**Adama Science and Technology University**

**School of Applied Natural Science**

**Department of Applied Mathematics**

**Final Research Project**

**On**

# Watermarking Colored Digital Image Using Singular Value Decomposition for Data Protection

**By**

Adugna Fita

*fitaadu@yahoo.com*

*adugna.fita@astu.edu.et*

***Applied Mathematics Program***

Bullo Endebu

***Applied Mathematics Program***

**Jan, 2020**

*Adama, Ethiopia*

## Abstract

Digital watermarking is the process of embedding information into a digital signal such as image, video, audio data to easily identify the ownership of the original data. Such information is embedded for many different purposes, such as copyright protection, source tracking, piracy deterrence, tamperproof etc. Therefore, it shall be embedded in a way that makes it difficult to be visualize with human eye and difficult to be removed. As computers are more and more integrated via the network, the distribution of digital data is becoming faster, easier, and requiring less effort to make exact copies. One of the current research areas is to protect digital watermark inside the information so that ownership of the information cannot be claimed by third party. In this paper, we propose an algorithm for colored digital image watermarking technique based on singular value decomposition. This study covers embedding algorithm and watermark extraction algorithm while both host and watermark images are colored. The quality of the watermarked image is tested through experiment against most common attacks such as image compression, filtering, cropping, injection of noise, blurring, and sharpening. Standard benchmark was used to test the robustness of the proposed watermarking algorithm. Experimental result shows that the algorithm is robust against geometric attacks.

**Acknowledgments**

First of all, we would like to express our deepest and special thanks to Adama Science and Technology University, Department of Applied Mathematics for their all rounded support including fund. We would like to extend our thanks to colleagues for their incredible comments.

**Contents** **Pages**

Abstract ..... ii
Acknowledgments ..... iii

Table of Contents ..... iv

Lists of figures and tables ..... v

*CHAPTER ONE*

*1* Introduction and Background ..... 1
1.1 Literature review ..... 2
1.2 Application Areas ..... 5
1.3 Objective of the study ..... 8
1.4 Methodology ..... 8

CHAPTER TWO

2 Mathematical Preliminaries ..... 9
2.1 Matrices ..... 9
2.2 Singular Value Decomposition ..... 12
2.3 The associated eigenvalues problems ..... 14

CHAPTR THREE

3 Colored Image Watermarking ..... 17
3.1 Embedding ..... 17
3.2 Extraction process ..... 18
3.3 Experimental Results ..... 20
4 Results and Discussion ..... 25
5 References ..... 26
6 Appendix ..... 28

## LIST OF FIGURES

**Figure 1**: Image pixels at given position ..... 17

**Figure 2**: Images show RGB components..... 17

## LIST OF TABLES

**Table 1**: The first row contains Host images while second row contains corresponding watermark images..... 20

**Table 2**: The Host, watermark, watermarked and extracted watermark at **($\alpha = 0.2$)**..... 21

**Table 3**: Extracted watermarks after different attacks (Experiment 1)..... 22

**Table 4**: Extracted watermarks after different attacks (Experiment 2)..... 23

**Table 5**: Extracted watermarks after different attacks (Experiment 3)..... 24

# CHAPTER ONE

## 1. Introduction and Background

Nowadays digital multimedia is undergoing dramatic changes; Digitized information is used in every possible area of our life. Images, texts, audio, video files contain information normally stored on conventional media and easily shared through internet.

However, all of these advancements lead to a serious problems of security, misuse and copyright problems. One of the most widely used copyright protection methods is digital watermarking.

Digital watermarking is the process of embedding watermark or information into a digital signal such as image, audio or video data to easily identify the ownership of the file and shall be embedded in a way that makes it difficult to be removed. Such information is embedded for many different purposes, such as copyright protection, source tracking, owner identification, broadcast monitoring, content authentication, copy control, piracy deterrence, tamperproof, etc.,

Over the past few years, digital watermarking has emerged as a leading candidate that could solve the fundamental problems of legal ownership [1].

In order to raise the respect for the intellectual property, digital watermarking technique has been proposed as a method to embed an invisible or visible signal into multimedia data so as to check the owner identification of the data and discourage the unauthorized copying. Unlike encryption, which is useful for transmission but does not provide a way to examine the original data in its protected form, the watermark remains in the content in its original form and does not prevent a user from listening, viewing, examining, or manipulating the content. Also, unlike the idea of steganography, where the method of hiding the message may be secret and the message itself is secret, in watermarking, typically the watermark embedding process is known and the message does not has to be secret [1].

### 1.1 Literature Review

According to the domain in which the watermark is inserted, these techniques are classified into two categories, i.e., spatial domain and transform domain methods [2]. The spatial domain methods modify the digital data (pixels) directly to hide the watermark bits and possess the advantage of low computational complexity. On the other hand, the transform (frequency) domain methods do not alter the pixel values directly but rather modify the transform coefficients to hide the watermark bits such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) [3, 4].

In [3], a hybrid image watermarking technique based on DWT and SVD has been presented where the watermark is embedded on the singular values of the cover image's DWT sub bands. The technique fully exploits the respective feature of these two transform domain methods: spatial-frequency localization of DWT and SVD efficiently represents intrinsic algebraic properties of an image. In [4], novel dual watermarking mechanism has been proposed for digital media that embeds a visible pattern into the spatial domain and an invisible logo into the frequency domain. The visible watermark indicates the ownership of the protected image through visual perception. Furthermore, even if the visible watermarked image incurs tampering, we can retrieve the invisible watermark to prove the copyright of the image. Only an authorized user can remove the dual watermarks to obtain an unmarked image with high fidelity. A hybrid image watermarking technique [5] has been presented for data hiding over Internet. The idea of the proposed technique is based on fusing multiple watermark images using wavelet fusion algorithm and embedding the resultant fused watermark in the original image using hybrid DWT-SVD watermarking algorithm to produce the watermarked image. The image watermarking technique using the hybrid DWT-SVD is more robust than that using the SVD only. The results also prove that the proposed watermarking technique improves both the capacity of the embedded information and robustness without affecting the perceptual quality of the original image. In [6], authors aimed at developing a hybrid image watermarking algorithm which satisfies both imperceptibility and robustness requirements. In order to achieve the objectives they have used singular values of wavelet transformation's HL and LH

sub bands to embed watermark. A secret embedding key is designed to securely embed the fragile watermarks so that the new method is robust to counterfeiting, even when the malicious attackers are fully aware of the watermark embedding algorithm. The DWT and DWT-SVD watermarking schemes had been proposed in [7] and there comparative study was done using the different peak signal to noise ratio (PSNR) values taken over different values of scale factor in gray scale images. In both DWT and DWT-SVD, two-level decomposition was performed and then after decomposing the host and watermarking images, singular values of the images were modified using SVD over the sub-bands.

Wavelet domain is a promising domain for watermark embedding. DWT is an orthogonal transform similar to the Discrete Cosine Transform that can be used for the audio and video compression, speech recognition, feature extraction, finger print, watermarking and many other applications in biomedical engineering [8]. This is a frequency domain technique in which firstly cover image is transformed into frequency domain and then its frequency coefficients are modified in accordance with the transformed coefficients of the watermark and watermarked image is obtained which is very much robust. In single level decomposition, DWT decomposes image hierarchically, providing both spatial and frequency description of the image. It decompose an image in basically three spatial directions i.e., horizontal, vertical and diagonal in result separating the image into four different components namely LL, LH, HL and HH. Here first letter refers to applying either low pass frequency operation or high pass frequency operations to the rows and the second letter refers to the filter applied to the columns of the cover image. LL level is the lowest resolution level which consists of the approximation part of the cover image. Rest three levels i.e., LH, HL, HH give the detailed information of the cover image [9].

In all transfer domains watermarking such as Discrete Cosine Transforms, Discrete Wavelet Transform and Discrete Fourier Transform (DFT), use linear transform of image intensity to frequency domain. The image is passed through a number of high-pass filters, also known as wavelet functions, to analyze the high frequencies and it is passed through a number of low-pass filters, also known as scaling functions, to

analyze the low frequencies. After filtering, half of the samples can be eliminated according to the Nyquist criteria. The advantages of transform domain watermarking are robustness against attacks like filtering, compression and resistance against frequency attacks. But The drawbacks of transform domain based watermarking are: not robust against geometric attacks, block effect, when image is reduced to higher compression ratios, these blocks become noticeable.

Wavelet filters produces blurring and noise near edge and DFT produce Complex output and complexity of Calculation. Cropping in the spatial domain changes the frequency sampling step and quantization [12, 13].

In this work, we focused on the invisible watermarking techniques based on singular value decomposition by embedding secrete image or message in singular vectors; both right and left singular unitary matrices are explored for watermarking algorithm. Singular value decomposition (SVD) is a mathematical based on linear algebra and used by factorization of a real matrix or complex matrix, with many useful applications in image processing. The use of SVD decomposition in the image hashing problem was proposed by (Kozat et al, 2004, vol. 5, pp. 3443 – 3446) [14], where SVD decomposition is used twice and has been shown to be robust to some small variations in rotation and scaling.

The singular value method of coding proposed in this work is in order to increase the security of watermarked image in transformed space.

The main advantages of using SVD from the viewpoint of image processing and properties of SVD to employ in digital watermarking schemes are [13]:

The singular values (SVs) of an image have very good stability, (i.e., small perturbation in SVs does not change the image significantly; Each singular value specifies the luminance of an image layer while the corresponding pair of singular vectors specifies the geometry of the image.

There is no need to embed all the SVs of a visual watermark. Depending on the magnitudes of the largest singular values, it will be sufficient to embed only few

singular values. SVD algorithms are highly strong against extensive range of attacks and no constraint on size of watermark and host matrices in SVD technique of watermarking.

### 1.2 Application Areas

Digital Watermarking describes methods and technologies that embed hidden information, for example a number or a string, in digital media, such as images, video, audio or any other kind of noise-tolerant digital signal such as multimedia data [8]. Digital watermarks can be easily detected and read by computers, networks and a variety of digital devices, validating the original content and/or initiating or preventing actions. Figure 1 illustrates the workflow of any watermark. Initially, the watermark is embedded inside the original image.

Then, the watermarked imaged is copied and (or) distributed.

After that, the image is often cropped, resized, compressed, etc. However the metadata within the watermark has to remain unchanged to allow traceability.

In the following, some existing application areas are described together with the reference technologies, and case studies are presented, highlighting some of the most common real world scenarios. Most of the examples shown refer to the watermarking of digital images, but they are in general applicable to other media, such as audio or video streams.

#### i. Copyright protection

The first application area to which watermarking was employed is the copyright protection of digital media. In the digital world it is possible for almost anyone to duplicate or manipulate digital data without losing quality.

This has allowed previously unseen copyright infringement issues. Digital watermarking provides an added layer of security to the content protection chain to deter unauthorized use/duplication of content by embedding watermarks that identify the original media and the permitted uses of the content.

In such a scenario, devices read the watermark during playback or copying of the content. If the watermark indicates that the use is unauthorized, the playback or copying is prevented (other actions are also possible, e.g. the audio is muted), and an explanatory message may be displayed.

Effective content protection helps content owners to protect audio, film and video entertainment content, communicate copyright ownership and usage rights of their content, protect it against common threats of piracy including camcorder recording, peer-to-peer file sharing, copying, format conversion, encoding and other forms of re-processing.

### ii. Content identification and management

Digital watermarking enables effective content identification by providing a unique digital identifier to all forms of media content in a way that persists with the content wherever it may travel. Digital watermarks are easily embedded into content without interfering with the consumer's enjoyment of it. It is imperceptible to humans, but easily detected and understood by computers, networks and a wide range of common digital devices. The watermark can carry such information, such as the owner identity, how it may be used or anything else the owner wants to convey. It can also trigger predefined actions, including linking to websites or other consumer experiences. Content identification helps:

- Consumers to find the content they are looking for, learn more about it, try it out, and locate where and how to purchase it;
- Copyright owners, brands and distributors to locate and learn about how, when and where content is being consumed and identify the source of leaks when confidential content inadvertently or intentionally makes its way onto the Internet.

### iii. Content filtering: triggering of actions and blocking

The data carried in the digital watermark can be rapidly cross correlated with other content or actions. On the one hand, a specific action or even piece of content can be triggered upon identification of the watermark, allowing customer interactivity. For instance, while watching a scene in a movie, a specific call to action (e.g., "Press the red button on your remote to find out more") could be triggered.

Similarly, a specific and targeted advertisement could be triggered. Instead of a commercial appearing at regular times, the commercial could be triggered according to what content is being watched and at specific times within the content.

On the other hand, digital watermarks could be used for blocking specific contents. Upon recognition and identification of a particular situation, the content could be blocked. Such applications can prove extremely useful for the Internet, such as blocking a copyrighted piece of audio or video from being uploaded to a website. Additionally, to ensure child safety and prevent children from being exposed to adult content, specific rules could be set up by the parent to warn, restrict or completely block the viewing of such content.

**iv. Online contents**

In the corporate world, images, documents and video quickly spread through emails and across the World Wide Web. In the case of major brands, for instance, marketing departments must carefully manage the release of product launch materials and ensure that their sales channels are correctly using the right images at the right time. Internet search services are available that constantly crawl the web looking for uniquely watermarked content. Reports are then generated notifying the owner of where their content was found, allowing them to take actions deemed necessary.

Once content is found, a wide range of automated actions or messages are available, from the classic "This content is available for licensing." to the more intimidating "This content is copyrighted; please remove it immediately".

**v. Document and image security**

A unique digital watermark can be easily embedded into each copy of a confidential document as they are being created and distributed. The data contained in the watermark can include who are the recipients of each copy so that any information that is inadvertently or intentionally leaked out is easily traced back to the source. Additionally, companies can use network detectors and email filters to check for digital watermarks within documents and images, providing notification if an attempt is made at uploading to the web or forwarding in email outside the company. Similarly, watermark detectors can be included in various printers, scanners and other devices to check for watermarks in confidential documents that someone is attempting to copy.

In this case the watermark can trigger an action, such as a do not copy or scan.

Therefore, document and image security helps to:

- Identify each copy of a confidential document and/or image with a unique digital identity;

- Trace back to the source of leaks if sensitive materials are distributed intentionally or inadvertently;
- Filter documents being uploaded to the web or forwarded in email to quickly identify confidential materials and stop distribution;
- Prevent the copying of confidential documents on copiers and/or scanners;

### 1.3. Objective of the Study

**The main objective of this research project is:**

- To design, implement and improve colored digital image watermarking system using singular value decomposition by proposing new methods of embedding and extracting the watermark.

**The specific objectives of this research project are**:

- To analyze the performance of proposed methods in terms of watermark imperceptibility of the watermarked image and robustness of the extracted watermark using standard attacks.
- It will be input for other study in field.

### 1.4. Methodology:

In this study, invisible digital image watermarking algorithm for colored images will was proposed using singular value decomposition (SVD) in spatial domain. Embedding was done in SVD transfer space.

It consists of watermark embedding, different attacks and watermark extraction algorithms. The performance of proposed methods has been evaluated in terms of imperceptibility and robustness shows robustness.

Different types of attacks were made in MATLAB and measurement has been taken with standard benchmark tool called Stir Mark which shows robustness with respect to some attacks.

The singular value decomposition (SVD) is very powerful and useful matrix decomposition, particularly in the context of data analysis, dimension reducing , image

hiding, image compression, noise reduction and camera calibration for satellite data etc, and is the method of choice for solving most linear least squares problems.

CHAPTER TWO

## 2. Mathematical Preliminaries

### 2.1 Matrices

A matrix is a rectangular (or square) array of numbers, functions, variables or other data such as strings of text arranged in rows and columns. The entries in a matrix are *elements* of the matrix. A matrix is a rectangular array of numbers (usually real) made up of rows and columns. The size of a matrix is its (number of rows) times (number of columns).

A matrix $A$ of size $mxn$ has the form

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} = (a_{ij})_{m\times n}$$

Multiplication of matrices in general involves multiple multiplications of rows and columns. If $A$ is a $mxn$ matrix and $B$ is a $nxp$ matrix, the product $C = AB$ is the matrix where each element $c_{ij}$ is made up of the product of the $i^{t\square}$ row of the left matrix A multiplied to the $j^{t\square}$ column of the right matrix $B$. That is,

$$AB = C = [c_{ij}]_{m\times n}, \qquad w\square ere\ c_{ij} = row_i(A) \cdot col_j(B)$$

Definition of symmetric matrix:

A $mxn$ matrix $A$ is defined as symmetric if $A = A^T$. That is,

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} = (a_{ij})_{\text{nxm}}.$$

$$A^T = (a_{ji})_{nxm}$$

Outer vector product

$$a = A = [a_{ij}]_{m\times 1};\ b^T = B = [b_{ij}]_{1\times n}$$

$$c = a \times b = AB, \text{ an } m \times n \text{ matrix}$$

Inner (dot) product

$$\boldsymbol{a^T \cdot b = \sum_{i=1}^{n} a_i b_i}$$

Orthogonal:

$$a^T \cdot b = \boldsymbol{\sum_{i=1}^{n} a_i b_i = 0 \Rightarrow a \perp b}$$

**Matrix inverse:**

Given a matrix A, its additive inverse is defined to be the matrix –A, where all the elements of A are negated. Note that A + (-A) = 0, where 0 is the zero matrix. We are more interested however with the multiplicative inverse of a matrix, or inverse for short.

The inverse of a $nxn$ matrix $A$, if it exists, is denoted by $A^{-1}$, and is defined to be the $nxn$ matrix where

$$\boldsymbol{AA^{-1} = A^{-1}A = I},$$

where $I$ is the $nxn$ identity matrix. It can be shown that $A^{-1}$, is unique. Note the inverse only exists for square matrices where the row and column number are the same.

Pseudo-inverse $(\boldsymbol{A^{\dagger}})$ for a non square matrix, provided $A^T A$ is not singular

$$\boldsymbol{A^{\dagger} = (A^T A)^{-1} A^T}$$

**Definition 2.1 Let $A$ be an $n \times n$ matrix and let $x$ and $\lambda$** be such that $Ax = \lambda x$ with $x \neq 0$ then $\lambda$ is called an ***eigenvalues*** of $A$ and and $x$ is called an ***eigenvector*** of matrix $A$.

**Theorem 2.1: (**Eigenvalues of symmetric matrices) If $A$ is an $n\times n$ symmetric matrix and $I$ be an $nxn$ identity matrix, then the following properties are true

1) $A$ is diagonalizable (symmetric matrices (except the matrices in the form of $A = \lambda I$, in which case $A$ is already diagonal) are guaranteed to have $n$ linearly independent eigenvectors and thus be diagonalizable)
2) All eigenvalues of $A$ are real numbers
3) If $\lambda$ is an eigenvalues of $A$ with the multiplicity to be $k$, then $\lambda$ has $k$ linearly independent eigenvectors. That is, the eigenspace of $\lambda$ has dimension $k$

**Theorem 2.2:** To finding eigenvalues and eigenvectors of a matrix $A \in M_{n\times n}$. Let $A$ be an $n\times n$ matrix.

(1) An eigenvalue of $A$ is a scalar $\lambda$ such that $\det(\lambda I - A) = 0$
(2) The eigenvectors of $A$ corresponding to $\lambda$ are the nonzero solutions of $(\lambda I - A)\mathbf{x} = \mathbf{0}$

Note: follwing the definition of the eigenvalues problem $A\mathbf{x} = \lambda\mathbf{x} \Rightarrow A\mathbf{x} = \lambda I\mathbf{x} \Rightarrow (\lambda I - A)\mathbf{x} = \mathbf{0}$ (homogeneous system)

$(\lambda I - A)\mathbf{x} = \mathbf{0}$ has nonzero solutions for $\boldsymbol{x}$ iff $\det(\lambda I - A) = 0$

Characteristic equation of $A \in M_{n\times n}$ is given by $\det(\lambda I - A) = 0$

$$\det(\lambda I - A)$$
$$= \left|(\lambda I - A)\right| = \lambda^n + c_{n-1}\lambda^{n-1} + \cdots + c_1\lambda + c_0$$

= polynomial of degree $n$ *in* $\lambda$.

**Diagonalizable matrix**

**Definition 2.2:** A square matrix $A$ is called **diagonalizable** if there exists an invertible matrix $P$ such that $P^{-1}AP$ is a diagonal matrix (i.e., $P$ diagonalizes $A$)

**Proposition 2.2:** A square matrix $A$ is called **diagonalizable** if $A$ is **similar** to a diagonal matrix and similar matrices have the same eigenvalues.

**Proof:**

If $A$ and $B$ are similar $n\times n$ matrices, then they have the same eigenvalues

Consider the characteristic equation of $B$:

$$\begin{aligned}|\lambda I - B| &= |\lambda I - P^{-1}AP| = |P^{-1}\lambda IP - P^{-1}AP| = |P^{-1}(\lambda I - A)P| \\ &= |P^{-1}||\lambda I - A||P| = |P^{-1}||P||\lambda I - A| = |P^{-1}P||\lambda I - A| \\ &= |\lambda I - A|\end{aligned}$$

Since *A* and *B* have the same characteristic equation, they have the same eigenvalues.

**Theorem 2.3** If the matrix $A$ is symmetric and the eigenvalues of $A$ are $\lambda_1, \lambda_2, \ldots, \lambda_n$ with corresponding eigenvectors $x_1, x_2, \ldots, x_n$

i.e. $Ax_i = \lambda_i x_i$ *if* $\lambda_i \neq \lambda_j$ *then* $x_i^T x_j = 0$

**Proof:** Note $x^T{}_j Ax_i = \lambda_i x^T{}_j x_i$

and $x^T{}_i Ax_j = \lambda_j x^T{}_i x_j$

$\left(\lambda_i - \lambda_j\right) x^T{}_i x_j = 0$

hence $x^T{}_i x_j = 0$

**Proposition 2.4** If A is symmetric then $U^T AU$ is also symmetric.

**Proof.** We want to show that $U^T AU$ is symmetric

$$\begin{aligned}(U^T AU)^T &= U^T AU. \\ &= U^T A^T U^{TT} \\ &= U^T AU\end{aligned}$$

## 2.2 Singular Value Decomposition

The singular value decomposition (SVD),is very powerful and useful matrix decomposition, particularly in the context of data analysis, dimension reducing transformations of images; satellite data etc, and is the method of choice for solving most linear least squares problems.

Singular Value Decomposition (SVD) is defined as: Let $A$ is a real mxn matrix and then there exist orthogonal matrices $U$ , $V$ and a diagonal matrix $D$ such that

$$A = UDV^T \qquad (1)$$

where

- $U$ is an $mxm$ orthogonal matrix ( rotation matrix)
- $V$ is an $nxn$ orthogonal matrix( rotation matrix)
- $D$ is an $mxn$ diagonal matrix (stretching matrix)

  $D = (\sigma_1, \dots, \sigma_r)$ are called the singular values.

  $U = (u_1, \dots, u_m)$ are called the left singular vectors.

  $V = (v_1, \dots, v_n)$ are called the right singular vectors.

$$\boldsymbol{A} = \begin{bmatrix} u_{1,1} & .. & u_{1,m} \\ : & \ddots & : \\ u_{m,1} & .. & u_{m,m} \end{bmatrix} \cdot \begin{bmatrix} \sigma_1 & 0 & \cdots & 0 \\ 0 & \sigma_r & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix} \cdot \begin{bmatrix} v_{1,1} & .. & v_{1,n} \\ : & & : \\ v_{n,1} & .. & v_{nn} \end{bmatrix}^T$$

$$D = \begin{pmatrix} \sigma_1 & & 0 \\ & \ddots & \\ 0 & & \sigma_n \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \quad \textit{and} \quad D = \begin{pmatrix} \sigma_1 & & 0 & 0 & \cdots & 0 \\ & \ddots & & \vdots & & \vdots \\ 0 & & \sigma_m & 0 & \cdots & 0 \end{pmatrix} \quad \textit{if} \quad m < n$$

*when* $m > n$

The entries of D are ordered in descending order according to $\sigma_1 \geq \sigma_2 \geq \cdots \sigma_r \geq 0$ , where $r = \min\{m, n\}$

The columns of $U$ are called the left singular vectors, the columns of $V$ the right singular vectors, and the diagonal elements of D the singular values of the matrix $A$.

To establish the decomposition, first multiply Equation (1) from the right by $V$ to obtain

$$AV = DU \qquad (2)$$

The $i^{\text{th}}$ column of equation (2) is given

$$Av_i = \sigma_i u_i \quad for \quad i = 1,2, \dots, n \qquad (3)$$

Note that Equation shows that $u_i$ may be calculated directly from knowledge of $A$, $v_i$ and $\sigma_i$.

We get another relation again by taking the transpose of Equation (3)

$$A^T = VD^TU^T \qquad (4)$$

and then multiply from the right by $U$ to obtain

$$A^TU = VD^T \qquad (5)$$

The $i^{th}$ column of equation (5) is given as

$$A^Tu_i = \sigma_i v_i \quad \text{for } i = 1,2,\dots,n \qquad (6)$$

Note that Equation (6) shows that $v_i$ may be calculated directly from knowledge of A, $u_i$ *and* $\sigma_i$.

**2.2 The associated eigenvalues problems**

There are two eigenvalues problems that can be obtained from the SVD. For the first eigenvalues problem we start with Equation **Error! Reference source not found.** and multiply from the left by $A^T$

$$\begin{aligned} A^TAV = A^TUD &= (UDV^T)^TUD \\ &= VD^TD, \\ &= VD^2 \end{aligned} \qquad (7)$$

$$D^2 = \begin{pmatrix} \sigma_1^2 & & 0 \\ & \ddots & \\ 0 & & \sigma_n^2 \end{pmatrix}$$

Let $R_1 = A^TA$ and $\Lambda_1 = D^2$, then we can write Equation (7) as the eigenvalues problem

$$R_1V = V\Lambda_1 \qquad (8)$$

For the second eigenvalues problem we start with Equation (2) and multiply from the left by $A$

$$\begin{aligned} AA^TU = (UDV^T)VD^T &= UDD^T \\ &= UD^T \end{aligned} \qquad (9)$$

Let $R_{12} = AA^T$ and $\Lambda_2 = DD^T$, then we can write Equation (9) as the eigenvalues problem

$$R_2 V = V\Lambda_2 \qquad (10)$$

Where $\Lambda_2$ is given by

$$\mathbf{\Lambda}_2 = DD^T = \begin{pmatrix} \sigma_1 & & 0 \\ & \ddots & \\ 0 & & \sigma_n \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} \sigma_1 & & 0 & 0 & \cdots & 0 \\ & \ddots & & \vdots & & \vdots \\ 0 & & \sigma_n & 0 & \cdots & 0 \end{pmatrix} \qquad (11)$$

which generates a square $mxm$ matrix with diagonal elements

$$\mathbf{\Lambda}_2 = \begin{pmatrix} \sigma_1^2 & & 0 & 0 & \cdots & 0 \\ & \ddots & & \vdots & & \vdots \\ 0 & & \sigma_n^2 & \vdots & & \vdots \\ 0 & \cdots & \cdots & 0 & \cdots & 0 \\ \vdots & & & & \ddots & \vdots \\ 0 & \cdots & \cdots & & \cdots & 0 \end{pmatrix} \qquad (12)$$

Because the diagonal elements $\Lambda_{kk} = 0$ for $k = n + 1$, the eigenvectors (singular vectors) $u_{n+1}$ ,$u_{n+2}, \dots, u_m$ are of no importance. As a result we define a new $mxn$ matrix $U$ (it is $U$ with the last $m - n$ columns deleted) and a new $nxn$ diagonal matrix $D$ (whose diagonal elements are $\sigma_1, \sigma_2, \dots \sigma_n$) and write the *thin* SVD (or *reduced* SVD) of $A$ as equation (12)

$$A = \widetilde{U}\widetilde{D}V^T \qquad (13)$$

it can be expressed as rank one matrix as,

$$\boldsymbol{A = \sigma_1 u_1 v_1^T + \sigma_2 u_2 v_2^T + \cdots + \sigma_r u_r v_r^T}$$

which very crucial in data compression.

We consider that a host $mxn$ image matrix ***'I'*** and apply SVD on host image to get matrix $U$, $S$ and $V$ and modifying singular value S using watermark image $\boldsymbol{W}$ of size $mxn$ as $S'$. Apply SVD on $S'$ to obtain its corresponding singular values as $S''$

**Properties of the SVD**

There are many properties and attributes of SVD, here we just present parts of the properties that we used in this project.

1) The singular value $\boldsymbol{\sigma_1}$ , $\boldsymbol{\sigma_2}$, … , $\boldsymbol{\sigma_n}$ are unique, however, the matrices U and V are not unique;
2) Since $A^TA = VD_1V^T$ , so $V$ diagonalizes $A^TA$, it follows that the $v_j$ s are the eigenvector of $A^TA$ .
3) Since $AA^T = UD_2U^T$ , so it follows that $U$ diagonalizes $AA^T$ and that the $u_i$ 's are the eigenvectors of $AA^T$ .
4) If A has rank of r then $\boldsymbol{v_1}, \boldsymbol{v_2}, \dots, \boldsymbol{v_r}$ form an orthonormal basis for range space of $A^T$, $R(A^T)$, and $\boldsymbol{u_1}, \boldsymbol{u_2}, \dots, \boldsymbol{u_r}$ form an orthonormal basis for .range space $A, R(A)$.
5) The rank of matrix A is equal to the number of its nonzero singular values.

We consider that a host $mxn$ image matrix '$\boldsymbol{I}$' and apply SVD on host image to get matrix $U$, $S$ and $V$ and modifying singular value S using watermark image $\boldsymbol{W}$ of size $mxn$ as $S'$. Apply SVD on $S'$ to obtain its corresponding singular values as $S''$

CHAPTER THREE

## 3. Colored Image watermarking

### 3.1 Embedding

Consider a *mxn* matrix ***'I'*** representing host image or watermark image**,** to apply singular value decomposition (SVD) a colored image have to be separated into three band monochrome images, where each band corresponds to a different color, typically red, blue and green or RGB each takes values from (0-255) as shown in Fig. 1 and Fig. 2.

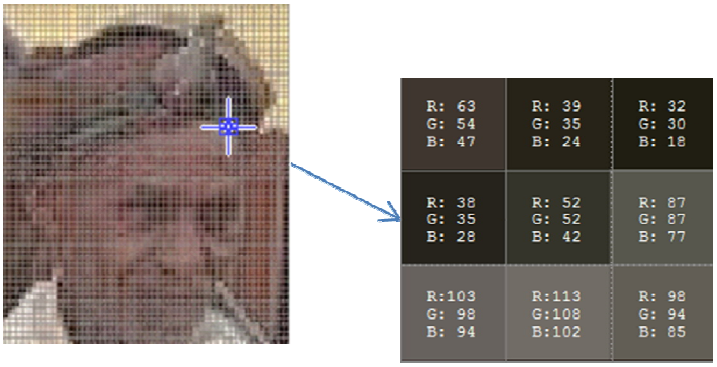



Fig.1. Image pixels at given position

A colored image is vector valued function and mathematically expressed as:

$$I(x,y) \rightarrow \begin{bmatrix} r(x,y) \\ g(x,y) \\ b(x,y) \end{bmatrix}$$ Representing RBG,

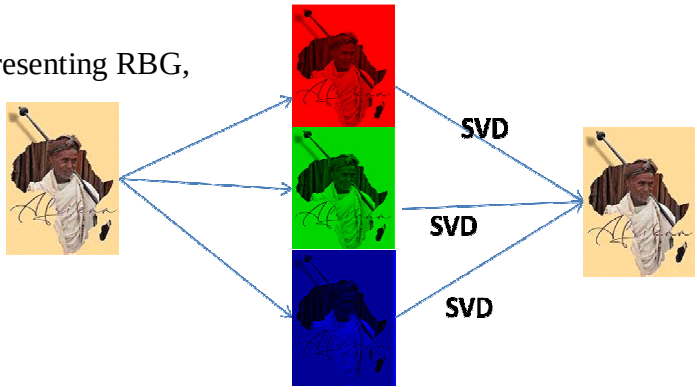



Fig.2 Images show RGB components

Then singular value decomposition applied to three matrices bands and obtained matrices $\boldsymbol{U}, \boldsymbol{D}$ and $\boldsymbol{V}$ for these three matrixes separately and recombined to get: $\boldsymbol{I = U\,D\,V^T}$

Modifying singular value $\boldsymbol{D}$ using watermark image $\boldsymbol{W}$ of size $mxn$

$$W' = D + \alpha W \tag{15}$$

Where:

$D:$ Singular values of original image

$W:$ Watermark image

$\boldsymbol{\alpha}$: Positive real adjusted for watermark strength

Apply SVD on $\boldsymbol{W'}$ *of equation (15)* to obtain its corresponding singular values $\boldsymbol{D'}$ in (16)

$$W' = U'D'V'^T \tag{16}$$

Combining, we obtain a colored watermarked image in equation (17)

$$I^w = U\ D'\ V^T \tag{17}$$

### 3.2 **Extraction process**

In this stage, an attempt is made to regain the watermark or signature from the watermarked image. This stage may need a private key or a shared public key, in combination with the original image, or just the watermarked image

This can be implemented first by applying singular value decomposes to watermarked image $I^w$ ***which is possibly distorted****, and obtain*

$$I^w = U^w D^w V^{wT} \tag{18}$$

Calculate matrix $\boldsymbol{E}$ according to equation (19)

$$E = U'D^wV'^T \tag{19}$$

Get the watermark image extracted from $I^w$ as

$$W^e = \frac{E-D}{\alpha}$$

$$= \frac{U'D^wV'^T-D}{\alpha}$$

The singular values of an image have very good stability, that is, when a same perturbation is added to an image, its Singular values do not change significantly. Each singular value specifies the brightness of an image layer while the corresponding pair of singular vectors specifies the geometry or rotation of the image. The quality of watermarking algorithm will be evaluated through JPEG compression, Rotation, cropping, scaling, Median filtering, Gaussian noise injection, and blurring, sharpening attacks [17].

The performance can be measured by imperceptibility and robust capabilities. Stir Mark (standard benchmark) will be used to test the robustness of the proposed watermarking algorithm. The peak signal to noise ratio (PSNR) between original image $I$ and watermarked image $\boldsymbol{I^w}$and mean square error (MSE) between original watermark $W$ and corresponding extracted watermark $W^e$ will be measured for the quality and robustness capability.

The performance of the watermarking methods can be measured by imperceptibility and robust capabilities. Imperceptibility means that the superficial quality of the original image should not be distorted by the presence of watermark image. On the other hand, the robustness is a measure of the intentionally attacks and unintenally attacks. It was found that the image quality measured by peak signal to noise ratio *(PSNR)* among the watermarked images was larger than 42 db (*B. Kim, J. G. Choi and D. Min 2003, pp.139-149)* [15]. This peak signal to noise ratio is defined as [16]

$$PSNR = 10log10\left(\frac{Max_i}{MSE}\right)^2 \quad (20)$$

Where

$Max_{i:}$ (19) is the largest value of pixel or picture element ranging from 0 - 255.

The PSNR is employed to measure the difference between an original image $I$ and watermarked image $I^w$. For the robust capability, mean absolute error (MSE) measures the difference between an original watermark $W$ and corresponding extracted watermark $W^e$ [16].

$$MSE = \frac{1}{nm}\sum_{i=1}^{m}\sum_{j=1}^{n}(W_{ij} - W_{ij}^e)^2 \quad (21)$$

*Where*

$W_{ij}$*: is watermark image and* $i = 1, 2, \ldots, m;\ j = 1, 2, \ldots, n$

$W_{ij}^e$*: is extracted watermark image and* $i = 1, 2, \ldots, m;\ j = 1, 2, \ldots, n$

Generally, if PSNR value is larger than 40 db the watermarked image is within acceptable degradation levels, i.e. the watermarked are almost invisible to human visual system. A lower mean absolute error reveals that the extracted watermark $W^e$ resembles the $W$ more closely. The strength of digital watermarking method is accessed from the watermarked image $I^w$, which is further degraded by attacks and the digital watermarking performance of proposed method is compared with MSE and If a method has a lower MSE, it is more robust.

### 3.3 Experimental Results

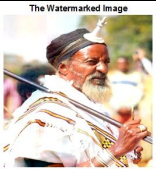
We performed extensive experiments in order to test the imperceptibility and robustness characteristics of the proposed colored image watermarking method. The experimental results are simulated with the software MATLAB R2017b version. All problems and solutions in Matlab are expressed in notation used in linear algebra and essentially involve operations using matrices and vectors. We are using a 256 × 256 pixel **"Lena", "Abba Geda", and "Logo"** colored original host images with JPEG format, and a 256 × 256 pixel colored images which is also in JPEG format for watermark images. These images are shown in Table1.

**Table 1**. The first row contains Host images while second row contains corresponding watermark images.

| **Host Images** | | |
|---|---|---|
|  |  |  |
| 1. Host Lena | 2. Host Abba Geda | 3. Host Logo |
| Watermark Images | | |
|  |  |  |
| 4. Bird | 5. Abba Geda | 6. missile |

We claimed the embedding algorithm and extracting algorithm to identify the ownership of the original colored watermarked image as shown in Tables 2. The watermarked colored image is as pretty good as original host image.

**Table 2.** Shows the Host, watermark, watermarked and extracted watermark at **(α = 0.2)**.

| **Host Images** | **Watermark Images** | **Watermarked images** | **Extracted watermarks** | PSNR (DB) |
|---|---|---|---|---|
|  |  |   |   | **34.856** |
|  |  |   |   | **35.390** |
|  |  |   |   | **37.091** |

For the following simulation alpha **(α = 0.2)** is used and the error ratio of the embedded watermark with attacks is measured by PSNR (DB). Simulation results suggest that this digital color watermarking algorithm is robust against many different common attacks such as cropping; rotation, noise, sharing, blurring and JPEG compression attacks see **Table 3, 4 and 5**. However, cropping is a geometrical manipulation and rotation is a geometrical distortion in practical application but due to singular vectors are rotation matrices the image is unaffected by rotation attack and less affected by cropping and JPEG compression attacks.

Generally, when we see the results of the experiment singular value based algorithm isles affected with geometric attacks and mostly affected with frequencies and noise attacks. If alpha's value is more than 0.2 then quality of original image and watermarked image is not good. So we are using the dumpy value in these techniques.

**Table 3. Extracted watermarks after different attacks (Experiment 1)**

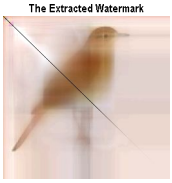
| **Host** | Types of Attacks after watermark | Attacked watermarked image | Extracted watermark | PSNR (DB) values |
|---|---|---|---|---|
| **Lena** | Noise Attacks ('salt & pepper',0.2) |   |   | 29.16 0 |
| | Rotation Attacks (45 counter clockwise) |   |   | 28.860 |
| | Cropping Attacks |   |   | 28.871 |
| | Sharping Attacks High pass filter |   |   | 28.846 |
| | Blurring Attacks Low pass filter |   |   | **29.576** |
| | JPEG compression (Taking 64 eigenvalues) |   |   | 29.252 |

**Table4. Extracted watermarks after different attacks (Experiment 2)**

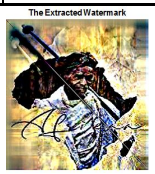
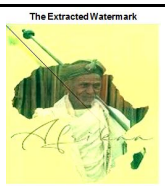
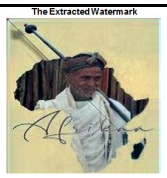
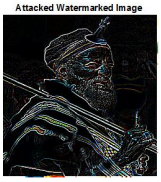
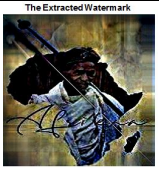
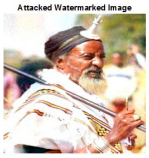
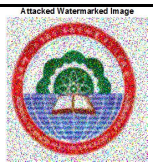
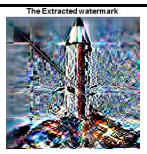
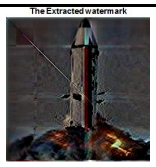
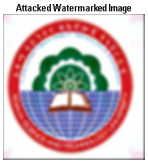
| **Host** | Types of Attacks after watermark | Attacked watermarked image | Extracted watermark | PSNR (DB) values |
|---|---|---|---|---|
| **Abaa Geda** | Noise Attacks ('salt & pepper',0.2) |   |   | **30.510** |
| | Rotation Attacks (45 counter clockwise) |   |   | **48.799** |
| | Cropping Attacks |   |   | **30.004** |
| | Sharping Attacks High pass filter |   |   | **28.990** |
| | Blurring Attacks Low pass filter |   |   | **30.482** |
| | JPEG compression (Taking 64 eigenvalues) |   |   | **30.351** |

**Table 5. Extracted watermarks after different attacks (Experiment 3)**

| Host | Types of Attacks after watermark | Attacked watermarked image | Extracted watermark | PSNR (DB) values |
|---|---|---|---|---|
| Logo | Noise Attacks ('salt & pepper',0.2) |   |   | 29.955 |
| | Rotation Attacks (30 counter clockwise) |   |   | 39.750 |
| | Cropping Attacks |   |   | 30.657 |
| | Sharping Attacks High pass filter |   |   | 28.909 |
| | Blurring Attacks Low pass filter |   |   | 30.376 |
| | JPEG compression (Taking 64 eigenvalues) |   |   | 32.970 |

## 4. Results and Discussion

In the past few years, the problem of protecting multimedia information becomes more and more important and a lot of copyright owners are concerned about protecting any illegal duplication of their data or work. Some serious work needs to be done in order to maintain the availability of multimedia information but, in the meantime, the industry must come up with ways to protect intellectual property of creators, distributors or simple owners of such data. This is an interesting challenge and this is probably why so much attention has been drawn toward the development of digital images protection schemes.

A color image watermarking scheme based on singular value decomposition for copyrights protection was studied in this paper. The main advantages of this method are both the host and embedded images are colored. Experiments show that watermarked colored image is perceptually invisible and also robust against different attacks; especially geometric attacks such as rotation and cropping. Therefore, we conclude that this method is suitable for using color image information to protect data of colored images that will be sent through digital Medias. For future work, metaheuristic algorithm will be used to improve the efficiencies of watermarking. The quality of watermarked and extracted image is the tradeoff values of alpha. If the value of alpha is less than 0.3 then quality of the original image and watermarked image is good and also seen in [17]. The experimental results also show that the proposed methods are effective and robust against geometrical attacks and JPEG compression attack

## 5. Reference


[1]. Podilchuk CI, Delp EJ (2001), Digital Watermarking: Algorithms and Applications. IEEE Signal Process Mag 18: 33-46.

[2]. Santhi V, Thangavelu A (2009), DWT-SVD Combined Full Band Robust Watermarking Technique for Color Images in YUV Color Space. Int J Comput Theor Eng 1: 424-9.

[3]. Lai CC, Tsai CC, (2010), Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition. IEEE Trans Instrum Meas 59: 3060-3.

[4]. Lin PY, Lee JS, Chang CC (2009), Dual Digital Watermarking for Internet Media Based on Hybrid Strategies. IEEE Trans Circuits Syst Video Technol 19: 1169-77.

[5]. Hemdan EED, El-Fishaw N, Attiya G, El-Samii FA (2013) Hybrid Digital Image Watermarking Technique for Data Hiding. IEEE 30th National Radio Sci Conf.

[6]. Ramakrishnan S, Gopalakrishnan T, Balasamy K (2015) SVD Based Robust Digital Watermarking For Still Images Using Wavelet Transform. Comput Sci Inf Technol 155-67.

[7]. Bisla N, Chaudhary P (2013) Comparative Study of DWT and DWT-SVD Image Watermarking Techniques. Int J Adv Res Comput Sci Eng 3: 821-5.

[8]. Malakooti MV, Panah ZF, Hashemi SM (2013) Image Recognition Method based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD).

[9]. Ram B (2013) Digital Image Watermarking Technique Using Discrete Wavelet Transform and Discrete Cosine Transform. Int J Adv Res Technol 2.

[10]. Singh P, Agarwal S (2013) A Hybrid DCT-SVD Based Robust Watermarking Scheme for Copyright Protection. Int Confon Emerging Trends Eng Technol.

[11]. Santhi V, Thangavelu A (2009) DWT-SVD Combined Full Band Robust Watermarking Technique for Color Images in YUV Color Space. Int J Comput Theor Eng 1: 424-9.

[12]. Lai CC (2011), A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. Digital Signal Process 21: 522-7.

[13]. Santhi V, Thangavelu A (2009 DWT-SVD Combined Full Band Robust Watermarking Technique for Color Images in YUV Color Space. Int J Comput Theor Eng 1.

[14]. Kozat SS, Venkatesan R, Mihcak MK (2004) Robust perceptual image hashing via matrix invariants. Int Conf Image Process 5: 3443-6.

[15]. Nan Run Zhou, An Luo, Wei Ping Zou (2018) Secure and robust watermark scheme based on multiple transforms and particle swarm optimization algorithm. Multimedia Tools Appl 1-17.

[16]. Nan Run Zhou, Wei Ming Xia, Ru Hong Wen (2018) imperceptible digital watermarking scheme in multiple transform domains. Multimedia Tools Appl 77: 30251-67.
[17]. Jia Sl (2014) A novel blind color images watermarking based on SVD. Int J Light Electron Opt.
[18]. Kim B, Choi JG, Min D (2003) Robust Digital Watermarking Method Against Geometric Attacks. Real Time Imaging 9: 139-49.
[19]. Manjit Thapa, Sandeep Kumar Sood (2011) On Secure Digital Image Watermarking Techniques. J Inf Secur 2: 169-84

## 6. Appendix

```
function f = svdwatermark
img=imread('gada.jpg');A=imresize(img,[256 256]);

[M N] = size(A);

s = size(A);
%imagesc(A)
R = A(:,:,1); G = A(:,:,2); B = A(:,:,3);
[ur,sr,vr]=svd(double(R));
[ug,sg,vg]=svd(double(G));
[ub,sb,vb]=svd(double(B));
%initialize matrices to zero matrices

%_____________________________________________________________
_____________
Wig=imread('logo.jpg');W=imresize(Wig,[256 256]);

figure(1),imshow(A); title('Host Image')
figure(2),imshow(W); title('The Watermark ')
Rk=zeros(s(1),s(2));
Gk=zeros(s(1),s(2));
Bk=zeros(s(1),s(2));
alfa = 0.2;
Rk = Rk + alfa*double(W(:,:,1))+double(sr);
Gk = Gk + alfa*double(W(:,:,2))+double(sg);
Bk = Bk + alfa*double(W(:,:,3))+double(sb);

Sk = W;
Sk(:,:,1)=Rk; Sk(:,:,2)=Gk; Sk(:,:,3)=Bk;

% now plot the rank-r approximation of image
%-----------------------------------------------------
%imagesc(A)
[urw,srw,vrw]=svd(double(Rk));
[ugw,sgw,vgw]=svd(double(Gk));
[ubw,sbw,vbw]=svd(double(Bk));
%initialize matrices to zero matrices

%initialize matrices to zero matrices
Rv=zeros(s(1),s(2));
Gv=zeros(s(1),s(2));
Bv=zeros(s(1),s(2));

for i=1:s, Rv = Rv + srw(i,i)*ur(:,i)*(vr(:,i))'; end
for i=1:s, Gv = Gv + sgw(i,i)*ug(:,i)*(vg(:,i))'; end
```

```
for i=1:s, Bv = Bv + sbw(i,i)*ub(:,i)*(vb(:,i))'; end

% Now form the rank-k approximation of A
Sh=Sk;
Sh(:,:,1)=Rv; Sh(:,:,2)=Gv; Sh(:,:,3)=Bv;
figure(3),imshow(Sh); title('The Watermarked Image')
%%%%%%%%----------------------------------------------------
---------------
% different attacks to the watermarked image
%Sh = imnoise(Sh,'salt & pepper',0.2);%adds "salt and
pepper" noise to the
    %image I, where D is the noise density.
%Sh= imrotate(Sh,-90,'bilinear','crop');%rotates image A,
using the interpolation
    %method specified by METHOD.
%Sh = imnoise(Sh,'gaussian');%adds Gaussian white noise of
mean M and
    %variance V to the image I. When unspecified, M and V
default to 0 and
   % 0.01 respectively.
%Sh = imnoise(Sh,'poisson');%generates Poisson noise from
the data instead
    %of adding artificial noise to the data.
% now plot the rank-r approximation of image
hp = [-1 -1 -1; -1 8 -1; -1 -1 -1];%high pass filtre
%Sh = imfilter(Sh,hp);
lpp= ones(5,5);
lp =lpp/25;%low pass filtre
%Sh = imfilter(Sh,lp);
%Cr = imcrop(Sh);
%Sh= imresize(Cr,[256,256]);%cropping and resize the image%
%----------------------------------------------------------
----------
%image compression attack
s=size(Sh)
%imagesc(A)
Rh = Sh(:,:,1); Gh = Sh(:,:,2); Bh = Sh(:,:,3);
[ur,sr,vr]=svd(double(Rh));
[ug,sg,vg]=svd(double(Gh));
[ub,sb,vb]=svd(double(Bh));
%Initializes matrices to zero matrices
Rk=zeros(s(1),s(2));
Gk=zeros(s(1),s(2));
Bk=zeros(s(1),s(2));
r =64; % r is the desired rank
% form the rank sums
for i=1:r, Rk=Rk + sr(i,i)*ur(:,i)*(vr(:,i))'; end
```

```
for i=1:r, Gk=Gk + sg(i,i)*ug(:,i)*(vg(:,i))'; end
for i=1:r, Bk=Bk + sb(i,i)*ub(:,i)*(vb(:,i))'; end
% Now form the rank-k approximation of A
Ak = Sh;
Ak(:,:,1)=Rk; Ak(:,:,2)=Gk; Ak(:,:,3)=Bk;
%%_____________________________________________________________
_____
figure(4),imshow(Ak); title('Attaced Watermarked Image')
%calculate image quality degradation after inserting
watermark
    %%%%%%%%%%%%%%%%%%%%%%%%%%
    mse=mean(squeeze(sum(sum((double(A)-
double(Ak)).^2))/(M*N)));
    PSNR=10*log10(255^2./mse);
    msg=sprintf('\n\n----------------\nWatermark by SVD
PSNR=%fdB\n--------------------\n\n', PSNR);
    disp(msg);


%% Extraction Part % ----------------------------------------
----------------------------------
Sp = Ak;
Rp=Sp(:,:,1); Gp=Sp(:,:,2); Bp=Sp(:,:,3);
[wur,wsr,wvr]=svd(double(Rp));
[wug,wsg,wvg]=svd(double(Gp));
[wub,wsb,wvb]=svd(double(Bp));

Rr=zeros(s(1),s(2));
Gr=zeros(s(1),s(2));
Br=zeros(s(1),s(2));
for i=1:s, Rr = Rr + wsr(i,i)*urw(:,i)*(vrw(:,i))'; end
for i=1:s, Gr = Gr + wsg(i,i)*ugw(:,i)*(vgw(:,i))'; end
for i=1:s, Br = Br + wsb(i,i)*ubw(:,i)*(vbw(:,i))'; end
Sr = Sp;
Sr(:,:,1)=Rr; Sr(:,:,2)=Gr; Sr(:,:,3)=Br;
Rl = (double(Sr(:,:,1))- double(sr))/alfa;
Gl = (double(Sr(:,:,2))- double(sg))/alfa;
Bl = (double(Sr(:,:,3))- double(sr))/alfa;
Sl=Sr;
Sl(:,:,1)=Rl; Sl(:,:,2)=Gl; Sl(:,:,3)=Bl;
figure(8);imshow(Sl);title('The Extracted Image')
%%%%%%%%%%%%%%%%%%%%%%%%%%
    %calculate image quality degradation extracted image
    %%%%%%%%%%%%%%%%%%%%%%%%%%
 WW=imresize(Sl,[256 256]);
 mse=mean(squeeze(sum(sum((double(rgb2gray(W))-
double(rgb2gray(WW))).^2))/(M*N)));
```

```
PSNR=10*log10(255^2./mse);msg=sprintf('\n\n----------------
\nWatermark by SVD PSNR=%fdB\n----------------------\n\n',
PSNR);
```