
```

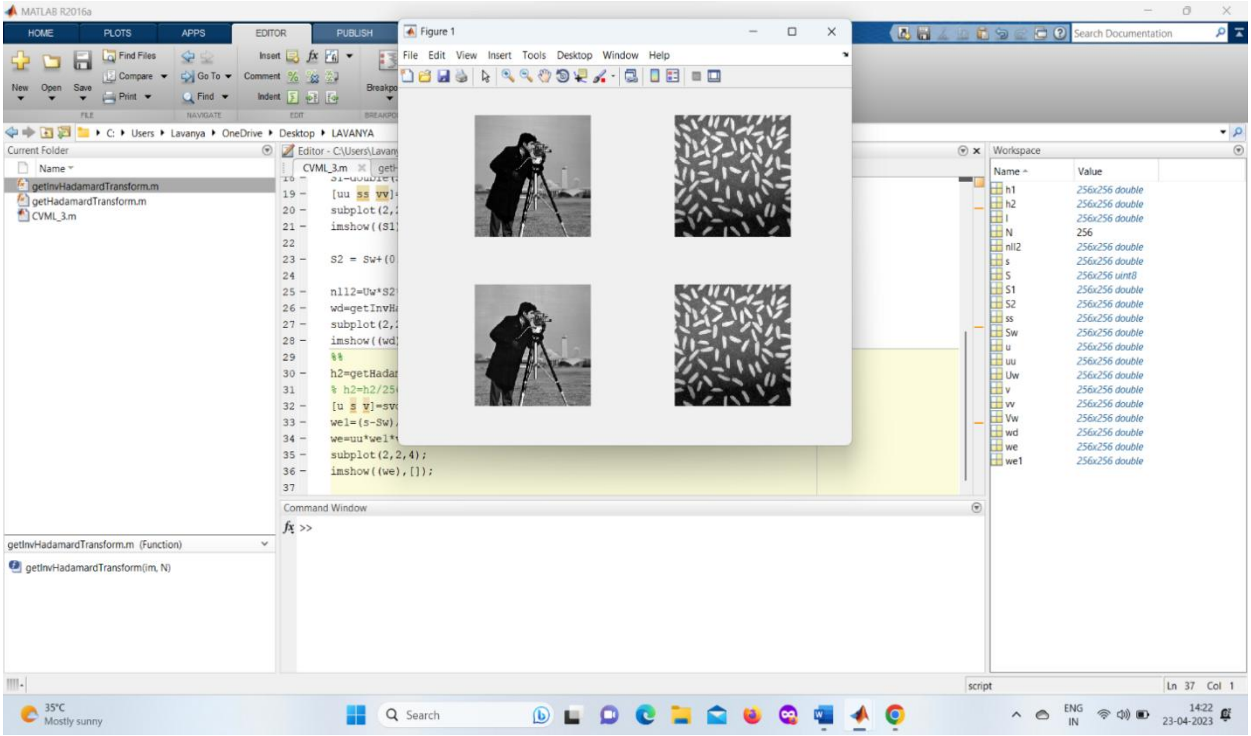
Name	Value
h1	256x256 double
I	256x256 double
N	256
nll2	256x256 double
S	256x256 uint8
S1	256x256 double
S2	256x256 double
ss	256x256 double
Sw	256x256 double
uu	256x256 double
Uw	256x256 double
vv	256x256 double
Vw	256x256 double
wd	256x256 double

Fig 6.5 Obtained watermarked Image

from the above figure we observe that there are different images are displaying, they are the cover image and the watermarked image. Here watermark is added to the original image then there is no difference is observed between the original image and the watermarked image.

❖ Recovered Image

Here we can observe the outputs of the digital image watermarking using the Walsh Hadamard Transform and Singular Value Decomposition using Matlab. We can see the afferent images while each image is attacking with different attacks. Here watermark is extracted from the watermarked image.



getInvHadamardTransform.m
getHadamardTransform.m
CVML_3.m

getInvHadamardTransform.m (Function)

getInvHadamardTransform(im, N)

```
    S1=double(
    [uu ss vv]=
    subplot(2,2
    imshow((S1)

    S2 = Sw+(0

    nll2=Uw*S2
    wd=getInvHa
    subplot(2,2
    imshow((wd)
    %%
    h2=getHadam
    % h2=h2/25
    [u s v]=svd
    we1=(s-Sw)/
    we=uu*we1*v
    subplot(2,2,4);
    imshow((we),[]);
```

```
>>
```

Name	Value
h1	256x256 double
h2	256x256 double
I	256x256 double
N	256
nll2	256x256 double
s	256x256 double
S	256x256 uint8
S1	256x256 double
S2	256x256 double
ss	256x256 double
Sw	256x256 double
u	256x256 double
uu	256x256 double
Uw	256x256 double
v	256x256 double
vv	256x256 double
Vw	256x256 double
wd	256x256 double
we	256x256 double
we1	256x256 double

fig 6.6 Final watermarked image and extracted watermark

CONCLUSION & FUTURE SCOPE

CONCLUSION

To enhance the security of data exchanged in telemedicine, in this work we had proposed a watermarking approach combining WHT and SVD. The proposed approach protects the images exchanged in telemedicine but also avoids any confusion among patient records (even at the local level). It is found that the proposed method is robust against band attacks. Using the MATLAB R2016 software, the proposed algorithm's numerical simulation is carried out. As a test image we used a grayscale host image coupled with watermark picture. The image's dimensions were designed to be uniform for accurate comparison and better visualizing the results. To check the availability of the watermark in the image, extraction must be done to show whether there is any information in the image.

FUTURESCOPOE

In this project, the image used is a grayscale image. A grayscale image is the easiest picture that can be processed by using an image processing technique because it only has one layer. Therefore, this technique is created more on the grayscale image rather than the colour image. The watermark embedded inside the colour image is hard to be extracted for this technique because it contains three layers. Future work recommended is to do more work on embedding and extracting a watermark from the colour image which is commonly used in this era. On the other hand, a system that can perfectly extract a watermark from a watermarked image is recommended for future research. The watermark with less distortion can prove the copyright of the owner on the digital product.

REFERENCES

[1] M. M. Abd-Eldayem, A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine, Egyptian Informatics Journal 14 (1) (2013) 1–13.

[2] S. Singh, R. K. Arya, H. Sharma, A robust deinterlacing multiple image watermarking technique in dwt, in: 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), IEEE, 2016, pp. 8–13.

[3] A. Benoraira, K. Benmahammed, N. Boucenna, Blind image watermarking technique based on differential embedding in dwt and dct domains, EURASIP Journal on Advances in Signal Processing 2015 (1) (2015) 55.

[4] P. K. Dhar, T. Shimamura, A blind lwt-based audio watermarking using fast walsh hadamard transform and singular value decomposition, in: 2014 IEEE International Symposium on Circuits and Systems (ISCAS), IEEE, 2014, pp. 125–128**.**

[5] R. Bamal, S. S. Kasana, Dual hybrid medical watermarking using walsh-slantlet transform, Multimedia Tools and Applications 78 (13) (2019) 17899–17927.

[6] S. M. Darwish, O. F. Hassan, A new colour image copyright protection approach using evolution-based dual watermarking, Journal of Experi- mental & Theoretical Artificial Intelligence (2020) 1–23.

[7] N. Salem, S. Hussein, Data dimensional reduction and principal components analysis, Procedia Computer Science 163 (2019) 292–299.

[8] T. Khanam, P. K. Dhar, S. Kowsar, J.-M. Kim, Svd-based image watermarking using the fast walsh-hadamard transform, key mapping, and coefficient ordering for ownership protection, Symmetry 12 (1) (2020) 52.

[9] E. E. Abdallah, A. F. Otoom, A. E. Abdallah, M. Bsoul, S. Awwad, A hybrid secure watermarking scheme using nonnegative matrix factoriza- tion and fastwalsh-hadamard transform, Journal of Applied Security Research 15 (2) (2020) 185–198.

[10] E. M. El Houby, N. I. Yassin, Wavelet-hadamard based blind image watermarking using genetic algorithm and decision tree, Multimedia Tools and Applications 79 (37) (2020) 28453–28474.

[11] M. K. Abdmouleh, A. Khalfallah, M. S. Bouhlel, A new watermarking technique for medical image using hierarchical encryption, arXiv preprint arXiv:1409.4587 (2014).

[12] Y. Wu, J. P. Noonan, S. Agaian, et al., Npcr and uaci randomness tests for image encryption, Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT) 1 (2) (2011) 31–38.

[13] S. Thakur, A. K. Singh, S. P. Ghrera, M. Elhoseny, Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications, Multimedia tools and Applications 78 (3) (2019) 3457–3470.

[14] S. Thakur, A. K. Singh, S. P. Ghrera, A. Mohan, Chaotic based secure watermarking approach for medical images, Multimedia Tools and Applications 79 (7) (2020) 4263–4276.

TEXTBOOKS

- "Digital Watermarking and Steganography: Fundamentals and Techniques" by Frank Y. Shih
- "Multimedia Security: Watermarking, Steganography, and Forensics" by Stan Z. Li and Yun Q. Shi
- "Information Hiding Techniques for Steganography and Digital Watermarking" by Stefan Katzenbeisser and Fabien A. P. Petitcolas

WEBLINKS

- "Image Watermarking using SVD" by Dr. V. Rajinikanth, Assistant Professor, Department of ECE, SRM Institute of Science and Technology: https://www.researchgate.net/publication/330603346_Image_Watermarking_using_SVD

- "Image Watermarking using Walsh Hadamard Transform (WHT)" by Dr. Rakesh Kumar, Professor, Department of Computer Science and Engineering, National Institute of Technology, Kurukshetra: https://www.researchgate.net/publication/323811695_Image_Watermarking_using_Walsh_Hadamard_Transform_WHT

- "Digital Image Watermarking using SVD and DWT Techniques: A Comparative Study" by Dr. P. S. Hiremath, Associate Professor, Department of Electronics and Communication Engineering, KLE Dr. M. S. Sheshgiri College of Engineering and Technology: https://www.researchgate.net/publication/313860369_Digital_Image_Watermarking_using_SVD_and_DWT_Techniques_A_Comparative_Study

- "A Survey of Image Watermarking Techniques" by T. Usha Rani, Research Scholar, Department of Electronics and Communication Engineering, Jawaharlal Nehru Technological University, Anantapur: https://www.researchgate.net/publication/328336141_A_Survey_of_Image_Watermarking_Techniques

Appendix

```
clc;
close all;
clear all;

%%
I = double(imread('cameraman.tif'));
subplot(2,2,1);
imshow((I),[]);

N=256;
h1=getHadamardTransform(I,N);
h1=h1/256;%% Apply SVD  on LL2
[Uw,Sw,Vw] = svd(h1);

%% Embed the watermarks in

S = imread('rice.png');
S1=double(S);
[uu ss vv]=svd(S1);
subplot(2,2,2);
imshow((S1),[]);

S2 = Sw+(0.001*ss);

nll2=Uw*S2*Vw';
wd=getInvHadamardTransform(nll2,256);
subplot(2,2,3);
imshow((wd),[]);
%%
h2=getHadamardTransform(wd,N);
```

```
% h2=h2/256;%% Apply SVD
[u s v]=svd(h2);
we1=(s-Sw)/(0.001);
we=uu*we1*vv';
subplot(2,2,4);
imshow((we),[]);
```