STEGANOGRAPHY IN IMAGES

Project report submitted in partial fulfillment of the requirement for the degree of Bachelor of Technology

in

Computer Science and Engineering/Information Technology

By

Sanya Sood(131401)

Under the supervision of

Ms.Ramanpreet Kaur

Department of Computer Science & Engineering and Information Technology **Jaypee University of Information Technology Waknaghat, Solan-173234, Himachal Pradesh**

Candidate's Declaration

I hereby declare that the work presented in this report entitled **"Steganography in images."** in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering/Information Technology** submitted in the department of Computer Science & Engineering and Information Technology**,** Jaypee University of Information Technology Waknaghatis an authentic record of my own work carried out over a period from August 2015 to December 2015 under the supervision of **(Ramanpreet)** (Assistant professor GradeII)The matter embodied in the report has not been submitted for the award of any other degree or diploma.

SanyaSood(131401)

This is to certify that the above mentioned made by the candidate is true to the best of my knowledge.

Supervisor name: Mrs. Ramanpreet Kaur

Designation:Assistant Professor(Grade II)

Department : Information and technology

Dated:

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGEMENT

Despite of efforts applied in this project, the accomplishment of athis project is dependant on the support and course of action of many others. As a result we obtain the chance to articulate our thankfulness to the person who are involved in the successful conclusion of this project.

We would also like to show our appreciation to our project guide Ms.Ramanpreet Kaur. Without her able guidance, tremendous support and continuous motivation,this project would not be carried out satisfactory. Her kind behavior and motivation provided us the required courage to complete our project.

We would thank our Director, Dean and Head of department of computer science for their continuous support and guidance. Special thanks to our project panel because it was their regular concern and appreciation that made this project carried out easily and satisfactorily.

ABSTRACT

The spreading of computerized interactive media these days has made copyright security a need. Confirmation and data stowing away have additionally turned out to be critical issues. To accomplish these issues, steganography is utilized.

In the recent years, a few steganography plans have been proposed and in view of DCT, DFT, and DWT changes.

This venture shows a square based advanced picture steganography conspire that is subject to the numerical strategy of solitary esteem decay (SVD). Customary SVD strategy as of now exists for watermark implanting on the picture all in all. In the proposed approach, the first picture is isolated into squares, and afterward the watermark is installed in the particular qualities (SVs) of each piece independently. This division and steganography prepare makes the watermark a great deal more vigorous to the assaults, for example, clamor, pressure, trimming. Watermark identification is executed by separating the watermark from the SVs of the watermarked squares. Tests demonstrate that removing the watermark from one square at any rate is sufficient to guarantee the presence of the watermark..

SUMMARY

The dispersal of digital multi media these days made copyright protection an essential requirement. The most important ones are authentication and information hiding.The only strategy for reaching these goals is steganography technology .Project provides a block based digital image steganography scheme. Customary SVD system as of now exists for watermark inserting on the picture all in all. In the proposed approach, the first picture is partitioned into squares, and after that the watermark is inserted in the particular qualities (SVs) of each piece independently. This division and steganography handle makes the watermark significantly more powerful to the assaults, for example, commotion, pressure, trimming.

1.INTRODUCTION

1.1 Introduction

In this modern era, the communication between one party and another is the essential requirement of ever growing population. Every communicator wants to secure their data in a secret and safe manner so that when it is transferred over a channel no attacker could detect the message. Nowadays , we are making use of numerous routes like internet , telephone, audio etc to communicate data from one place to another but it is not at all secure at a particular level. For making our information safe and secure, we can use two techniques which are steganography and cryptography . Cryptography is the process in which information is coded by using encryption key.This encrypton key is acknowledged by sender and receiver only.

Information can not be predicted by anyone who doesn't know the encryption key. However, when this information is transmitted over a channel , intruder may detect the presence of secret message and the information can be predicted easily. To overcome this big advantage of cryptography, steganography technique is used.Steganography is the study of applying various mechanisms so that message is hidden from attacker. Steghanography secures the data in such a manner that no attacker could predict the existence of message. Steganography is mainly the process of hiding data in any multimedia content and this is known as embedding. This process enhances the confidentiality of communicating data

Types of Steganography

1.Text Steganography : Text steganography is the process of hiding communicating data inside text . Communicating data is secured after every mth letter of text. Methods for securing data :

- Format Based Method;
- Random and Statistical Method;
- Linguistics Method.

2. Image Steganography: Image steganography is process of securing data by image as carrier to secure the data. It makes use of pixel intensities to secure the data.Images are most commonly used as .Number of bits presents in digital representation of an image.

- Data is hidden in pixel intensities of image.
- These days number of image file formats are available and they are used for different specific purposes. For each kind of image file format, different steganographic algorithms are available.

3. *Audio Steganography:* Audio steganography secures the data in audio files such as mp3,mp4 etc. such as WAV, AU and MP3sound files. Techniques are

i) Low Bit Encoding
ii) Phase Coding
iii) Spread Spectrum.

4. Video Steganography: Video steganography is the involvement making data secure in video files. Video , aggregation of pictures together ,is used as a way for securing data. Specifically discrete cosine transform (DCT) is the technique used in this method. It changes the values which is used to secure the data in every picture used in the video and such pictures are unobservable to human eye.It appears as a normal video.
eye.

Steganography is made up of two terms .One of the term is message and the other one is cover image. Message is the information which sender wants to send in a safe manner. Cover image is the base thing in which data is hidden.

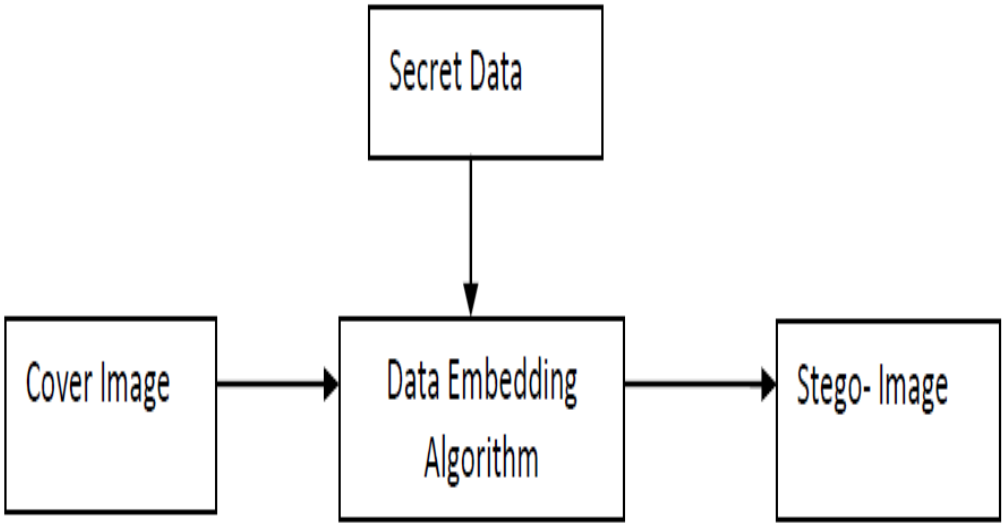
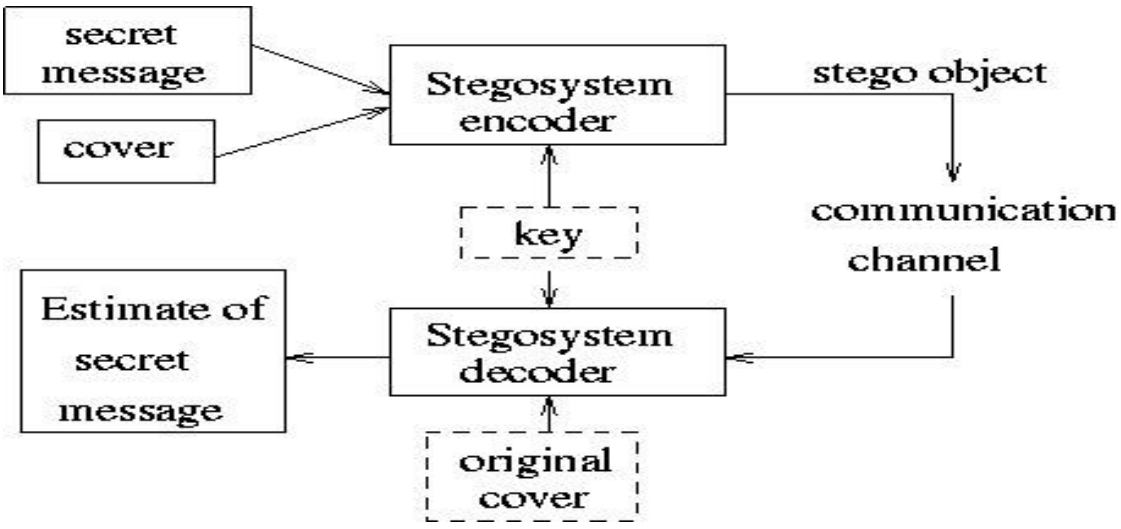


Fig 1 : Steganography Diagram



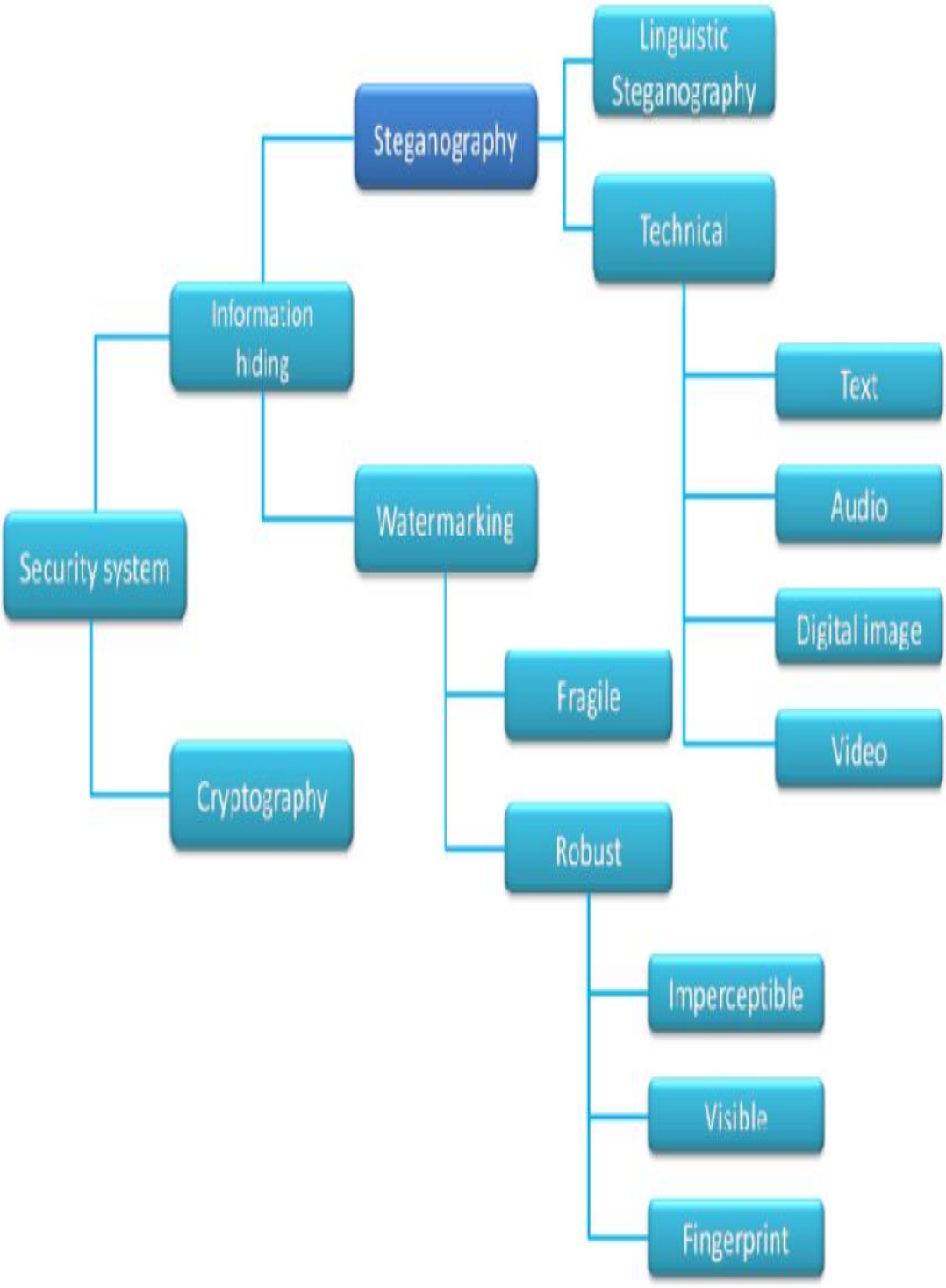
Steganeography application

i) Confidential Communication and Secret Data Storing
ii) Protection of Data Alteration
iii) Access Control System for Digital Content Distribution
iv) E-Commerce
v) Media
vi) Database Systems
vii) digital watermarking.

Watermark is the process of detecting the copyright holder. Steganography is the technique of encoding message in such a way that no attacker could predict it. These days people are using internet as a way of communicating with other people.. In order to provide solution to these issues , we make use of steganography technology

Day by day as people are making use of internet, researchers are studying its significance. If image steganography had not been discovered it would have been a great difficult task for researchers to secure data but now it is comparatively easier to achieve authentication. Each steganography algorithm is made up of embedding algorithm and a detection algorithm.

As the utilization of web is expanding step by step, a few number of issues, for example, duplicating, falsification, extortion, are rising . Any individual having a sound card, scanner joins copyrighted material into introductions, website compositions, and Internet advertising efforts. As a result of this, copyright mishandle is rising step by step. Steganography is being considered for some duplicate counteractive action and copyright security applications. In duplicate aversion, watermark ensures that product and equipment doent not foresee the copyright data.


Linguistic Steganography
Steganography
Technical
Information hiding
Text
Audio
Watermarking
Security system
Digital image
Fragile
Video
Cryptography
Robust
Imperceptible
Visible
Fingerprint

1.2 Overview

Steganography is the process of hiding message in multimedia .It does so in a manner that it is not observable to human eye, but it can be easily detected by a receiver.

Robustness, fidelity tamper resistance are the significant features steganography that it process. Robustness property of steganography is that image does not get distorted when it is transmitted over a channel.When information is encoded into a message it goes through several Fidelity is the property in which message encrypted inside the image can not be detected by any attacker without knowing the encryption key. Tamper resistance is the property in which message does not go through any change while steganographic algorithms are applied to the image and message. These properties of steganography plays a significant role in different applications.

1.3 Objective

Embedding message inside an image without editing the message is the main objective of this project. Although there are various number of steganographic techniques available in this today world, each steganographic technique has its own advantage and disadvantage. In this project,we have used singular value decomposition(SVD) technique. This technique makes use of block based digital image steganography scheme.

In particular esteem disintegration ,the bearer picture is partitioned into pieces and this message is encoded in these blocks.and then the watermark is installed in the solitary qualities (SVs) of each square independently. This division and steganography prepare makes the watermark significantly more powerful to the assaults, for example, commotion, pressure, trimming.

1.4 Scope of the project

Various number of steganographic techniquesare being discovered . Each of them is best suited for solving only a limited scope of specific goals. While visible steganography is widely used, easy to implement, and exhibits excellent results in preventing unauthorized image use, it also significantly degrades the aesthetic value of the original. Invisible steganography is a promising approach for solving a wide variety of problems associated with distribution, copyright management and verification control of digital images.

2. LITERATURE REVIEW

2.1 Issues

The key to develop a successful and an effective solution is possible by having a clear understanding of the underlying problem. Solutions become handy when a complex problem is broken into several simpler tasks.

On the same ground, a system can be developed to implement a solution to a problem. A thorough knowledge of technologies to be used is very essential. Literature Survey is an attempt to discuss such technologies.

Factor Affecting image format

- Invisibility
- Payload capacity
- Robustness against statistical attacks
- Robustness against image manipulation
- Independent of file format Unsuspicious files

FACTORS	BMP	GIF	JPEG
Invisibility	High*	Medium*	High
Payload capacity	High	Medium	Medium
Robustness against statistical attacks	Low	Low	Medium
Robustness against image manipulation	Low	Low	Medium
Independent of file format	Low	Low	Low
Unsuspicious files	Low	Low	High

Types of steganography

Visible Steganography:

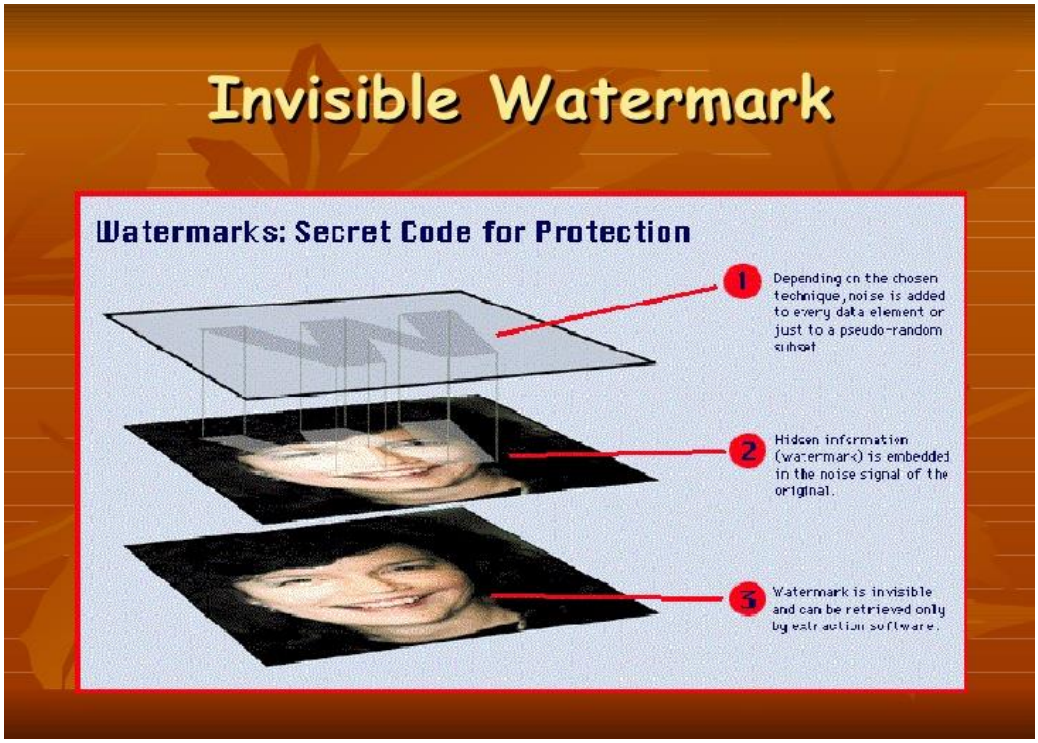
A visible watermark must so be designed in such a way that no attacker could remove the confidentiality of the owner.Most frequently, various type of steganography technology is available these days.Computer programmers could write any program to detect these hidden codes inside the image.Digital forgery is the main issue which is related to this.The most easier way of doing this is by providing a license and the user at any cost has to agree with this license without doing any change to the image .

(a) Watermark at an arbitrary position (29.8720 dB)

(b) Insert 4 watermarks (23.7475 dB)

Invisible Steganography:

Invisible steganography is the technique in which consideration of bits is taken itno account.These are improved in the file through a decoding .



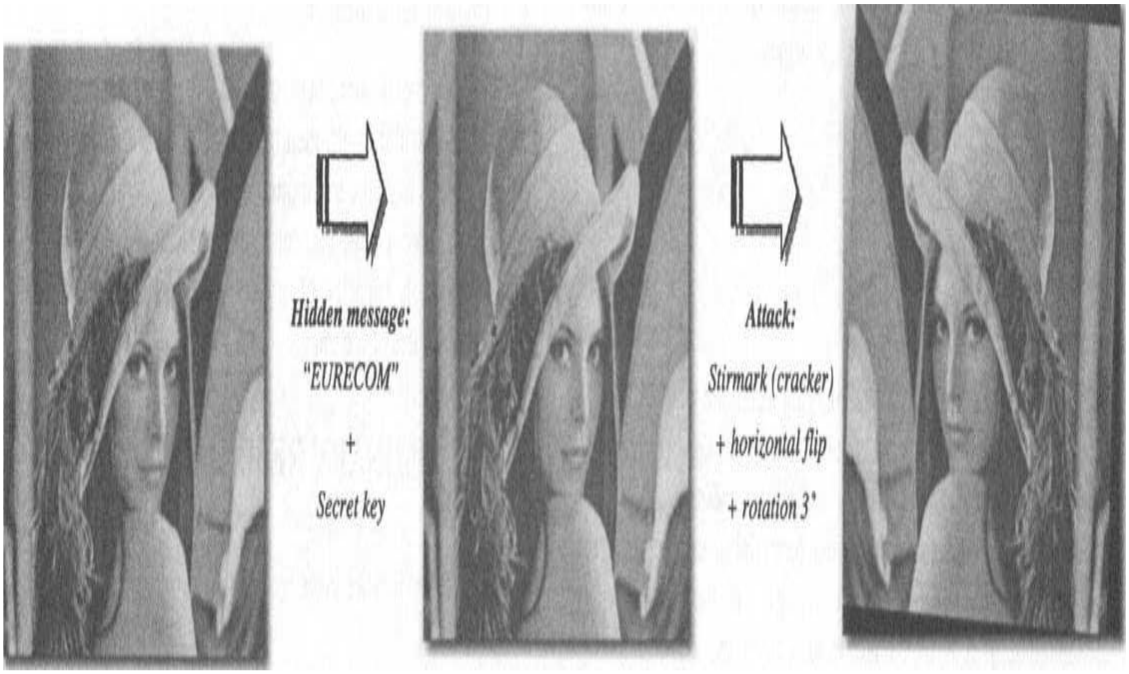
- Protect your valuable images by communicating your copyright
- Track down uses of your images on the Web
- Generate incremental revenue by embedding an ad in every image

EX:

Even if we do this across a big image and with a really large message, it is still hard to tell that anything is wrong.

Original

With Hidden Message



2.2.1 **Purposes of digital steganography**.

- **Ownership Assertion**
- **Fingerprinting**.
- **Authentication and integrity verification**
- **Content labeling**
- **Usage control**
- **Content protection**

2.2.3 Attacks on watermarks

- **Active Attacks** .
- **Passive Attacks**
- **Collusion Attacks**
- **Forgery Attacks**
- **Distortive Attacks**

2.2.4 Singular Value Decomposition (SVD)

Bergman and Davidson discovered a steganography technique that calculates the Singular value decomposition of matrices of the image. This technique then involves
Embedding of the secret message in the left singular vectors .This algorithm overcomes some of steganoalytic attacks which analysie images directly.
Hadhoud and Shallan recommended a similar image steganographic technique which states that embedding the secret message in the left singular vectors of submatrices is the safer step and then not to be touched the diagonal matrix .Advantages of such secheme is less embedding error and better image fidelity . Chung widened this image hiding scheme based on the SVD and vector quantization .Compression ratio and image quality are the main advantages of scheme discovered by chung. Basically this method involves the conversion of message bits into singular values of small blocks of carrier image by less alteration.This ensures the property of robustness of steganography technique.the scheme discovered by chung increased the invisibility and
capacity whilst embed the information into singular vectors of the SVD

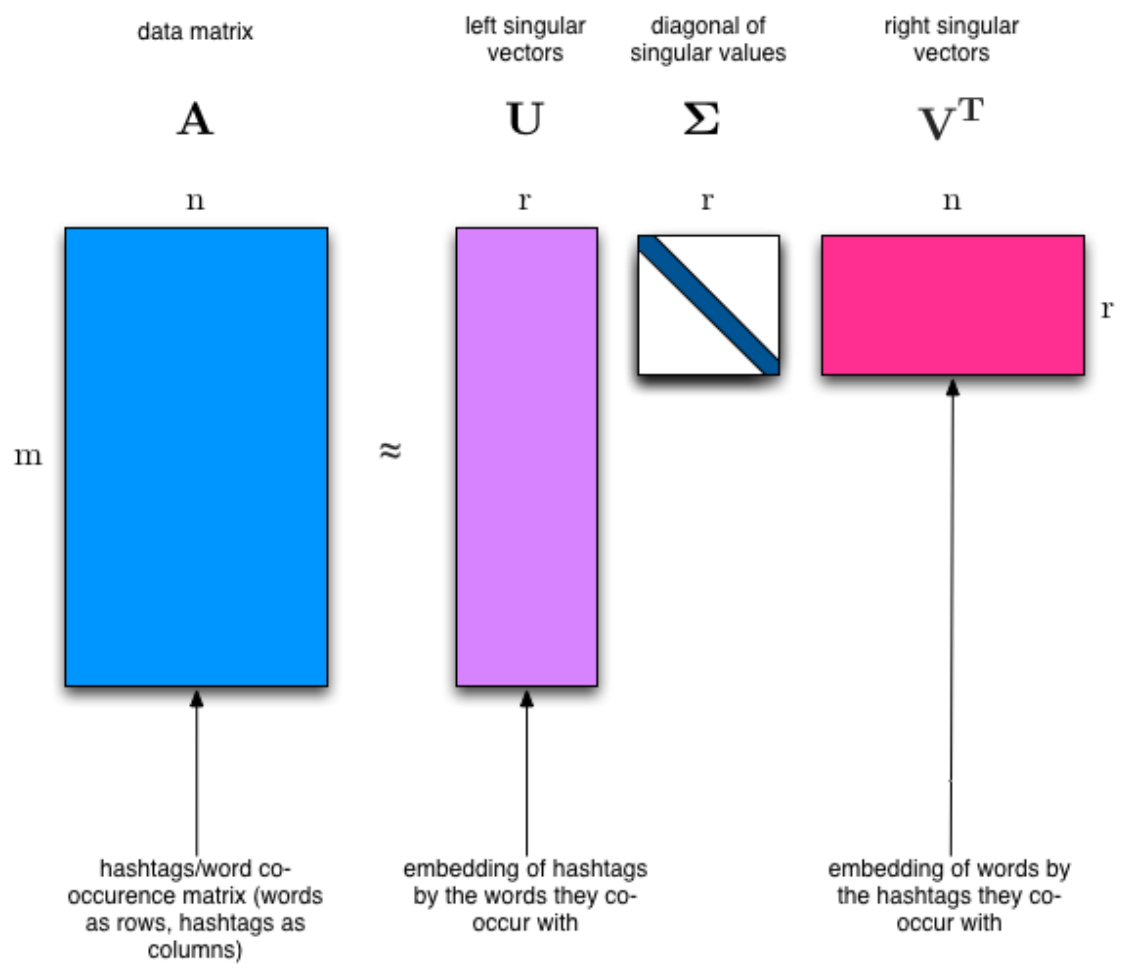
In 1965 G. Golub and W. Kahan introduced Singular Value Decomposition (SVD) as a decomposition technique. General method of finding out singular values of matrices of pixels of images involves conversion of a matrix to a row-echolon form. Rank of a matrix is found out by number of nonzero rows or columns of the echolon form,. The smaller value of this two will tell the rank of matrix.

SVD is a single dimensional algebra method of dividing matrices in its parts these constituent parts are hand matrix which are seggregated by a expressive sloping

surrounding substance The particular principles of a matrix decreases with increasing rank. This reduces the noise and compresses the matrix data by removing the small singular values .

Application of singular value decomposition are in noisy environments which reduces data storage requirements, and pseudo-inverse calculations.

Application areas for the SVD include digital signal processing , image processing, bioinformatics and physical simulation..



3.SVD ALGORITHM

3.1 Introduction to SVD algorithm:

SVD is a linear algebra.

Rank of matrix A whose size is M × M and r ≤ M. The SVD of A is calculated as

A= U S VT

where, U and V are M× M orthogonal matrices, S is an M× M diagonal matrix, and si‘s are singular values satisfying s1 ≥ s2 ≥ · · · ≥ sr = sr+1 = · · · = sN = 0,

3.2 The Proposed Scheme :

. In our scheme, the image is first divided into various blocks and we will be embedding watermark bits into various image blocks then we will do reverse steganography to get the image back. To maintain the robustness of the hidden watermark, each binary value of the P × P binary image will be embedded into three separate blocks in the image. However, the extra information which will be used for recovering is fixed into the last non-zero coefficient in the S matrix of block to make sure the watermarked image can be restored with higher image quality.

3.3 Embedding procedure

To provide robustness of the hidden watermark and maintain the image quality of the watermarked image, each binary value of the watermark is embedded into the second non-zero coefficients of the S matrices in the image. Later, the extra information required for recovering image is embedded into the fourth non-zero coefficients of the S matrices in the image. To make sure the order of non-zero coefficients in each S will not be changed and the hidden watermark can be successfully extracted in the extracting and restoring procedure, different modification principles are designed for various conditions. The proposed embedding algorithm is presented below in detail.

The Embedding Algorithm:

- Input: coordinate (xi, yi),
- Output: a watermarked image

1: Let i = 1.

2: Perform singular value decomposition operation on block Bj which is located in the coordinate (xi, yi) to produce its Uj , Sj, and Vj matrices.

$$\begin{bmatrix} s_1 & 0 & 0 & 0 \\ 0 & \overline{s}_2 & 0 & 0 \\ 0 & 0 & s_3 & 0 \\ 0 & 0 & 0 & \overline{s}_4 \end{bmatrix}_j$$

3: If s1 > s2, then this block is embeddable

4: Let s4 be equal to |s2 − s3| .Otherwise, let s4 be equal to −|s2 − s3|, so that matrix S0j is generated as

$$\begin{bmatrix} s_1 & 0 & 0 & 0 \\ 0 & s_2 & 0 & 0 \\ 0 & 0 & s_3 & 0 \\ 0 & 0 & 0 & \overline{s}_4 \end{bmatrix}_j$$

5: Let s2 be equal to s2 + σ ×Wi so that matrix S0j is changed to

$$\begin{bmatrix} s_1 & 0 & 0 & 0 \\ 0 & \overline{s}_2 & 0 & 0 \\ 0 & 0 & s_3 & 0 \\ 0 & 0 & 0 & \overline{s}_4 \end{bmatrix}$$

6: Perform SVD inverse operation matrices

7: Let i = i + 1. Go to Step 2 until all binary values of watermark have been embedded into t

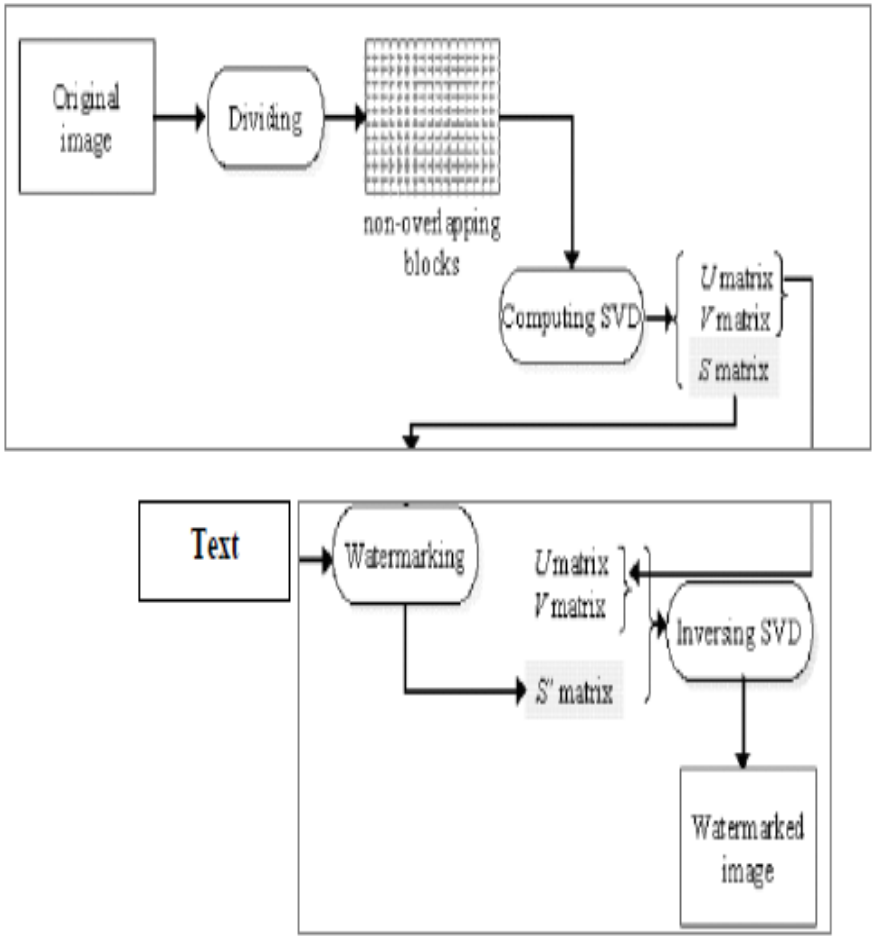
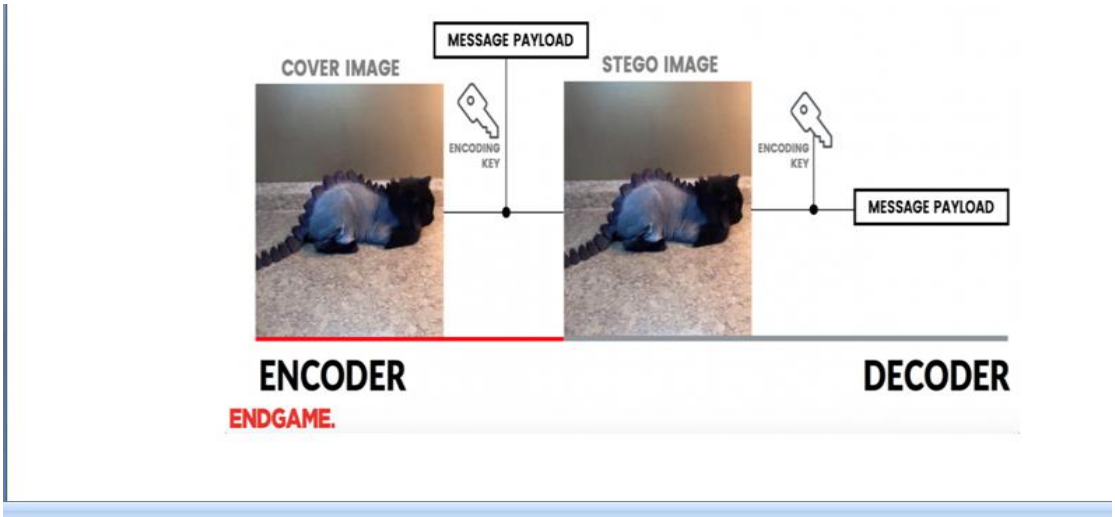


Figure 3.1 Watermark embedding procedure



3.4 Extracting and restoring procedure:

In this , hidden watermark is distracted exactly from the watermark and then the watermarked image is restored with high image quality.After the hidden bits are extracted. As the watermark has to embed 3 times intside the image, the extracted watermark is simply dogged by these 3 extracted watermarks .Consequently, the correction rate of the distracted watermark is produced.

The Extracting Algorithm

I/P: coordinate (xi, yi) and embedded block BW0 j
O/P: the extracted watermark

1: Let i = 1.

2: Perform SVD operation on block BW0 j which is located in coordinate (xi, yi) to generate its corresponding UWj, SWj , and VWj matrices.

$$SW_j = \begin{bmatrix} s_1 & 0 & 0 & 0 \\ 0 & \overline{s}_2 & 0 & 0 \\ 0 & 0 & s_3 & 0 \\ 0 & 0 & 0 & \overline{s}_4 \end{bmatrix}_j$$

3: If s1 ≤ s2 then this block has nothing embedded, i = i+1 and go to Step 2; otherwise, go to Step 4.

4: Extract the hidden watermark by Equation (4).

$$WT_i = \begin{cases} 1, & \text{if} \quad \overline{s}_2 - s_3 > \sigma/2, \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

5: Let i = i+1. Go to Step 2 until P ×P ×3 watermark bits have been extracted.

6: Let i = 1.

7: If WTi + WTi+p×p + WTi+p×p×2 ≥ 2, let W0 i = 1. Otherwise, let W0 i = 0.

8: Let i = i + 1. Go to Step 6 until i = P × P.

3.5 Advantages of SVD algorithm in image steganography

- It provides fidelity against Gaussian noise, cropping and JPEG .It has good stability. Fidelity signifies that the watermark should not be observable to the l.ooker nor downgrading the quality of the content.

- Robustness is also provided. Robustness implies that the watermark should not undergo transformations..

- There is no need for embedding all the singular values of a visual watermark.

Four major goals of SVD algorithm are:

- Reaction is provided to the owner..
- It involves decomposing the problem into its constituent parts.
- SRS serves as the parent document to subsequent documents.
- It serves as a product validation check

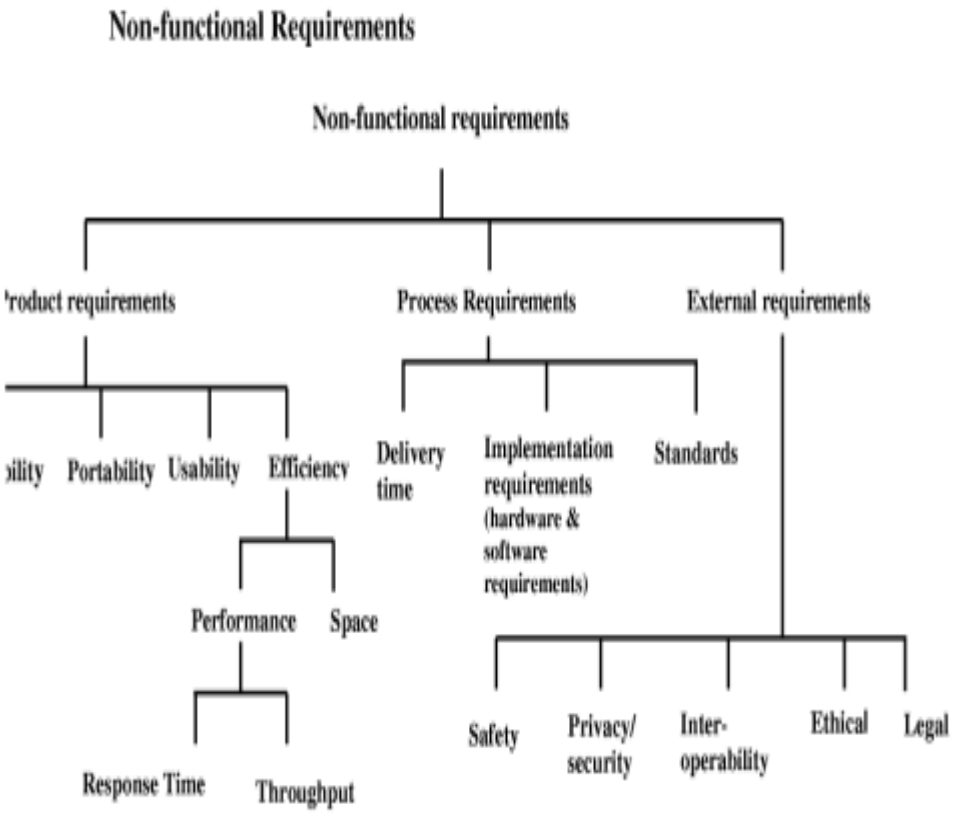


Fig. 2 Non-functional requirements.

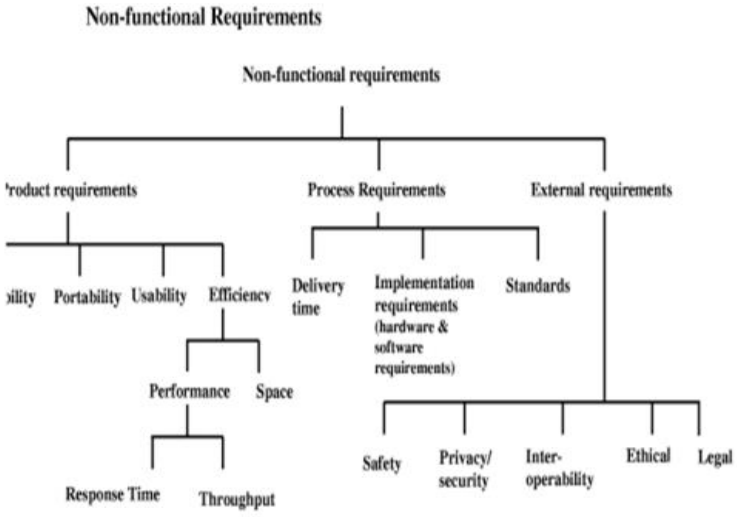


Fig. 2 Non-functional requirements.

4. REQUIREMENT SPECIFICATION

4.1 Functional Requirements

These are statements which system at any cost must provide. It tells that the system will react in response to exacting inputs .Also the system should behave in the expected manner. Functional supplies may also prove what the system is not expected of doing it. Functional supplies explain how organization functions in detail, its inputs and outputs, exceptions, and so on.

Functional Requirements are:

- Embed extra information as invisible watermarks into digital images
- Detect and read watermarks

4.2 Non-Functional Requirements

Non-practical prerequisites are those necessities which is not straightforwardly stressed with the correct capacities to be conveyed by the framework. They may connect to new framework properties, for example, unwavering quality, reaction time and inhabitance. Non-useful prerequisites are less ordinarily connected with individual framework highlights. It indicates framework execution, security, accessibility and other rising properties.

Non-utilitarian prerequisites are not quite recently worried with the product framework to be created. Some non-utilitarian prerequisites may oblige the procedure that ought to be utilized to build up the framework. Non-practical prerequisites emerge through client needs, spending limitations, hierarchical strategies and outer elements, for example, wellbeing directions or security enactmen

The types of non-functional requirements are:

- Organizational requirements
- External requirements

4.3 System Configuration

The configurations needed for implementing the SVD Image Steganography are:

4.3.1 Requirement subsets

- Memory 256 MB RAM, 1GB Secondary Storage
- Pentium III/IV processor
- Monitor Any Color VGA monitor
- Standard Keyboard with 101 keys and Mouse with 2 or 3 buttons

4.3.2 Computer Requirements

- Operating system Vista
- Development Kit: Jdk1.5 or higher version

5. SYSTEM ANALYSIS

Analysis is an iterative process which involves investigation of the application domain, i.e., what are the services that the system should provide in order to meet the users requirements.

5.1 Problem definition

Steganography technique is significant in playing secure game in digital media .It does nothing but only secures data inside image so that attacker could not trace the data

5.2 Purpose

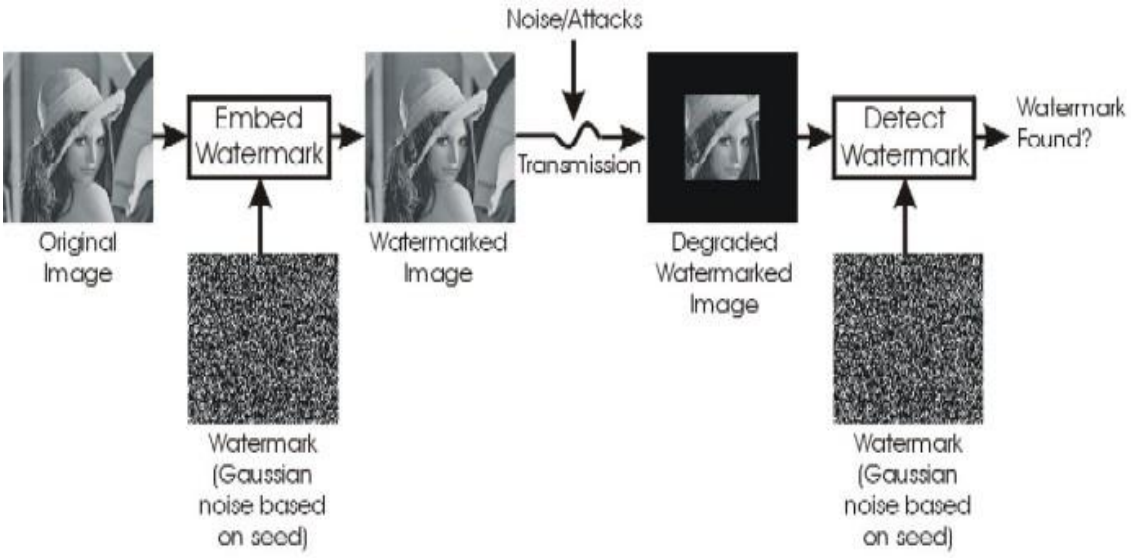
The spreading of computerized mixed media these days has made copyright insurance a need. Confirmation and data stowing away have additionally turned out to be vital issues. To accomplish these issues, SVD based picture steganography innovation is utilized.

5.3 Objective

To implement a well established SVD based image steganography scheme that gives fidelity and robustness such that the matrix of an image has good stability.

5.4 Scope

This project provides a visually undetectable, robust STEGANOGRAPHY scheme.



6. SYSTEM DESIGN

6.1 Problem Definition

Main objective of this project is to design and implement several modules and user interfaces for the proper functioning of the SVD based Image STEGANOGRAPHY. Various modules must be designed to handle Files, to give image and text input to steganography, to retrieve watermark my providing the watermarked image as input to the Reverse steganography, to design User Interface and to Integrate and handle Errors.

6.2 Design Considerations

The following aspects were considered when designing the project

- The front-end representation is to be user-friendly, simple to understand, pleasing, self expressive.
- The users should be provided with reliable, consistent and efficient services

6.3 System Development Strategy

The system is developed based on sustainable development model. This development is based on development of an implementation.

6.4 User Interface Design

The various designs of interface provided to the user to interact with the system are provided below

6.4.1 Steganography Window

Here the user has to provide inputs of the path where the image file and text file are present by browsing through a file dialogue.

The window looks like Figure 5.1 as shown below:

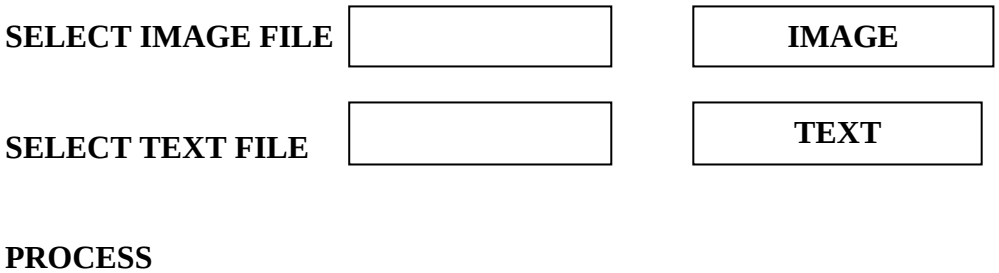
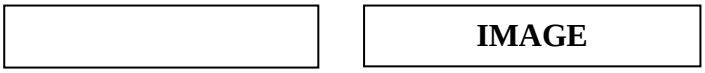


Figure:Steganography

6.4.2 Reverse steganography Window

Here the user has to provide input of the path where the watermarked image file is present by browsing through a file dialogue.
The window is as shown in Figure 5.2,



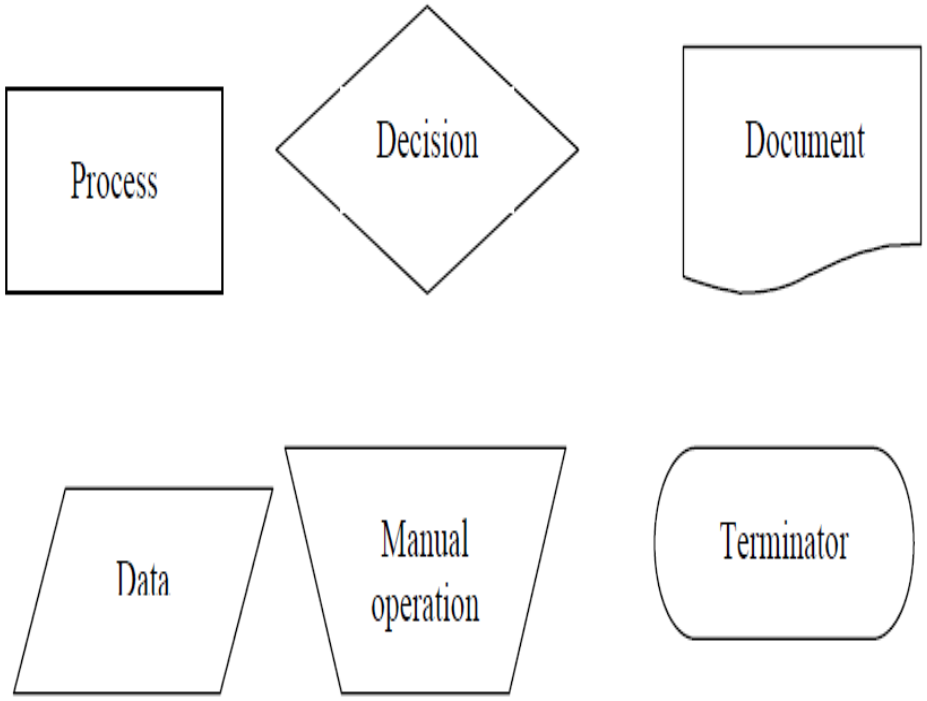
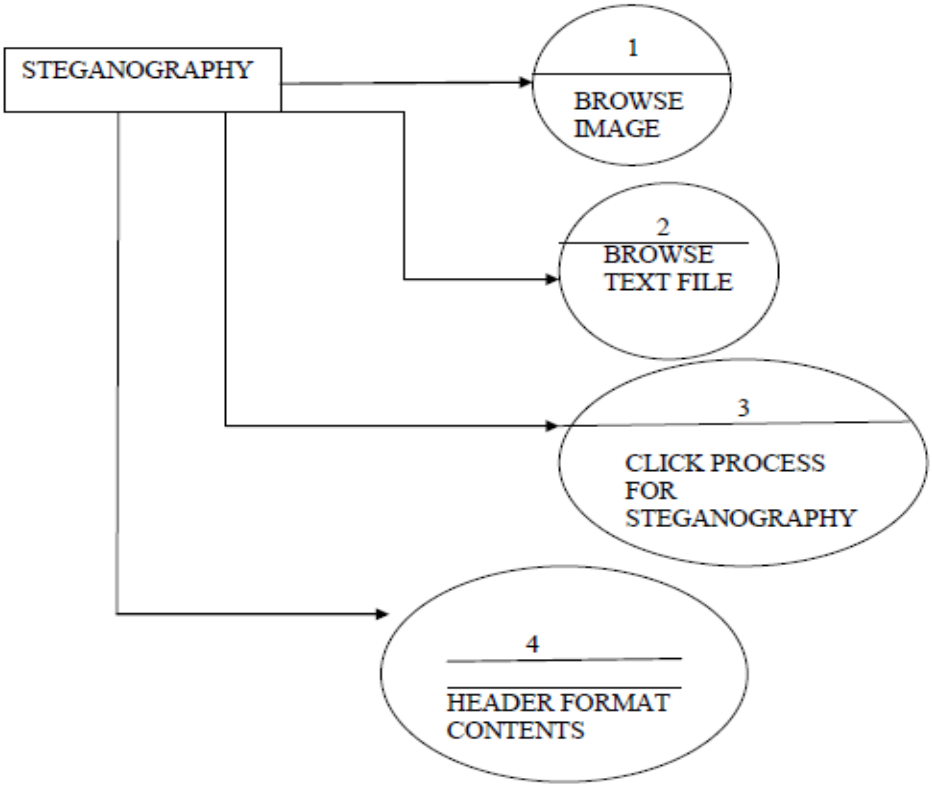
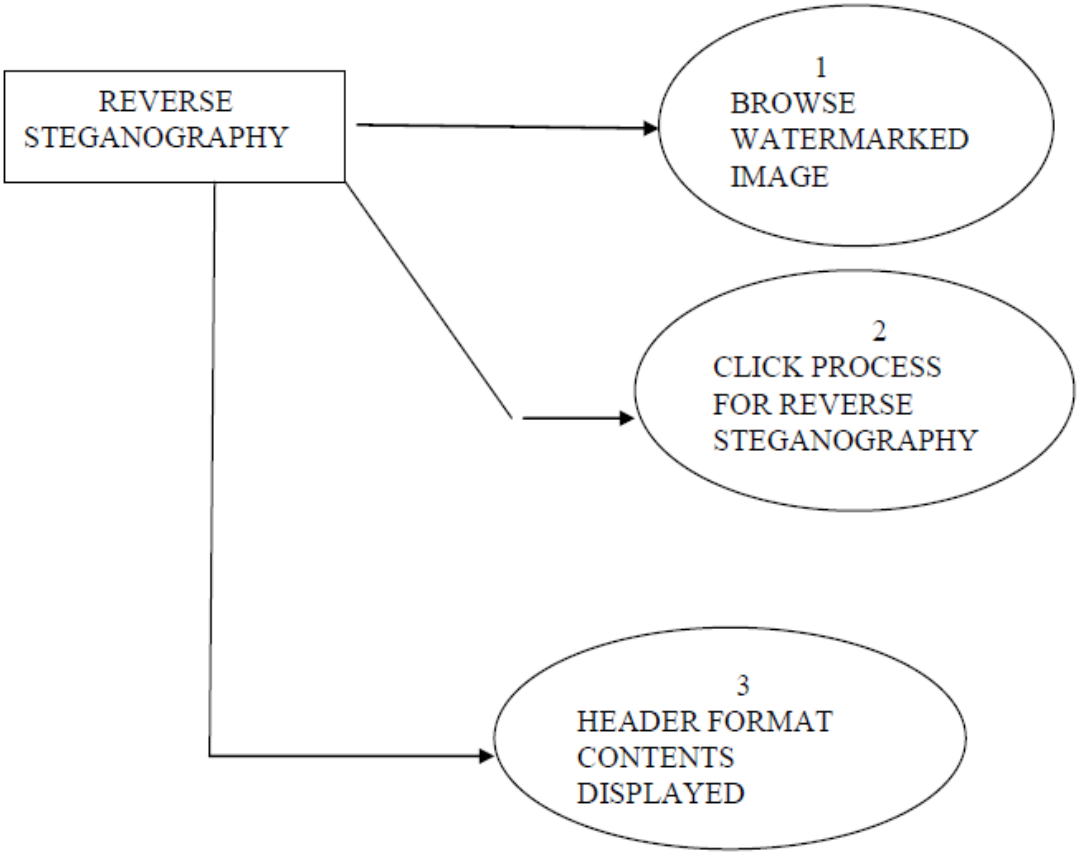


Figure : Components of flow chart


STEGANOGRAPHY
1
BROWSE IMAGE
2
BROWSE TEXT FILE
3
CLICK PROCESS FOR STEGANOGRAPHY
4
HEADER FORMAT CONTENTS



In the reverse steganography process we browse the image file then perform reverse steganography and header content is displayed.

Use Case Diagram:

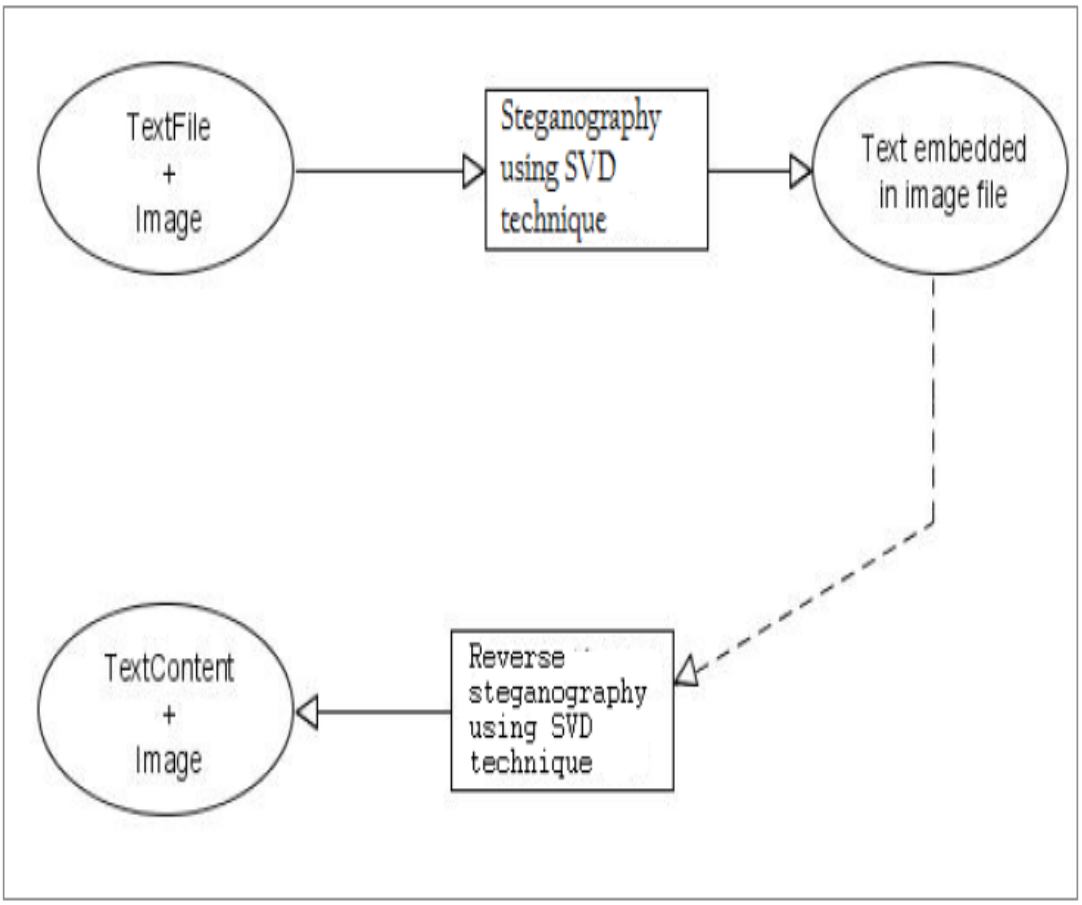


Figure : Steganography and Reverse steganography

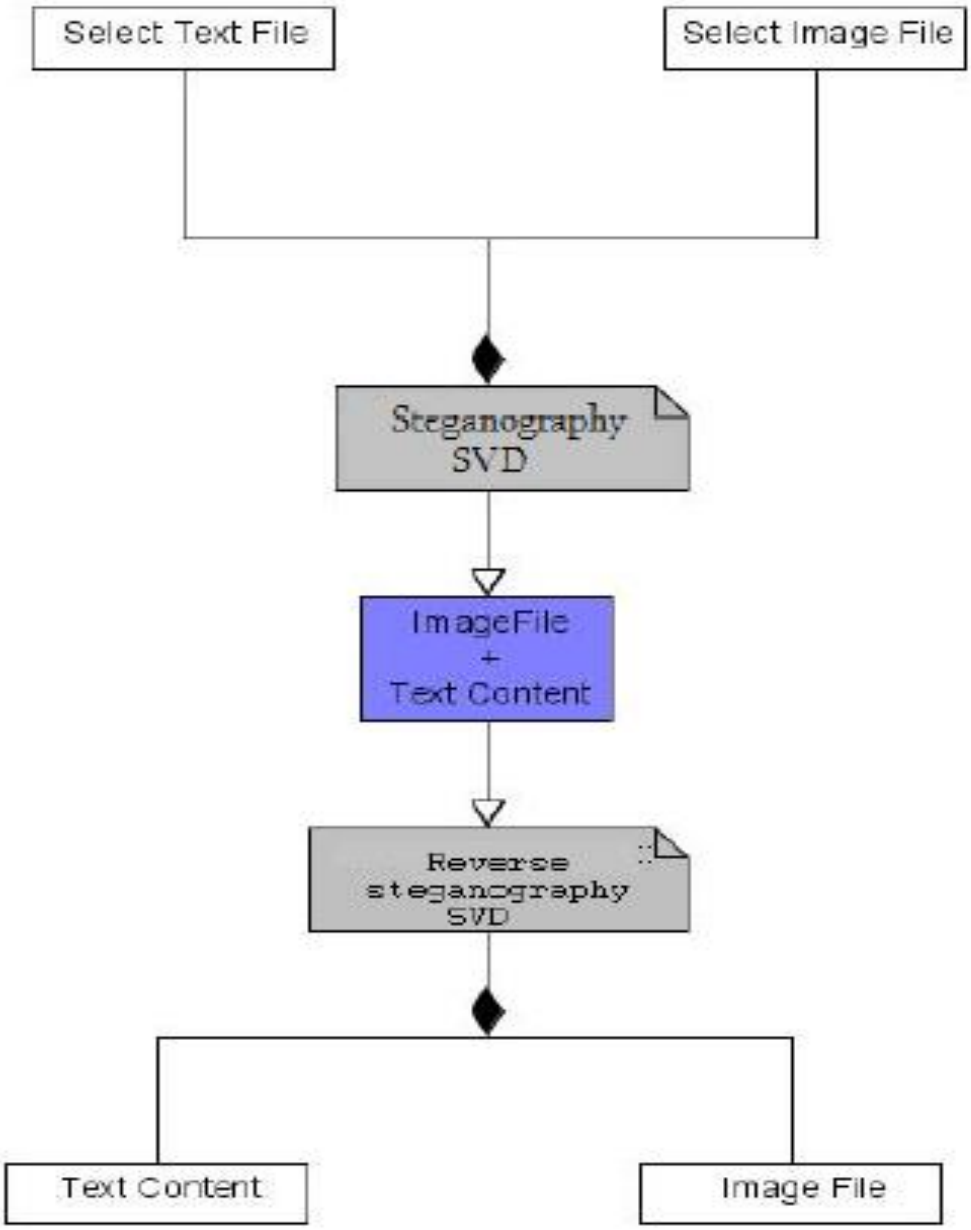


Figure :- Steganography and Reverse Steganography

Activity Diagram:

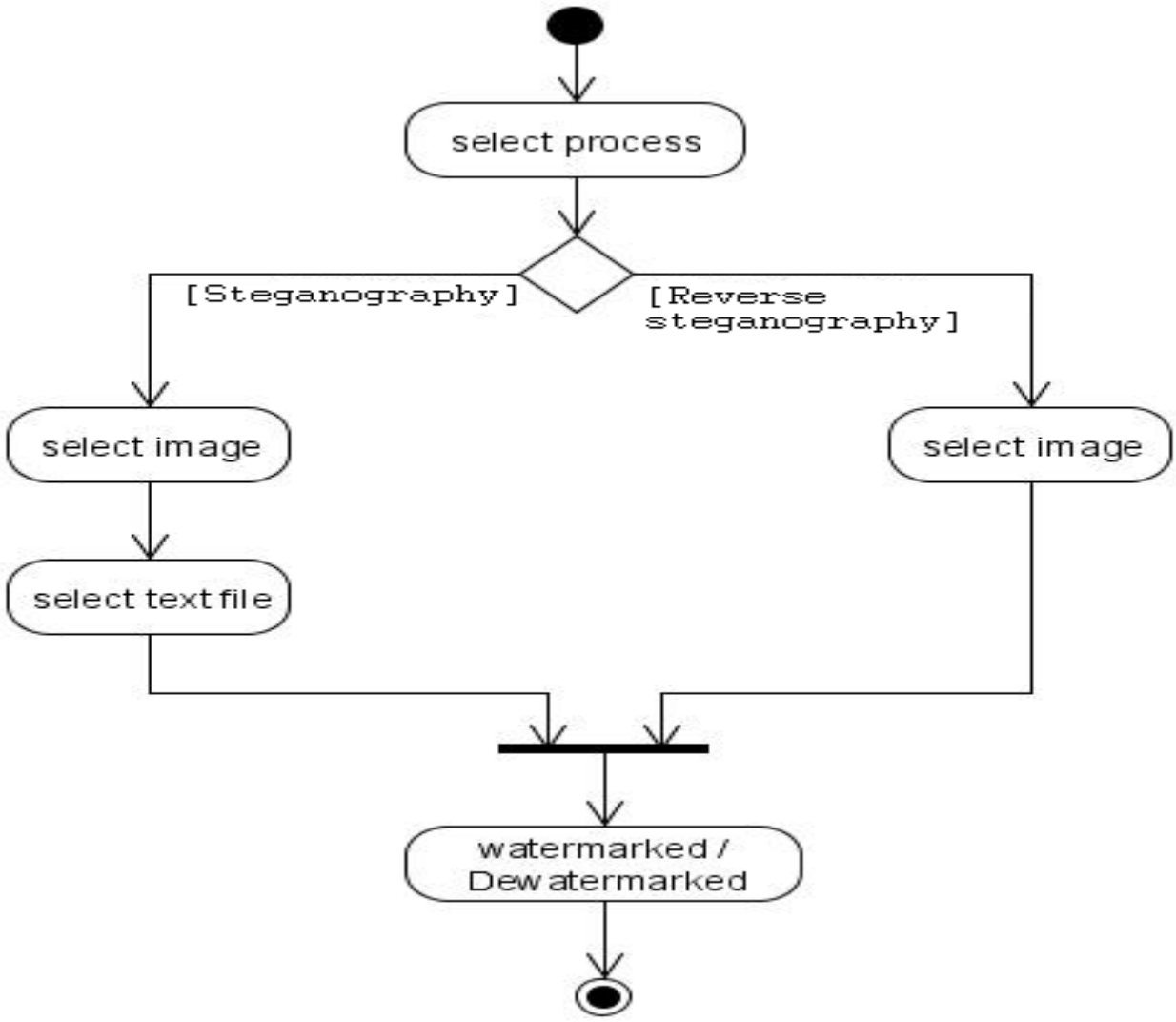


Figure :- Activity Diagram for steganography and Reverse steganography

USE CASE DIAGRAM:

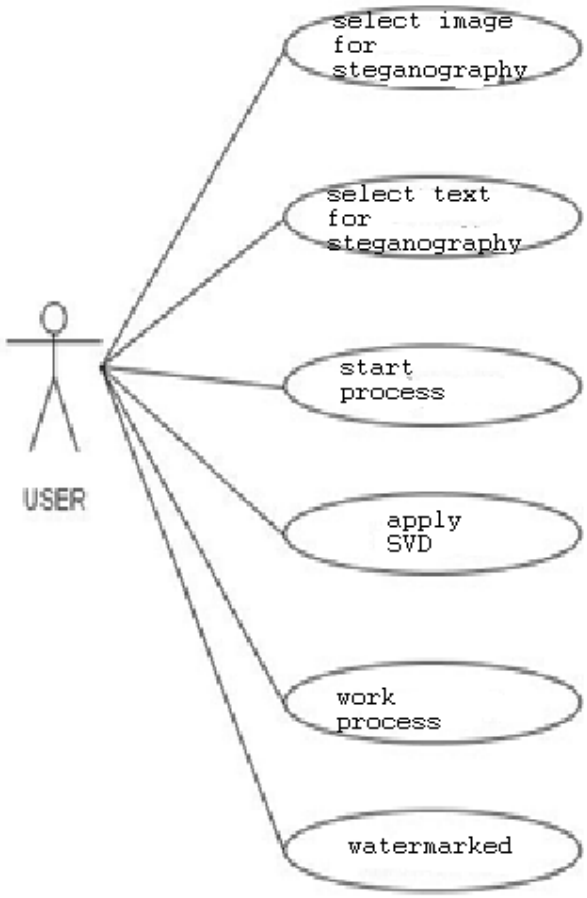


Figure:Steganography and reverse Steganography

7. CONCLUSION

The very purpose of the project is to design and implement several modules and user interfaces for the proper functioning of the SVD based Image STEGANOGRAPHY. Various modules must be designed to handle Files, to give image and text input to steganography, to retrieve watermarkmy providing the watermarked image as input to the Reverse steganography, to design User Interface and to Integrate and handle Errors.

Security of digital images and information is increasing importance these days.

STEGANOGRAPHY:

The text is embedded into the selected image file to give an output image file named _out.bmp‘ at the same location as that of the original image file. The out.bmp file appears to be same as the the original image but in reality it has the text embedded in it.

REVERSE STEGANOGRAPHY:

When out.bmp file is selected and processed a text file _tmp.txt‘ is created which contains the text that was embedded in the image file. This .txt file is created in the workspace.

8. FUTURE PROSPECTS

Steganography is becoming a widely used technique to send data in a secure manner. The project can be further modified for other formats of image files, audio files and video files as the cover for hiding data. Other modifications in the project can be use of DCT, DFT and DWT. Inclusion of the various filetypes and encryption techniques will make the software more resistant to attacks and more reliable and safer

9. BIBLIOGRAPHY

1. Digital Image processing by Rafael C. Gonzalez & Richard E. Woods

2. Research paper of Matthew St. Peter

3. Research of the topic theory through various sites.

4. Research paper by B.chandra Mohan,B.N. chatterjee issued on june 2008 on the topic ―A Robust Digital Image Watermarking Scheme using Singular Value decomposition (SVD), Dither Quantization and Edge Detection‖.

5. Research paper by Eric Tyler Hansen on ―Analysis of the singular value decomposition in data hiding‖,2007

6. Mutlimedia Encryption and watermarking by Borko Surht, Edim Musaremagic, Daniel Socek.

7. http://en.wikipedia.org/wiki/Steganography

8. http://www.jjtc.com/Steganography/

9. http://vision.ece.ucsb.edu/

10.A. A. Al-Ataby, & F. M. Al-Naima. "High Capacity Image Steganography Based on CurveletTransform". In Proc. of the International Conference of the Developments in E-systems Engineering(DeSE), IEEE, 2011, pp. 191-196.

11. H. Abdallah, M. Hadhoud, & A. Shaalan. "An efficient SVD image steganographic approach". Paperpresented at the Computer Engineering & Systems (ICCES), IEEE, 2009. pp. 257-262.

12. S. Mutt & S. Kumar. "Secure image Steganography based on Slantlet transform". In Proc. of theInternational Conference of the Methods and Models in Computer Science (ICM2CS), IEEE, 2009, pp

13. N. F. Johnson and S. Jajodia. "Exploring steganography: Seeing the unseen". Computer, IEEE, vol. 31(2), pp. 26-34, 1998.