INORMATION HIDING TOOL

By

Bhavana U Narikot
(Reg.No:71202621008)
of

KUMARAGURU COLLEGE OF TECHNOLOGY
COIMBATORE

A PROJECT REPORT

Submitted to the

FACULTY OF INFORMATION AND COMMUNICATION ENGINEERING

In partial fulfillment of the requirements
for the award of the degree

of

MASTER OF COMPUTER APPLICATION

JUNE, 2005

Kumaraguru College Of Technology

Coimbatore-641023

Department of Computer Science and Enginnering

Bonafide Certificate

Certified that this project report titled **Information Hiding Tool** is the bonafide work of **Ms. Bhavana U Narikot (Reg No. 71202621008)** who carried out the research under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form part of any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

GUIDE

HEAD OF DEPARTMENT

Submitted for the University Examination held on 24/6/05

Internal Guide

External Guide

24/6/05

dhs

DHS Informatics Pvt. Ltd.

52-53, 3rd Floor, Anam Plaza, 8th 'F' Main, 3rd Block
Jayanagar, Bangalore - 560 011.
✆ : + 91 80 5130 7435 / 2634 7666
Fax : + 91 80 2299 1833

Certificate

This is to certify that Ms.**BHAVANA.U.NARIKOT** (REG.NO: 71202621008), final year student of MCA (Master of Computer Application) of **Kumara Guru College Of Technology,** Coimbatore has successfully completed the project titled "**INFORMATION HIDING TOOL**" in J2EE and ORACLE 9i. This is in partial fulfillment of the requirements for the award of M.C.A Degree. She was working on the project during December 2004 to April 2005. Her overall project performance was excellent.

We wish her success in all her future endeavors.

For DHS Informatics Pvt. Ltd.

DHS INFORMATICS PVT. LTD
Jayanagar
Bangalore-11

S.Palanivel
Manager – Operation

Date: 29-04-2005

Place: Bangalore

ACKNOWLEDGEMENT

I would like to thank our principal **Dr.K.K Padmanabhan** for having given me the opportunity to do this project.

I would like to express my deep sense of gratitude to **Dr.Thangaswami**, HOD, Computer Science for providing moral support towards this project work.

I wish to place on record, my heartfelt gratitude to **Mr A. Muthukumar,** Course Coordinator, Master of Computer Applications, Kumaraguru College of Technology, Coimbatore.

I express my gratitude to **Mr R. Rajasehar**, who has been my guide with valuable and timely suggestions and extended kind of operation and encouragement.

I express my sincere thanks to **Mr.G.SaravanaRajan M.C.A.,** CEO of DHS Informatics Ltd, Bangalore for providing me the opportunity of working in an ideal environment and for encouraging me during the tenure of the project work for giving me permission to do this project in DHS Informatics Pvt. Ltd.

And I would like to thank all those who helped me in this project and whose names are leftover.

ABSTRACT

ABSTRACT

Information Hiding Tool is an application software used to transmit data with a higher level of security among the users within a network. This application is implemented in DHS Infomatics, Bangalore.

Only authorized members can use this application. Each user can enter using his login and corresponding password. On logging on the user will be able to view all the files that he/she has received from the other users in the network. This provides a greater level of security as the files and mails can be accessed only by the people who are within the network and only to people within the network. The application does not allow the files to be sent to any person who does not have a valid login id in the application.

Here, the hiding of information is done into digital objects such as images. The project first gets the data, which can be either a plain message or an encrypted message, and that data is attached to the image in such a way that it does not destroy the view of the image. The color, appearance and other attributes of the image is not damaged or damage may be very negligible in case of the secret message is large in volume.

Then the image file can be transferred or mailed to others. This allows us to hide the data being transmitted from being viewed to the unauthorized people. The data being sent can be either a plain text message or an encrypted text message it is very necessary to provide a good encryption algorithm in order to encode the data.

In our application the text is encrypted using the blow fish algorithm. That is using a 64-bit pin secret key. This pin is used for both encrypting and decrypting. In the algorithm, the encoding is done in patches. The data is broken into clusters and then encoded. The clusters are usually multiples of 2. The algorithm for detaching the message from the image is written to get back the secret information.

LIST OF TABLES

LIST OF FIGURES

TABLE OF CONTENTS

TITLE **PAGE NO.**

INTRODUCTION

ORGANIZATION PROFILE

DHS Informatics Private Limited is a multi-national IT consulting, software development, and outsourcing firm with head offices by name IntersoftKK in Japan and branch offices in the United States, Singapore, and an offshore development center in Bangalore, India. We work globally to deliver locally.

VISION

DHS Informatics mission is to provide top quality software engineering services to help our clients achieve and maintain a competitive advantage. Collaboration is key; our international team of engineers brings together decades of expertise in various systems, deep knowledge of information technology and cutting-edge business know-how. We work side-by-side with you to build a long-term partnership for mutual success. Teamwork, commitment, integrity ad confidentiality are the principles on which we've built our business.

SERVICES

With a focus on finance, including banking, insurance and security, we offer the following services:

- Complete Help Desk outsourcing
- Outsourcing of Engineers
- Software development (onshore & offshore)
- Market Data Consulting
- Business analysis & system design

1.2 PROBLEM DEFINITION

The project is developed to allow users to transmit data in a very secure and safe manner between the users in the network. The major problem is that in case of an organization where data needs to be sent across from one place to another, it is very necessary to transmit the data in a secure manner. The user used to earlier send only plain text this if seen to unauthorized members could lead to a lot of data loss, hence a provision for data encryption is necessary to be provided. Even it may happen that the data may be sent from the organization's network to people outside the network as mails, to overcome this it was necessary to allow the users of the project to only be able to send mails using these applications to people within the network alone.

1.3 SYSTEM JUSTIFICATION

This application was developed in order to provide an effective communication medium between the users of the organization. Every user of the application must have a valid login to log into the application. The user enters the data once he has logged on into the application. It also provides users to encrypt their data and then send the data across to the other users. However data can be sent in both the format either as the plain text or as the encrypted text.In the application, it also allows users to send the processed image within the users of the network. The user can select the message from the list of processed image database. The user can send the image only to people within the network, the name of the other users will appear on the mailing list, there by allowing the user to select the person and mail the processed image. When the user logs on to the application all the new mails that have arrived for the user will appear on the screen.

1.4 SYSTEM AIMS

The aim of the system will be to develop a program for efficiently transmitting data within organization and avoid data loss.

- The system must have details of all the users going to use the system.
- The system must provide data encrypting and decrypting functions.
- The system must provide the user to merge the data into images.
- The user interface should provide the user with a simple navigation through the possible operations it can perform.
- The system must allow users to mail the processed data among valid users.

1.5 ORGANIZATION OF THESIS

Chapter 2 discusses the research and background analysis conducted.
Chapter 3 gives the design of the system.
Chapter 3 explains the implementation of the system.
Chapter 4 discusses the system study.
Chapter 5 discusses the Testing Details.
Chapter 6 deals with the Conclusions and Future Enhancements.

BACKGROUND AND RESEARCH

2.1 DATA HIDING:

Data hiding, embeds data into digital media for the purpose of identification, annotation, and copyright. Several constraints affect this process: the quantity of data to be hidden, the need for invariance of these data under conditions where a "host" signal is subject to distortions, e.g., lossy compression, and the degree to which the data must be immune to interception, modification, or removal by a third party. We explore both traditional and novel techniques for addressing the data-hiding process and evaluate these techniques in light of three applications: copyright protection, tamper-proofing, and augmentation data embedding.

Digital representation of media facilitates access and potentially improves the portability, efficiency, and accuracy of the information presented. Undesirable effects of facile data access include an increased opportunity for violation of copyright and tampering with or modification of content. The motivation for this work includes the provision of protection of intellectual property rights, an indication of content manipulation, and a means of annotation. Data hiding represents a class of processes used to embed data, such as copyright information, into various forms of media such as image, audio, or text with a minimum amount of perceivable degradation to the "host" signal; i.e., the embedded data should be invisible and inaudible to a human observer. Note that data hiding, while similar to compression, is distinct from encryption. Its goal is not to restrict or regulate access to the host signal, but rather to ensure that embedded data remain inviolate and recoverable.

Two important uses of data hiding in digital media are to provide proof of the copyright, and assurance of content integrity. Therefore, the data should stay hidden in a host signal, even if that signal is subjected to manipulation as degrading as filtering, resampling, cropping, or lossy data compression. Other applications of data hiding, such as the inclusion of augmentation data, need not be invariant to detection or removal, since these data are there for the benefit of both the author and the content consumer. Thus, the techniques used for data hiding vary depending on the quantity of data being hidden and the required invariance of those data to manipulation. Since no one method is capable of achieving all these goals, a class of processes is needed to span the range of possible applications.

The technical challenges of data hiding are formidable. Any "holes" to fill with data in a host signal, either statistical or perceptual, are likely targets for removal by lossy signal compression. The key to successful data hiding is the finding of holes that are not suitable for exploitation by compression algorithms. A further challenge is to fill these holes with data in a way that remains invariant to a large class of host signal transformations.

2.2 ORACLE 9I:

Oracle9*i* maximizes the usefulness of traditional business and intranet applications while also providing users with the functionality needed to foster the growth of the emerging hosted applications market on the Internet.

Oracle9*i* builds on historic Oracle strengths to offer the first complete and simple software infrastructure for the Internet's next generation of intelligent, collaborative applications. Oracle9*i* new features expedite delivery of the performance, scalability, and availability that is crucial to providing hosted service software for anyone, anywhere, and anytime.

The Oracle9*i* Database introduces the following advanced and automated design features to stand alone or to work in conjunction with the Oracle9*i* Application Server or the Oracle9*i* Developer Suite to optimize performance for traditional applications and for the emerging hosted applications market.

Systems Management

Integrated system management products in Oracle9*i* create a comprehensive view of all critical components that drive e-business processes. From the client and application server to the database and host, Oracle9*i* quickly and completely assesses the overall health of an e-business infrastructure.

High Availability

Setting a new standard for high availability, Oracle9*i* introduces powerful new functionalities in the areas of disaster recovery, system fault recovery, and planned downtime.

High Security

Oracle9*i* offers the most secure internet platform available to protect company information with multiple layers of security for data, users, and companies. Included are features for building internet-scale applications, for providing security for users, and for keeping separate the data from different hosted user communities.

Tools

Oracle Internet Developer Suite includes the following tools:

- **Oracle Forms Developer**, which enables developers to leverage declarative capabilities and visual editors to automatically generate highly interactive Java clients without having to code in Java.
- **Oracle Designer,** which models business processes, data entities, and relationships. Models are automatically transformed into designs, which automatically generate complete applications and databases.
- **Oracle JDeveloper and Business Components for Java,** which includes a J2EE(tm) development environment with end-to-end support for developing, debugging, and deploying e-business applications.
- **Oracle Reports Developer,** which can build enterprise-level reports rapidly and productively and which is wizard-driven, includes a graphical layout editor, and delivers advanced capabilities to tackle the most challenging reports involving complex queries and programmatic logic.
- **Oracle Discoverer,** which provides users with powerful, on-demand query and reporting capabilities to gain strategic insight into their business and to formulate new ebusiness strategies.

Other Features

All applications are single, middle-tier deployable with Oracle9*i* Application Server

JAVA:

Java technology was created as a computer programming tool. The Java programming language has been thoroughly refined, extended, tested, and proven by an active community of over four million software developers.

Mature, extremely robust, and surprisingly versatile Java technology has become invaluable in allowing developers to:

- Write software on one platform and run it on practically any other platform
- Create programs to run within a web browser and web services
- Develop server-side applications for online forums, stores, polls, HTML forms processing, and more
- Combine Java technology-based applications or services to create highly customized applications or services
- Write powerful and efficient applications for mobile phones, remote processors, low-cost consumer products, and practically any device with a digital heartbeat

In fact, its versatility, efficiency, platform portability, and security have made it the ideal technology for network computing, so that today, Java powers more than 1.75 billion devices:

- over 650 million PCs
- 579 million mobile phones and other handheld devices
- 750 million smart cards
- set-top boxes, printers, web cams, games, car navigation systems, lottery terminals, medical devices, parking payment stations, etc.

SYSTEM DESIGN

3.1: SYSTEM DESIGN APPROACHES.

INPUT DESIGN:

Input Design plays a vital role in the life cycle of software development.It requires a very careful attention of the developers.The Input Design is to feed data to the application as accurate as possible.The Input Design is responsible for all interactions between the user and applications.The Application can work only based on the input given by the users.Hence it is very necessary to obtain the right sort of input from the user.So inputs are supposed to be designed effectively ,so that the errors occurring while feeding data can be minimized.According to the software engineering concepts the input forms or screens are designed to provide to have a validation control over the input limit, range and other related validations. Input design does not only include the design of the form but alos the design of the various components that make the form,such as the text boxes, drop down list boxes and the radio buttons.

This system has input screens in almost all the modules.All the inputs are taken in the forms and are processed.The screens in the application have been developed using JSP in java. Error messages have been developed whenever he comes a mistake and helps in guiding him the right way. All error messages are very descriptive and uses the exact reason as to why the error has occurred. For eg: When the user wants to register himself to the application he or she has to fill a form with a lot of details. In case the user misses a field, in the form, the appropriate error will be created as to which field has been left empty. All the forms have a similar uniform look through out the application. The input design has been made very user friendly and simple for easy compatibility with the user.

Some of the Components used are:

Label:

Label is used to display the information that the user cannot change.

Textbox:

It is used to assign a value to a text box, or read a value that a user has entered into it. Multiline property is assigned the value multiline,and a text area is displayed.

Button Control :

It renders as the same as the form submit button as rendered by the normal HTML tag.

Image button:

Is used to display an image.

Hyperlink:

It can display either a text for an image as a link.

List Box Control:

It enables user to select only one option at a time or to create a muliti select list box.

Radio Button List:

It represents a family of mutually exclusive options. Each Radio Button can be either checked or unchecked. Not more than one radio button of a group can be selected.

OUTPUT DESIGN:

Output Design is the most important and direct source of information to the user that has to be more efficient. Remaining part of the system analysis is based on this output design only. The output design was made with four objectives in mind.

- Output is designed to serve for intended purposes.
- Output is designed to fit the users requirement.
- The appropriate quality of output is delivered.
- Output is to be generated as and when required in the system.

The following are the output design to meet the requirement. The output is the only one method by which the user receives the information. So the output comprises of all the necessary information the user needs. We can judge is if the user requirements are met only based upon the output given by the system. The output must be designed on the basis of what the user expects from the system. All testing and validations can be done only based on the requirements and the output generated by the system.

3.2 REGUIREMENT DEFINITION:

This specifies the requirement in order for the application to work in an efficient manner.

3.2.1 Hardware Specification:

CPU	:	Pentium IV Processor
Hard Disk	:	80 GB
RAM	:	64 MB
Keyboard	:	108 Keys
Mouse	:	Logitech Scrolling Mouse
Monitor	:	Samsung CRT Screen
Floppy Disk	:	1.44 MB

3.2.2 Software Specification:

Front End	:	Java 2.0 , JSP
Back End	:	Oracle 9i
Platform	:	Microsoft Windows 2000

3.3 SUB-SYSTEMS IDENTIFICATION:

- **USER REGISTERATION MODULE**
- **MESSAGE ENTRY MODULE**
- **ENCRYPTION AND DECRYPTION MODULE.**
- **IMAGE SELECTION MODULE**
- **MESSAGE AND IMAGE MERGING.**
- **SENDING AND RECEIVING MAILS WITHIN NETWORK.**

3.4 DATABASE DESIGN:

1. TABLE NAME : USER DESC			
FIELD NAME	**varchar2**	**Width**	**Remark**
intucode	Number	8	Primary Key
struid	varchar2	15	Unique, Not Null
strpass	varchar2	10	Not Null
strname	varchar2	40	Not Null
straddr	varchar2	100	
strcity	varchar2	40	
strstate	varchar2	40	
strcountry	varchar2	40	
strpin	varchar2	6	
strphone	varchar2	20	
strmob	varchar2	20	
stremail	varchar2	20	

2. TABLE NAME : PLAINMESSAGE			
FIELD NAME	Type	Width	Remark
intmsgno	Number	6	Primary Key
intucode	Number	6	Foreign Key
mdate	Date	8	Not Null
strsubject	varchar2	200	
blobmsg	varchar2	500	

3. TABLE NAME : ENCRYPTEDMESSAGE

FIELD NAME	Type	Width	Remark
intemsgno	Number	6	Primary Key
intucode	Number	3	Foreign Key
emdate	Date	8	Not Null
stresubject	varchar2	200	
blobemsg	blob	500	

4. TABLE NAME : PICTURES

FIELD NAME	Type	Width	Remark
intpicno	Number	6	Primary Key
strpicpath	varchar2	50	
strpicdesc	varchar2	50	

5. TABLE NAME : PROPICTURE

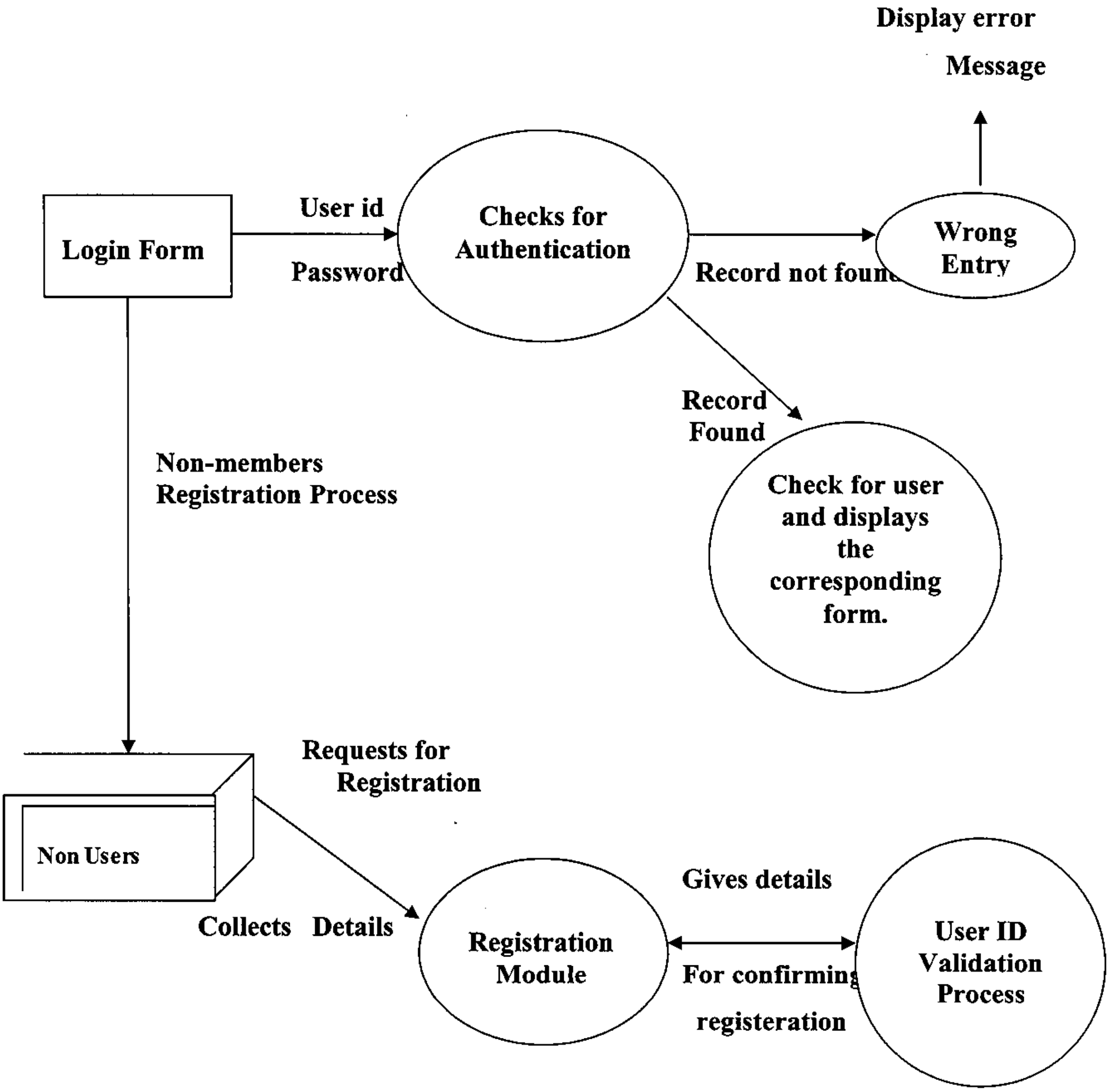
FIELD NAME	Type	Width	Remark
intpropicno	Number	6	Primary Key
intucode	varchar2	6	Foreign Key
strpropath	varchar2	50	
strprodesc	varchar2	50	
strmsgtype	varchar2	1	

6. TABLE NAME : RECEIVED IMAGES

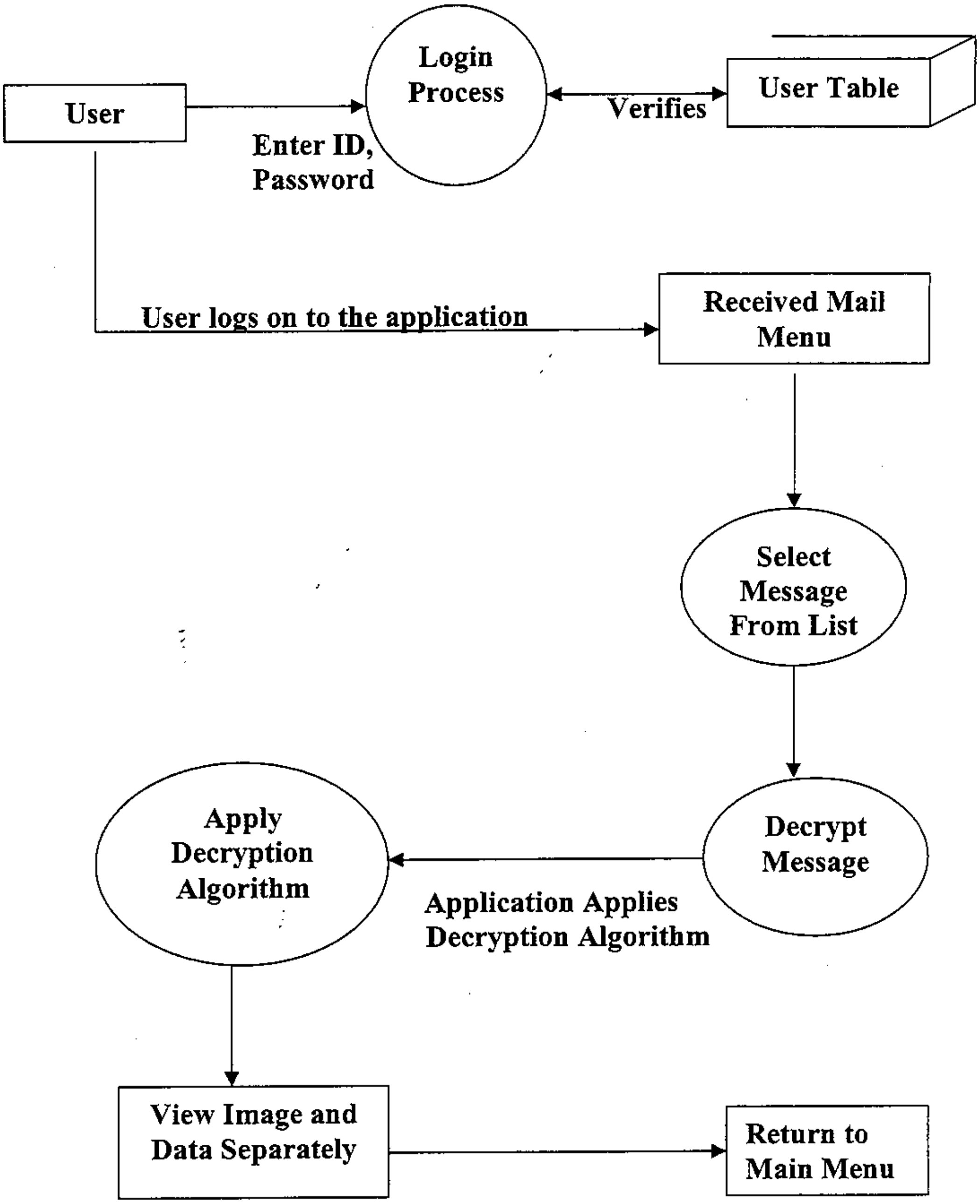
FIELD NAME	Type	Width	Remark
intfrom	Number	6	Foreign Key
into	Number	6	Foreign Key
intpicno	Number	6	
recdate	Date		
strrecdes	varchar2	50	

3.5: DATAFLOW DESIGN:

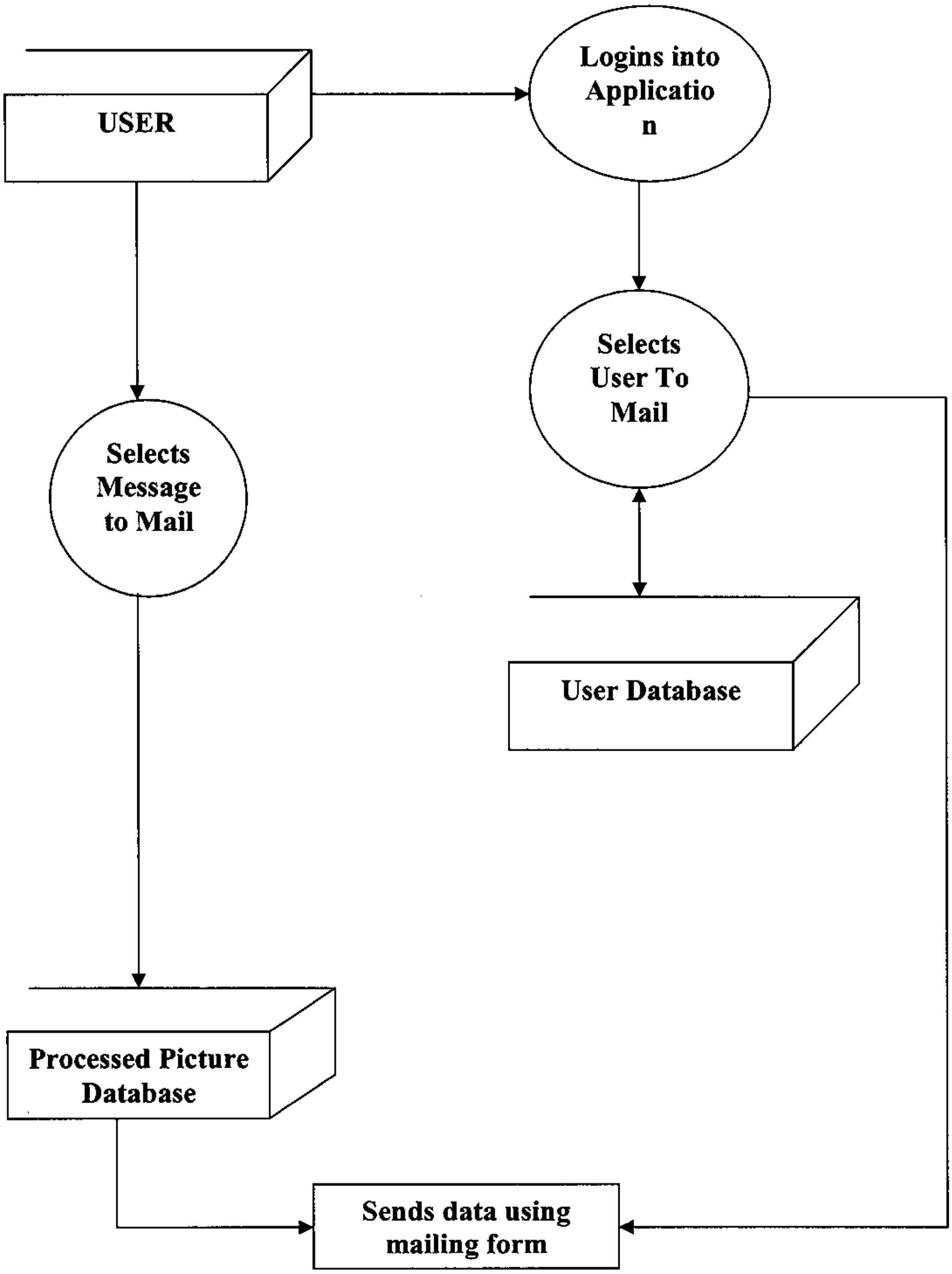
DFD for User Login



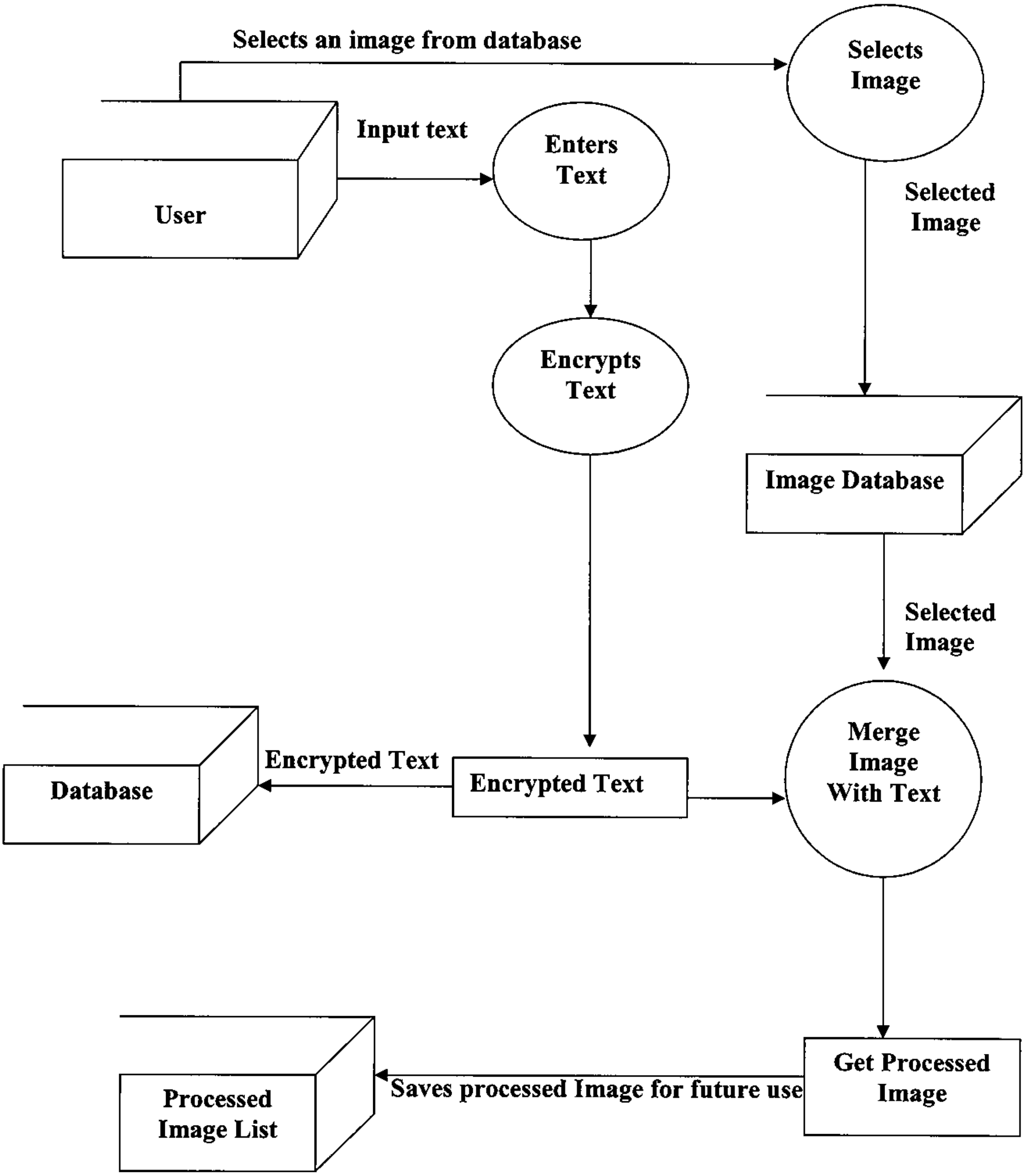
Decrypting Message Received To The User



Data Flow Diagram for Sending Mails Within Users in Network



Data flow Diagram for processing and merging Data to Image



SYSTEM STUDY

4.1 EXISTING SYSTEM:

The existing system was developed as a process in C++. The system does not have any facility to sender receive messages that are being sent. It also does not allow for encryption and decryption of messages. That is the major disadvantage of the existing system is that the user has to manually send data across to the other user. This reduces the security level of the system as the data being sent can be easily misguided to an authorized person, there by reducing the effectiveness of the system. More over the existing system can be used only for merging and transmitting plain text. Hence if an image reaches an unauthorized user, he will easily be able to read it. The existing system also supports only a few file formats such as the .bmp file formats. Hence the system cannot be used with other file formats. This also limits the digital objects that can be used. This system does not provide for much security and other secure features. It is also not user friendly as only single processing software has been developed. The system was not developed as a whole as an application.

LIMITATIONS OF THE EXISTING SYSTEM:

- It is a tedious one.
- It is not user friendly.
- It has limited facilities.
- It provides lower level of security.

4.2 PROPOSED SYSTEM:

The proposed system is a technologically accepted computer based system. The proposed system is designed to remove almost all the problems of the existing system. The proposed system is called the 'Information Hiding Tool'. In this application most of the disadvantages of the existing system are overcome. The application allows users to transmit their data in a much more secure manner through the application. The data is encrypted in this application using the secure blowfish algorithm. The application uses the same key for both encryption and decryption.

The application allows users to transmit both the plain text as well as the encrypted text. The application also allows users to transmit data among themselves there by allowing them to only transmit data to valid users of the network. The user can view the messages that have been received by him, on logging on to the application for the very next time.

The application is very user friendly. This makes it very convenient for the users to use this application. All the various commands given in the application are also written using simple English language.

BENEFITS OF PROPOSED SYSTEM:

- Very user friendly.
- Provides more security and integrity
- Advances application.
- Allows sending and receiving mails across a network.

4.3 INTRODUCTION:

Information Hiding tool allows users to transfer data among the users in a network in a much more secure manner. This application was developed in order to provide an effective communication medium between the users of the organization. Every user of the application must have a valid login to log into the application. The user enters the data once he has logged on into the application. It also provides users to encrypt their data and then send the data across to the other users. However data can be sent in both the format either as the plain text or as the encrypted text. In the case of encryption the blowfish algorithm is used. After the data has been entered the user has to select an image in order to hide the data into the image. The image can be selected from a list of images that are present in the database. Once the data has been got and the image has been selected it is processed. Merging the data into the Least Significant Bits of the image does the processing for hiding data. The processed image is also stored in the database in order to store it for future reference.

In the application, it also allows users to send the processed image within the users of the network. The user can select the message from the list of processed image database. The user can send the image only to people within the network, the name of the other users will appear on the mailing list, there by allowing the user to select the person and mail the processed image. When the user logs on to the application all the new mails that have arrived for the user will appear on the screen. The user can select the mail or message that has arrived and decrypt it. The decryption is done using the same algorithm.

The various modules involved in this application are:

i. User Registration Module.
ii. Data Entry and Encryption Module.
iii. Processing and Data Attachment Module.
iv. Detachment and Decryption Module.
v. Message Sending Module.
vi. View Received Messages and other Processed Images.

1. User Registration:

The user needs to register with the application with a valid user id and password. In case of new users the user can register him by getting all the details such as username, password, name (last name and first name), phone number, address, pin, etc. The user registration process allows users to select a unique username to enter the application. However each user has a unique user code which is numeric and is used to identify the users.

2. Encryption Algorithm:

The algorithm used in application is the blowfish algorithm. Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypts and decrypt messages. Blowfish is also a block cipher, meaning that it divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded. Blowfish requires about 5KB of memory.

2.1 Implementation:

In cryptographic circles, plaintext is the message you're trying to transmit. The process of encryption converts that plaintext message into ciphertext, and decryption converts the ciphertext back into plaintext. In this algorithm, a 64-bit plaintext message is first divided into 32 bits. The "left" 32 bits are XORed with the first element of the key to create a value lets call it P', run through a transformation function called F, then XORed with the "right" 32 bits of the message to produce a new value called F'. F' then replaces the "left" half of the message and P' replaces the "right" half, and recombined to produce the 64-bit ciphertext.

2.2 Advantages:

This encryption algorithm provides for such as data security, data integrity that is it gives the assurance that the recipient received the same message you sent. Blowfish encryption algorithms can also provide authentication, the assurance that a message came from whom it says it came from. This can also assure data privacy, a way to prevent someone other than the intended recipient from reading the message.

3. Data Attachment Process:

In order to attach the data and the image into a single unit, we have to first receive the data from the user. This is the data that has to be sent across by the user. This data can be either sent as a plain text or as an encrypted text. As mentioned in the earlier notes the application uses blowfish algorithm to perform the encryption and the decryption process. After entering the data, the user has to select the image onto which the data is to be merged. This image can be selected from a given list of images.

3.1Methodology:

The data, which is received, is broken into bits and represented in the form of 0's and 1's. A digitized photograph is stored as an array of colored dots, called pixels. Each pixel typically has three numbers associated with it, one each for red, green, and blue intensities, and these values often range from 0-255. Each number is stored as eight bits (zeros and ones), with a one worth 128 in the most significant bit (on the left), then 64, 32, 16, 8, 4, 2, and a one in the least significant bit (on the right) worth just 1. A difference of one or two in the intensities is imperceptible, and, in fact, a digitized picture can still look good if the least significant four bits of intensity are altered -- a change of up to 16 in the color's value. This gives plenty of space to hide a secret message. Text is usually stored with 8 bits per letter, so we could hide 1.5 letters in each pixel of the cover photo. A 640x480 pixel image, the size of a small computer monitor, can hold over 400,000 characters. That's a whole novel hidden in one modest photo.

3.2 Application:

The above methodology is used to bind the data and the image. Once this has been done the user can store the processed image into the database for future reference. The user can later view the processed image or can even delete it from the database. The processed image on viewing does not certify any changes to the human eye. There is no difference in the color, appearance or the structure of the image that was earlier taken from the database and the new image that is formed after binding the data with the image.

4. Detachment Of Data From Image:

The processed image is the merged form of the data and the image. The data can be very easily detached from the Image. The process, which is used to bind the data and the image, can itself be used to detach the data from the image. The Least Significant Bits of the image can easily get the data. The bits contain the data along with the pixel information within themselves. Using these bit information the data can be easily obtained from the image.

5. Decryption Algorithm:

In the earlier part of the report we had mentioned that the blowfish algorithm is used to encrypt and decrypt the data. Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypts and decrypt messages. Hence this provides a very easy way to decrypt the data. The decryption process also uses the same secret key that was used in the encryption process during the earlier part of the application process

6. Sending Messages:

The application also allows users to transfer messages as mails between the users in the network. This application allows a user to send the mail only to valid users within the network. The user first has to log on to the application. The user can then select the message from the list of processed image. The user selects the user's id from the list of users that appear in the user list. The user can be selected by clicking on the name of the user that appears on the list. It is not possible for the user who has logged on to the application to send the message to a person outside the network or who is not a valid user of the network.

7. Received Messages:

When the user first logs onto the application the user can go to the received mails form and view all the messages that he has received along with the details of the person who has sent the mails. In order to read the message the user applies the detachment process to get the data. The decryption process follows the detachment process in order to read the actual data as in case of an encrypted data

FORMS

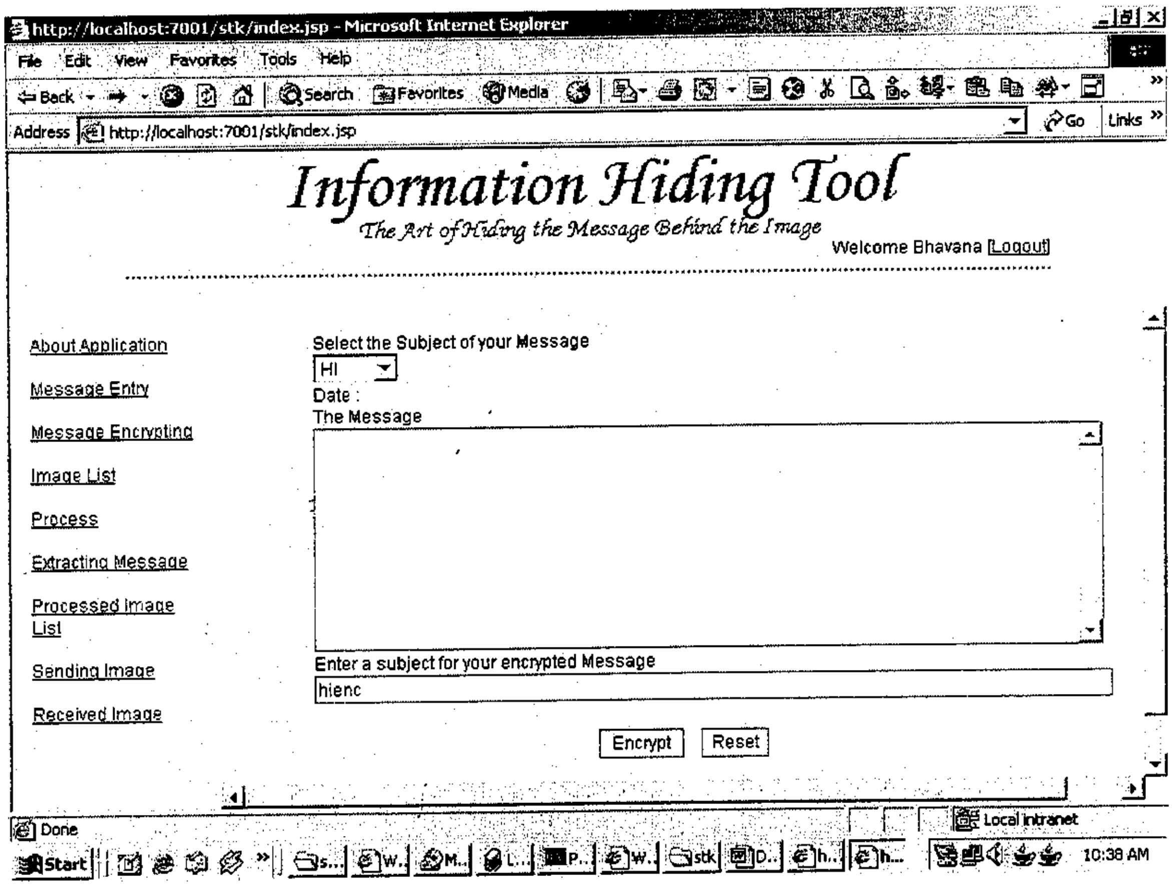
SYSTEM IMPLEMENTATION

5. IMPLEMENTATION:

Implementation is the stage where the theoretical design is to be converted into a working system. The implementation phase also helps the user in testing the application that has been developed, the error identification, making changes if any as per the requirements of the user, training the user, appraising the user of the various special facilities and features.

As and when the system has been installed, the supervisor was asked to inspect the system. The output or report that was generated was shown to the manager. They also were asked to give sample data and asked to scrutinize the operations being carried out by the application. It is in this phase that the higher official gave the recommended changes and modifications to be made to the system. It is also to note if the system works as per the specification and notification.

The implementation phase of software developed is concerned with translating design specification into source code. The primary goal of implementation is to write source code as per the necessary use requirements. The client wanted a user friendly operation. So the software is implemented using GUI. The system is developed in the more interactive way.


http://localhost:7001/stk/index.jsp - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost:7001/stk/index.jsp
Go Links
Done
Local intranet
Start
10:38 AM

Information Hiding Tool

The Art of Hiding the Message Behind the Image

Welcome Bhavana [Logout]

About Application

Message Entry

Message Encrypting

Image List

Process

Extracting Message

Processed Image List

Sending Image

Received Image

Select the Subject of your Message

HI

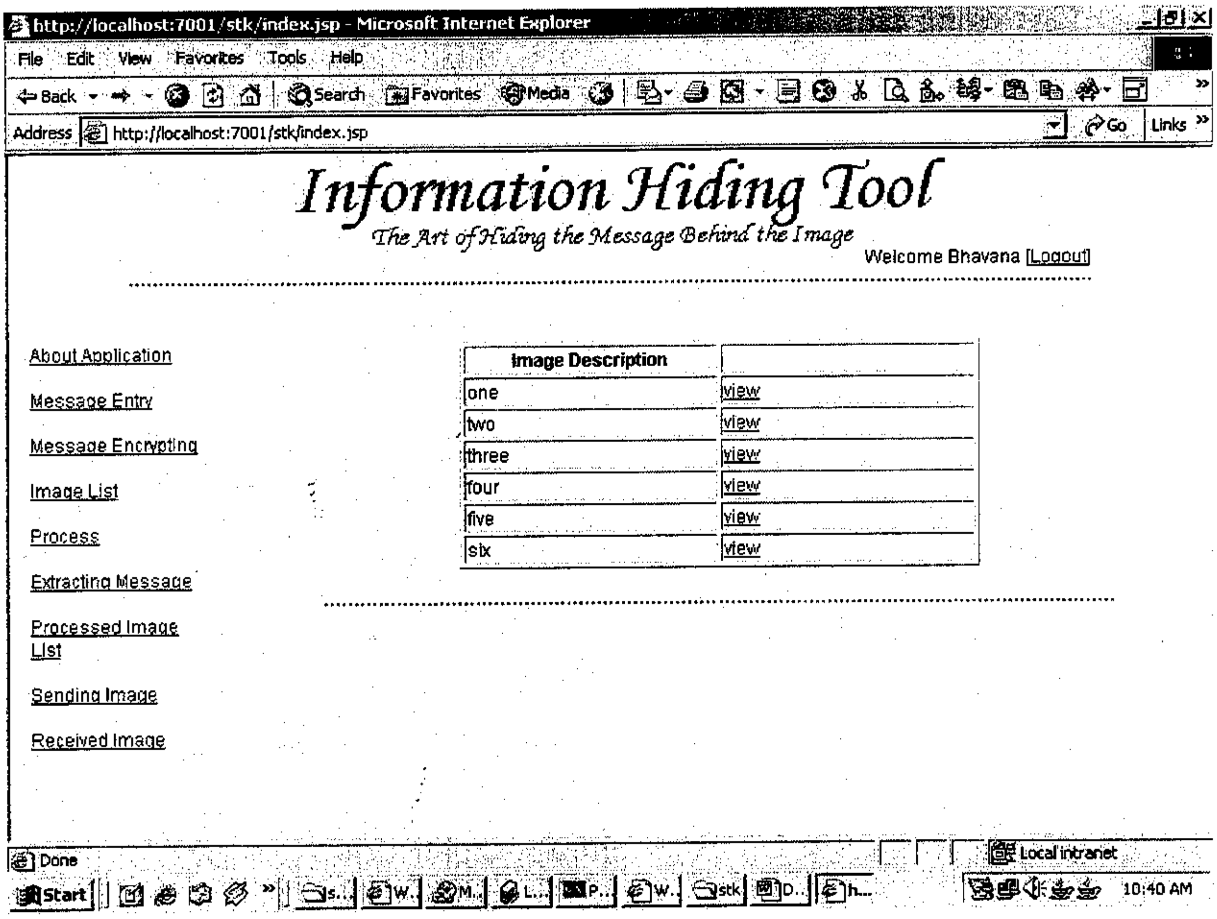
Date :

The Message

Enter a subject for your encrypted Message

hienc

Encrypt Reset



http://localhost:7001/stk/index.jsp - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost:7001/stk/index.jsp
Go Links
Done
Local intranet
Start
10:40 AM

Information Hiding Tool

The Art of Hiding the Message Behind the Image

Welcome Bhavana [Logout]

About Application

Message Entry

Message Encrypting

Image List

Process

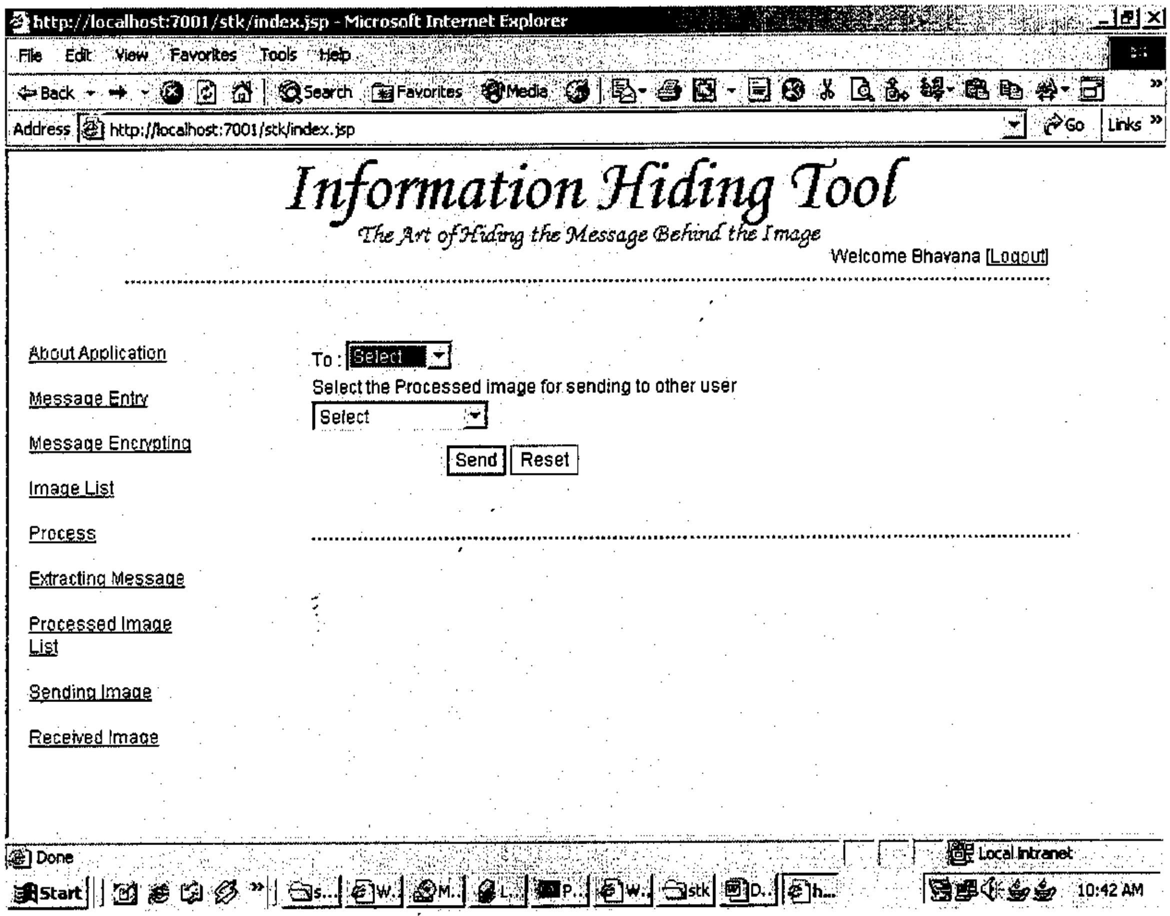
Extracting Message

Processed Image List

Sending Image

Received Image

Image Description	
one	view
two	view
three	view
four	view
five	view
six	view



http://localhost:7001/stk/index.jsp - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost:7001/stk/index.jsp
Go Links
Done
Local intranet
start
10:42 AM

Information Hiding Tool

The Art of Hiding the Message Behind the Image

Welcome Bhavana [Logout]

About Application

Message Entry

Message Encrypting

Image List

Process

Extracting Message

Processed Image List

Sending Image

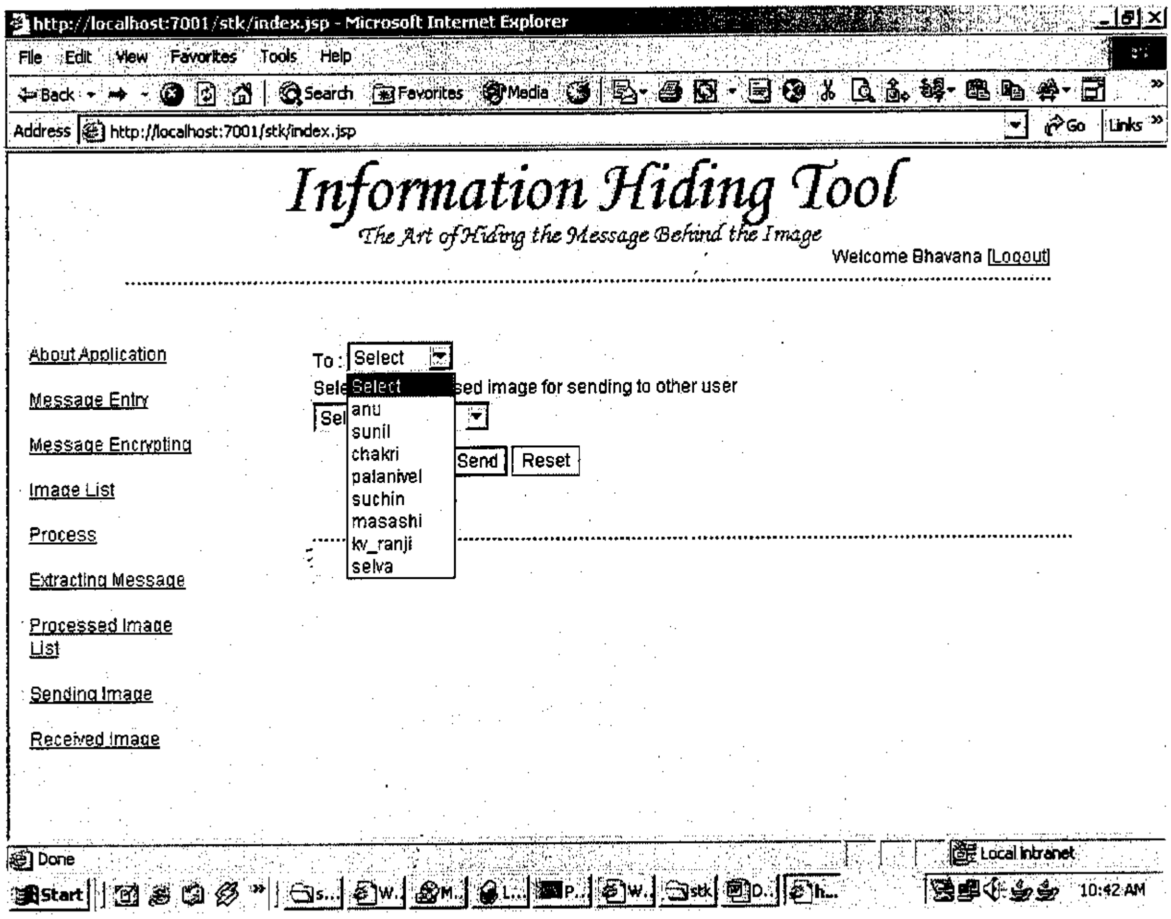
Received Image

To : Select

Select the Processed image for sending to other user

Select

Send Reset



Information Hiding Tool

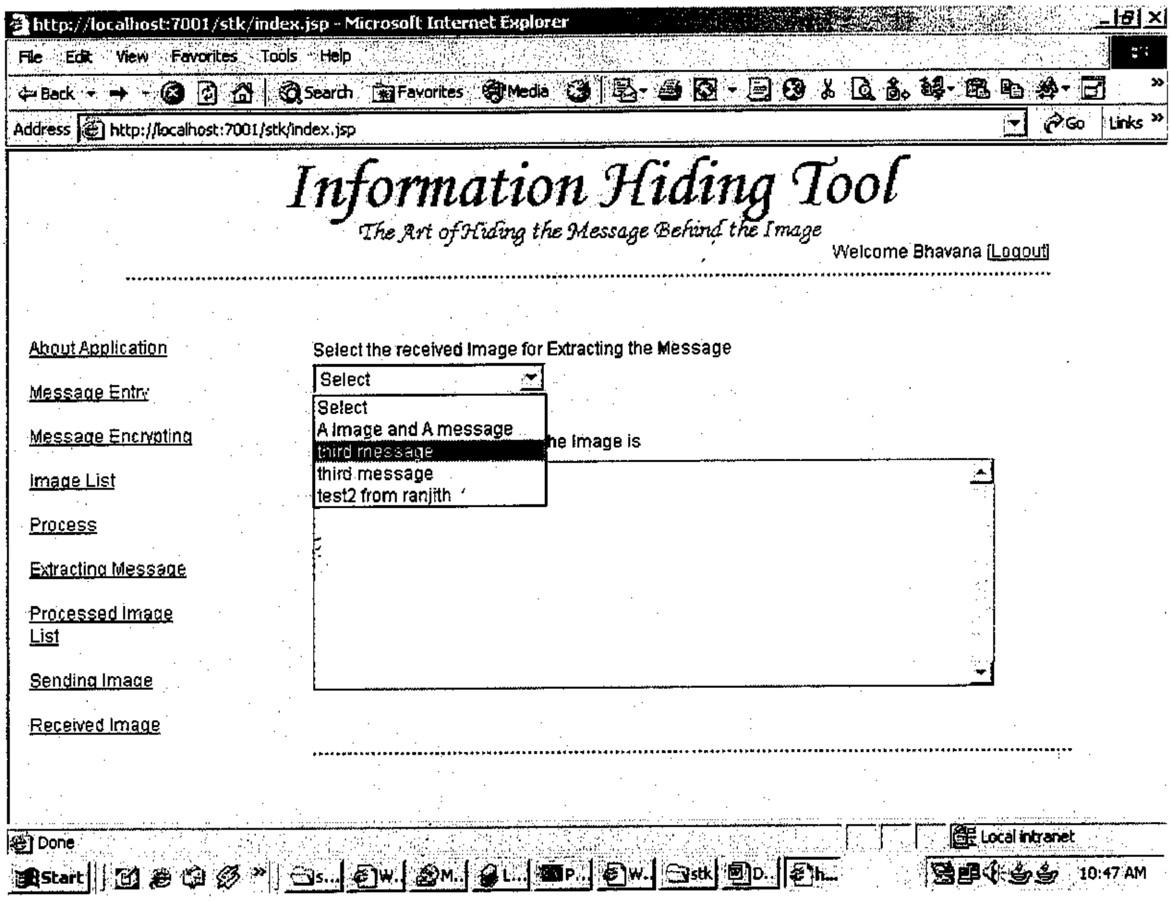
The Art of Hiding the Message Behind the Image

Welcome Bhavana [Logout]

To : Select

Sele[Select]sed image for sending to other user

Sel


http://localhost:7001/stk/index.jsp - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost:7001/stk/index.jsp
Go Links
About Application
Message Entry
Message Encrypting
Image List
Process
Extracting Message
Processed Image List
Sending Image
Received Image
Done
Local intranet
Start
10:47 AM

Information Hiding Tool

The Art of Hiding the Message Behind the Image

Welcome Bhavana [Logout]

Select the received Image for Extracting the Message

Select

- Select
- A Image and A message
- third message
- third message
- test2 from ranjith

he Image is

SYSTEM TESTING

6. SYSTEM TESTING:

Testing is the process where the test data is prepared and used for testing the module individually and later the validation given for the fields. Actually testing is the state of implementation aimed at ensuring that the system works accurately and efficiently before the actual operation commences. Testing is done with real time data obtained from the client. The results obtained are often tested with the results obtained manually in order to ensure the working of the application effectively. The system should also be tested with invalid data in order to check if the application accepts these invalid data and produces the necessary error messages. If system accepts these invalid data then it is not a perfect application. During testing if any variations are found, then necessary actions and procedures are to be taken in order to avoid it. In case of any variation it is very necessary to check all the procedures to know where the variation has occurred and ignoring such error may lead to improper working of the system.

OBJECTIVE OF TESTING:

- Testing is the process of executing a program with the intent of finding and error.
- A good test case is one that has a high probability of finding an undiscovered error.

UNIT TESTING:

Unit testing comprises the set of tests performed prior to integration of the unit into larger system. In unit testing every modules are tested independently. Subroutines in every module are tested for the correct data flow and normal exit.

INTEGRATION TESTING:

In the integration testing, the modules are joined together to make sure that they work as a group. Integration tests are performed incrementally by adding another module to the system and testing to make sure that it works properly after adding the next module.

For example, in the user registration & verification system, the user code is passed into database to check if they are valid user or not. If the condition satisfies the index page will be displayed otherwise the access to the index page is denied and through 'Sign In' link the new user can register.

VALIDATION TESTING:

Validation can be defined in many ways but a simple definition is that validation succeeds when the software function in a manner that can be reasonably expected by the customer. Software validation is achieved through a series of tests that demonstrate conformity with requirements. In certain places where the input has to be given, validation testing is done.

For example, in the User Registration module, it is mandatory for the user to enter the user id, user name, password fields. If any of these fields are left a message will be displayed asking for the fields to be filled. Another validation is also done to check whether the 'password' and 'Confirm Password' fields contain same value. If not the message "Both Password and Confirm Password must be same" will be displayed.

CONCLUSION

7. CONCLUSION:

A lot of effort has been put into this application called ‘ Information Hiding Tool’ . This tool has been developed for DHS Infomatics, Bangalore. This tool allows users to transmit data within the network in a better manner with a higher level of security and integrity. The application hides the data into digital objects like the image and then transmits the data with in the users of the network. The data may be in plain format or in encrypted format.

The users of the system have tested the application and all the necessary changes were made based on the requirements of the user and as per the guidance provided by the managers and team leads at superior levels.

APPENDIX

SOURCE CODE

Query to Create the stuser table

----

stuser

```
create table stuser
(intucode number(6) primary key,
struid varchar2(15) unique not null,
strpass varchar2(10) not null,
strname varchar2(20) not null,
straddr varchar2(100),
strcity varchar2(20),
strstate varchar2(20),
strcountry varchar2(20),
strpin varchar2(20),
strphone varchar2(15),
strmob varchar2(15),
stremail varchar2(20)
)

/
```

stmsg

```
create table stmsg
(intmsgno number(6) primary key,
intucode number(6),
mdate date,
strsubject varchar2(50),
blobmsg blob,
encryprted varchar(1),
Constraint UCODE Foreign Key (intucode)references stuser(intucode)
)


/
```

Create Query for the strecimages (Received Images table)

```
Create table strecimages
(
intfrom number(6),
intto number(6),
intpicno number(6),
recdate date,
strrecdes varchar2(50),
Constraint CoRec1 Foreign Key (intfrom)references stuser(intucode),
Constraint CoRec2 Foreign Key (intto)references stuser(intucode)
)
```

Procedure to insert into the (Received Images Table)

```
create or replace procedure
ins_send_img
(fromco in number,
toco in number,
picno in number,
rdate in date,
des in varchar
)
as
begin
insert into strecimages values (fromco,toco,picno,rdate,des);
end;
/
```

Insert Procedure for Message

```
create or replace procedure ins_msg
( ucode in number,
mdate in date,
sub in varchar,
msg in blob)
is
begin
insert into stmsg
values(intmsgno.nextval,ucode,mdate,sub,msg,'N');
end;
```

Create for the encrpted Message Table.

```
create table stemsg
(intemsgno number(6) primary key,
intucode number(6),
emdate date,
stresubject varchar2(50),
blobemsg blob,
Constraint UECODE Foreign Key (intucode)references stuser(intucode)
)
/
```

Insert procedure for Encrypted Message

```
create or replace procedure ins_emsg
( ucode in number,
emdate in date,
esub in varchar,
emsg in blob)
is
begin
insert into stemsg
values(intemsgno.nextval,ucode,emdate,esub,emsg);
end;
/
```

Picture table

```
create table stpicture
(intpicno number(6) primary key,
strpicpath varchar2(50),
ptrpicdesc varchar2(50)
)
```

Processed Picture Table.

```
create table stpropic
(intpropicno number(6) primary key,
intucode number(6),
strpropath varchar2(50),
strprodesc varchar2(50),
strmsgtype varchar2(1),
Constraint FPRO Foreign Key (intucode)references stuser(intucode)
)
/
```

Very New Insert Procedure

```
create or replace procedure
ins_pro_img
(ucode in number,
imgdis in varchar,
msgtype in varchar,
picno out integer)
as
begin
select intpropicno.nextval into picno from dual;
insert into stpropic (intpropicno,intucode,strprodesc,strmsgtype) values
(picno,ucode,imgdis,msgtype);
end;
/
```

BIBILOGRAPHY

SCOPE FOR FURTHER DEVELOPMENT

Every end line is the new beginning for this project. According to cryptography and virus it keeps on new invention. The authentication may be little more added, some which existing in the project will be supporting.

The security can be improved by adding the authentication. Such as online voice reorganization, video tracking of the user can be controlled using the user. The algorithm which is new will be defeated by global hackers and there will be new algorithm to develop new security program.

The designing face is well and it is suitable for future enhancement and with that the existing algorithm can be used with some other combination to keep the system and data transferring in the network secure.

BIBILIOGRAPHY

1. Professional Java Server Programming (2000 Edition) – by Work Programmer to Programmer

2. JSP Tag Libraries by Gal Shachar, Adam Chace and Magnus Rydin.

3. Java 2 Complete Reference by Herbert Schildt (Tata McGrawHill Publishing Company Lmt)

4. Java Server Pages Fast & Easy Web Development – Aneesha Bakharia

5. Oracle 9i –HandBook

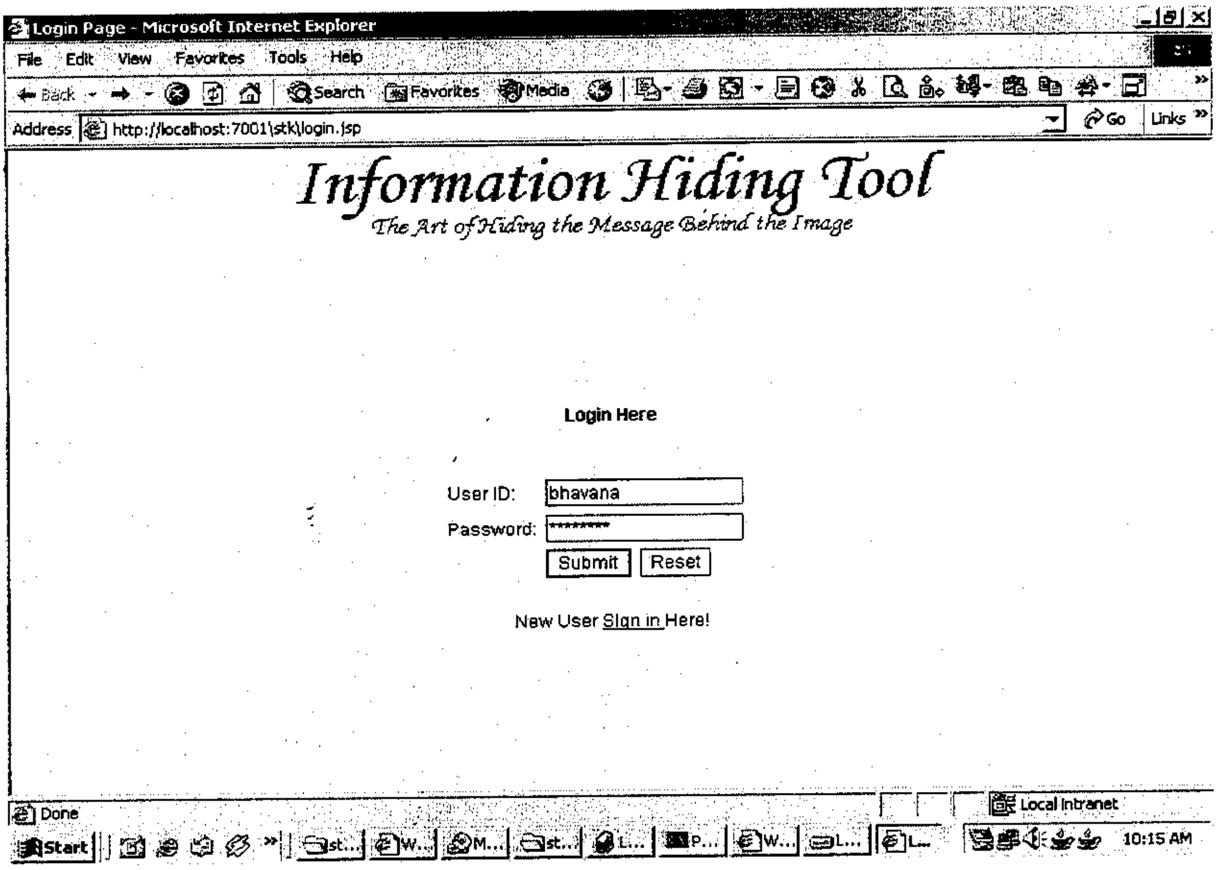
6. www.jsptags.com

7. www.jspin.com

8.Elias M.Awad, "System Analysis And Design", -Galgotia Publications (p) Ltd…

Appendix

Forms



Login Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost:7001\stk\login.jsp
Go Links
Information Hiding Tool
The Art of Hiding the Message Behind the Image
Done
Local intranet
Start
10:15 AM

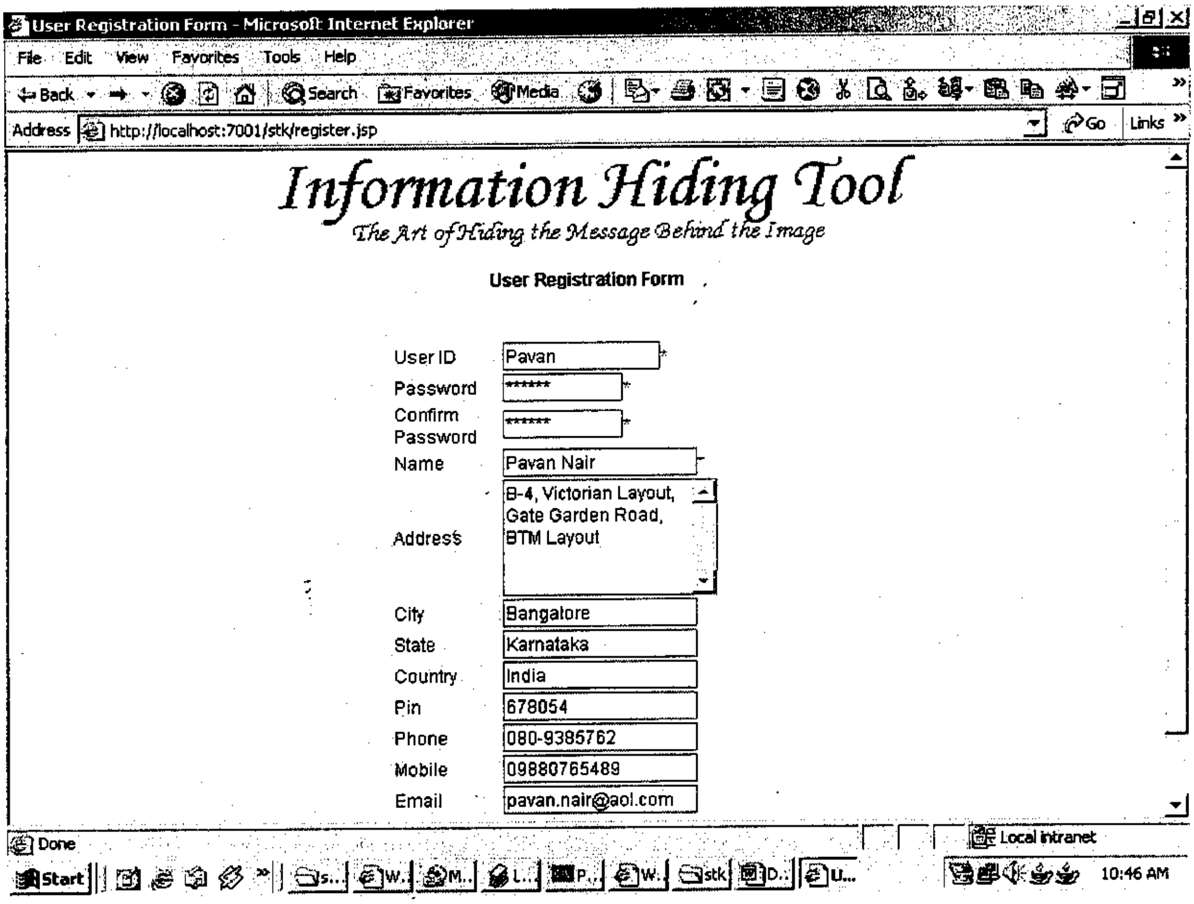
Login Here

User ID: bhavana

Password: *********

Submit Reset

New User Sign in Here!



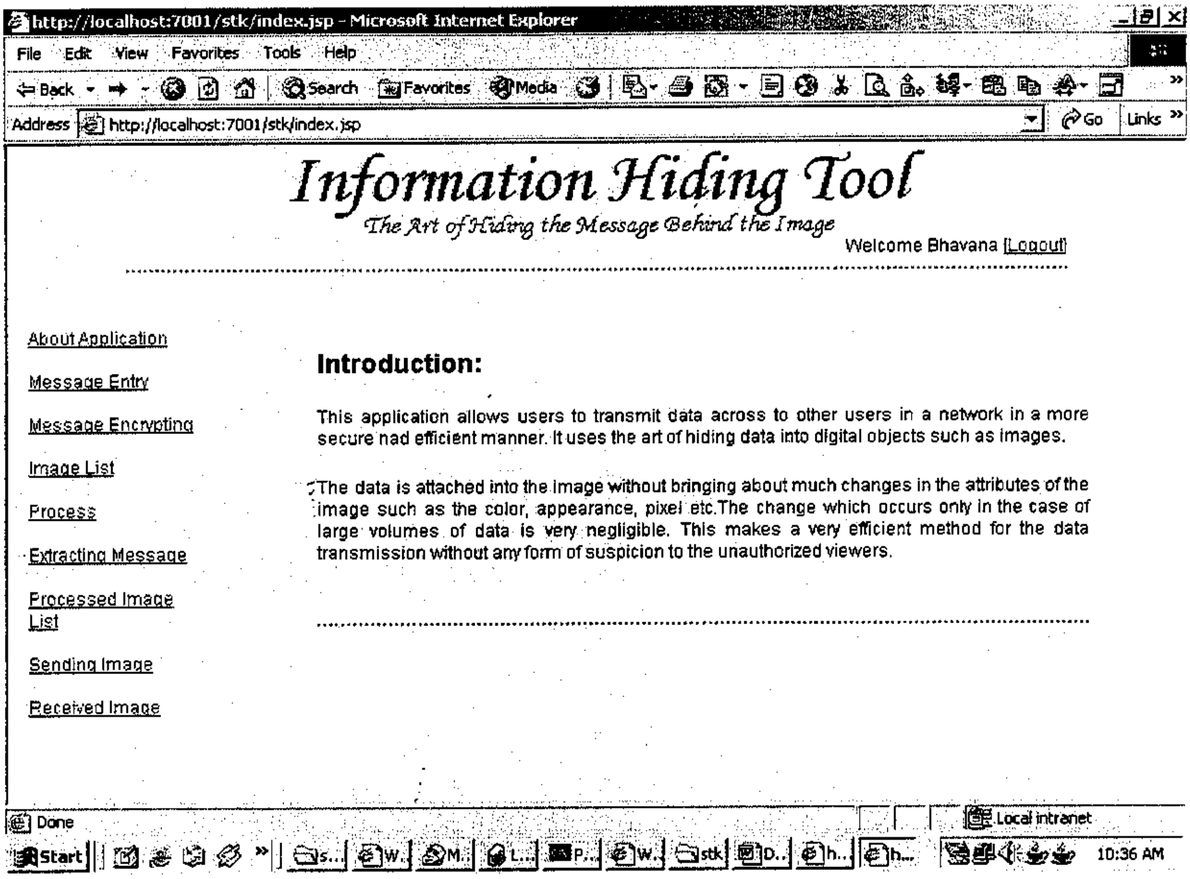
User Registration Form - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost:7001/stk/register.jsp
Go Links
Done
Local intranet
Start
10:46 AM

Information Hiding Tool

The Art of Hiding the Message Behind the Image

User Registration Form

User ID	Pavan *
Password	****** *
Confirm Password	****** *
Name	Pavan Nair *
Address	B-4, Victorian Layout, Gate Garden Road, BTM Layout
City	Bangalore
State	Karnataka
Country	India
Pin	678054
Phone	080-9385762
Mobile	09880765489
Email	pavan.nair@aol.com



Information Hiding Tool

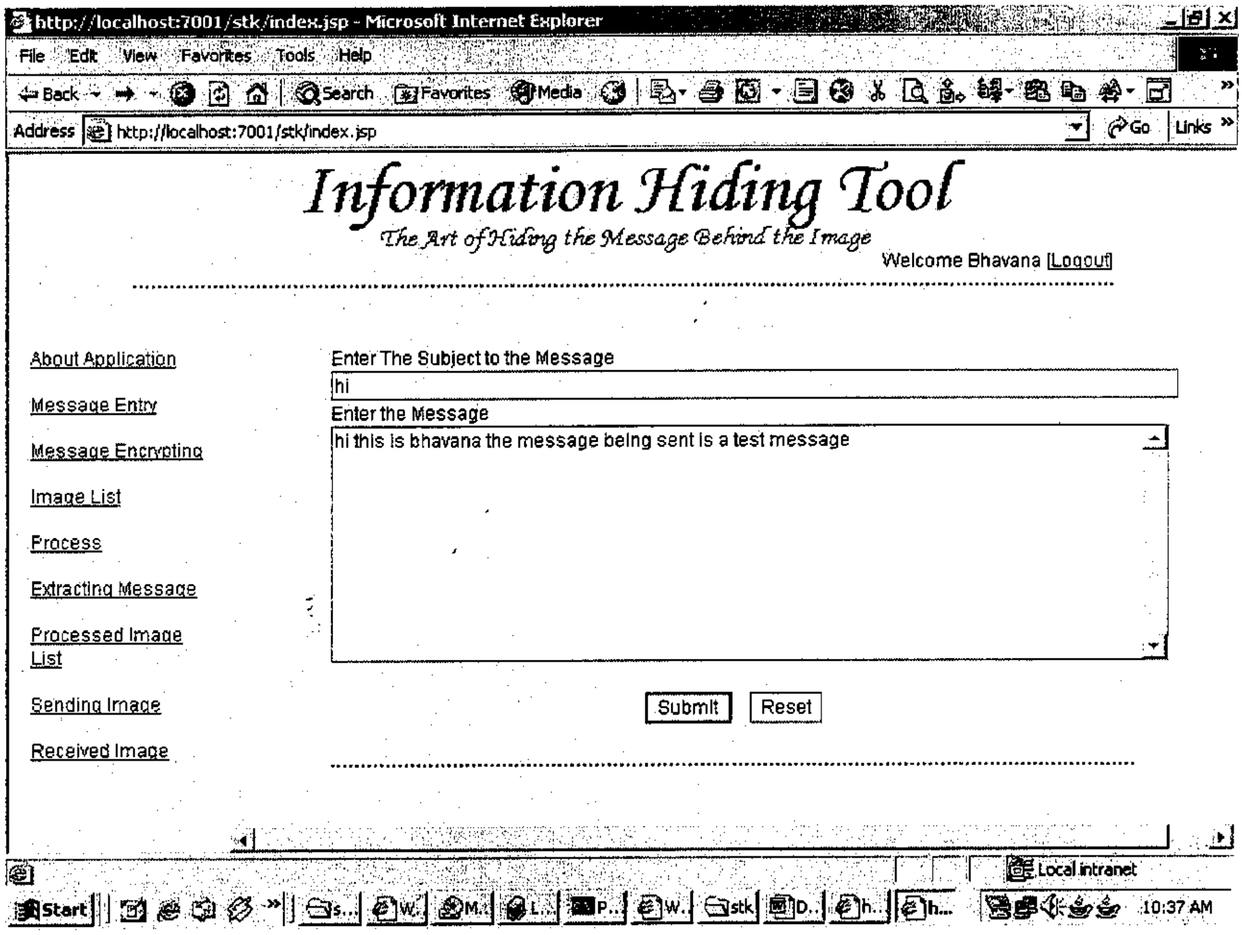
The Art of Hiding the Message Behind the Image

Welcome Bhavana [Logout]

Introduction:

This application allows users to transmit data across to other users in a network in a more secure nad efficient manner. It uses the art of hiding data into digital objects such as images.

The data is attached into the image without bringing about much changes in the attributes of the image such as the color, appearance, pixel etc.The change which occurs only in the case of large volumes of data is very negligible. This makes a very efficient method for the data transmission without any form of suspicion to the unauthorized viewers.



Information Hiding Tool

The Art of Hiding the Message Behind the Image

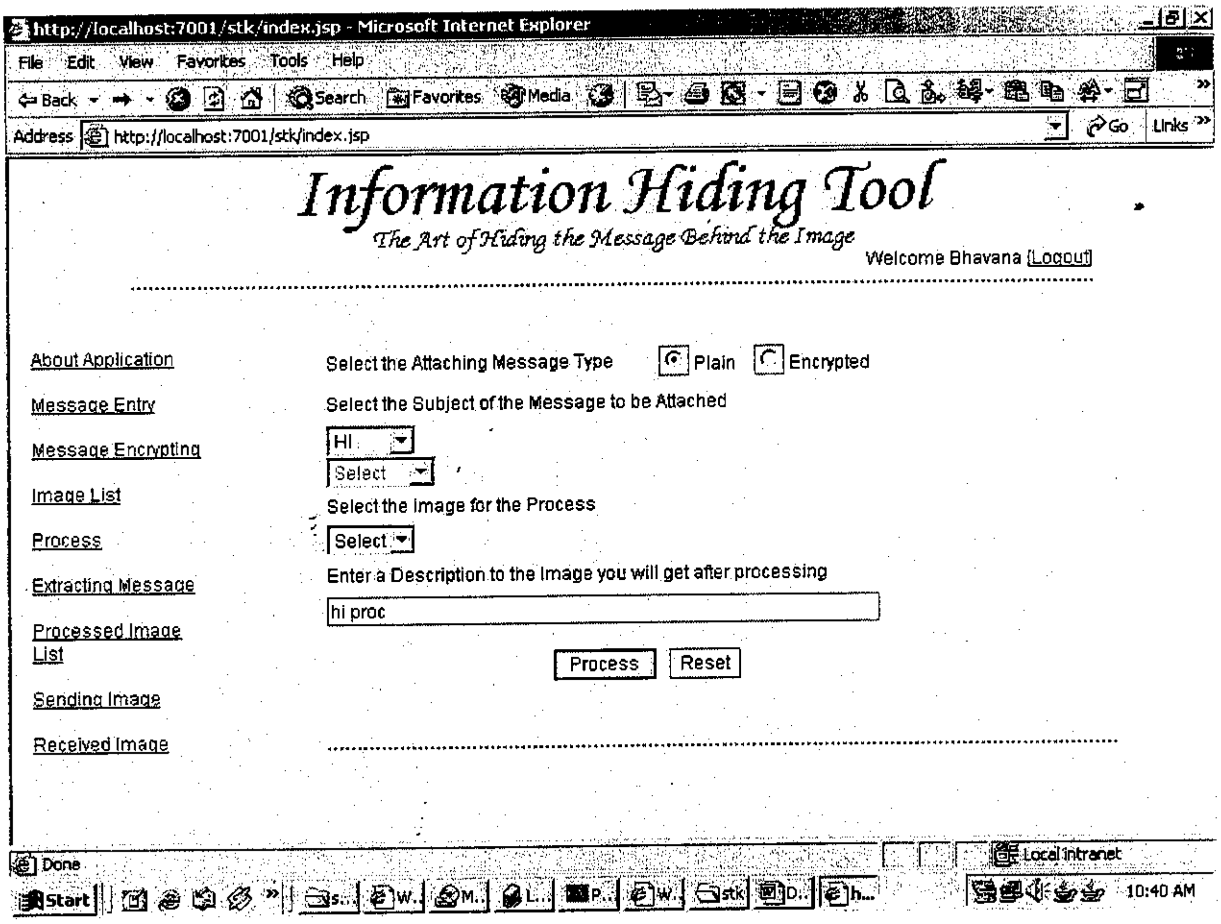
Welcome Bhavana [Logout]

Enter The Subject to the Message

hi

Enter the Message

hi this is bhavana the message being sent is a test message



http://localhost:7001/stk/index.jsp - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost:7001/stk/index.jsp
Go Links
Done
Local intranet
Start
10:40 AM

Information Hiding Tool

The Art of Hiding the Message Behind the Image

Welcome Bhavana [Logout]

Select the Attaching Message Type ● Plain ○ Encrypted

Select the Subject of the Message to be Attached

HI

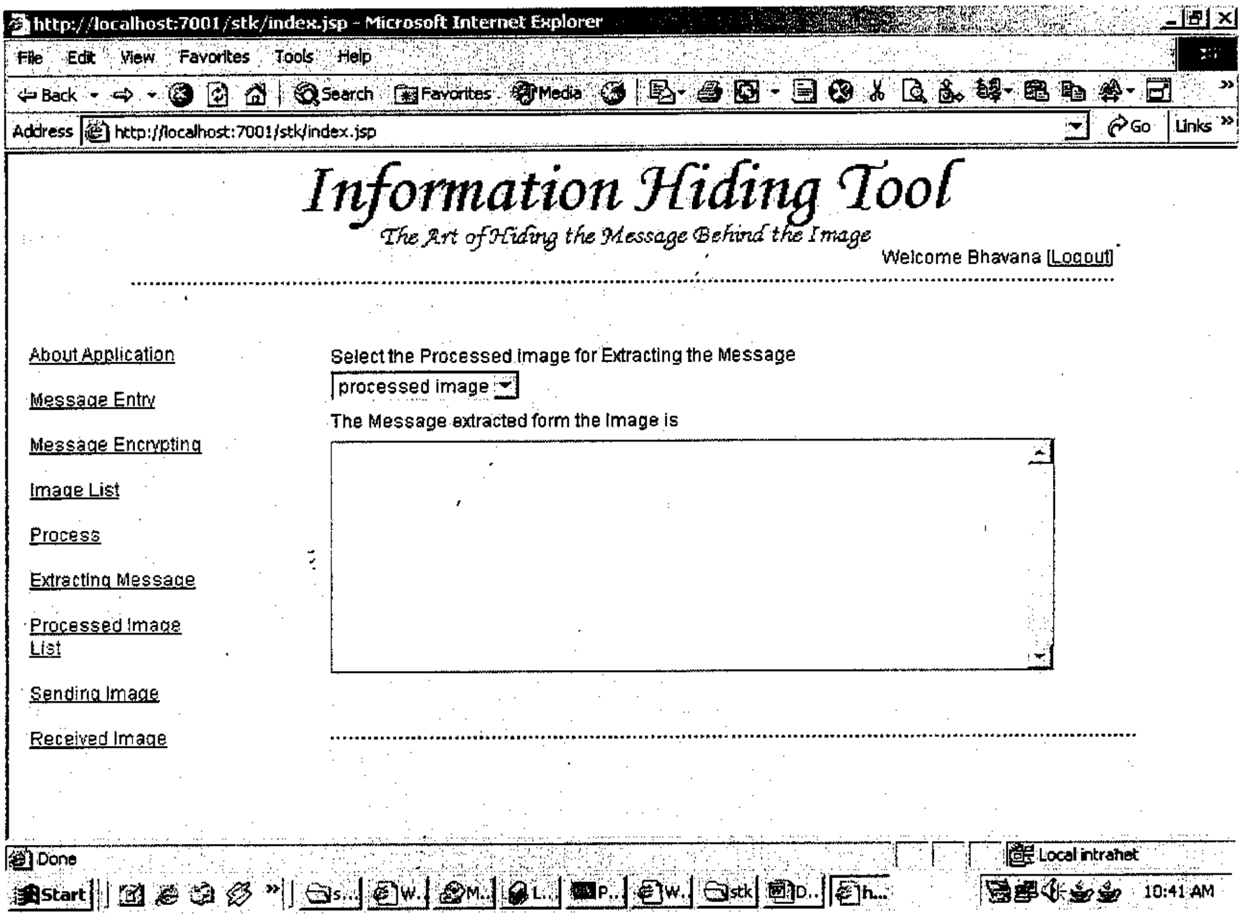
Select

Select the Image for the Process

Select

Enter a Description to the Image you will get after processing

hi proc


http://localhost:7001/stk/index.jsp - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost:7001/stk/index.jsp
Go Links
Done
Local intranet
Start
10:41 AM

Information Hiding Tool

The Art of Hiding the Message Behind the Image

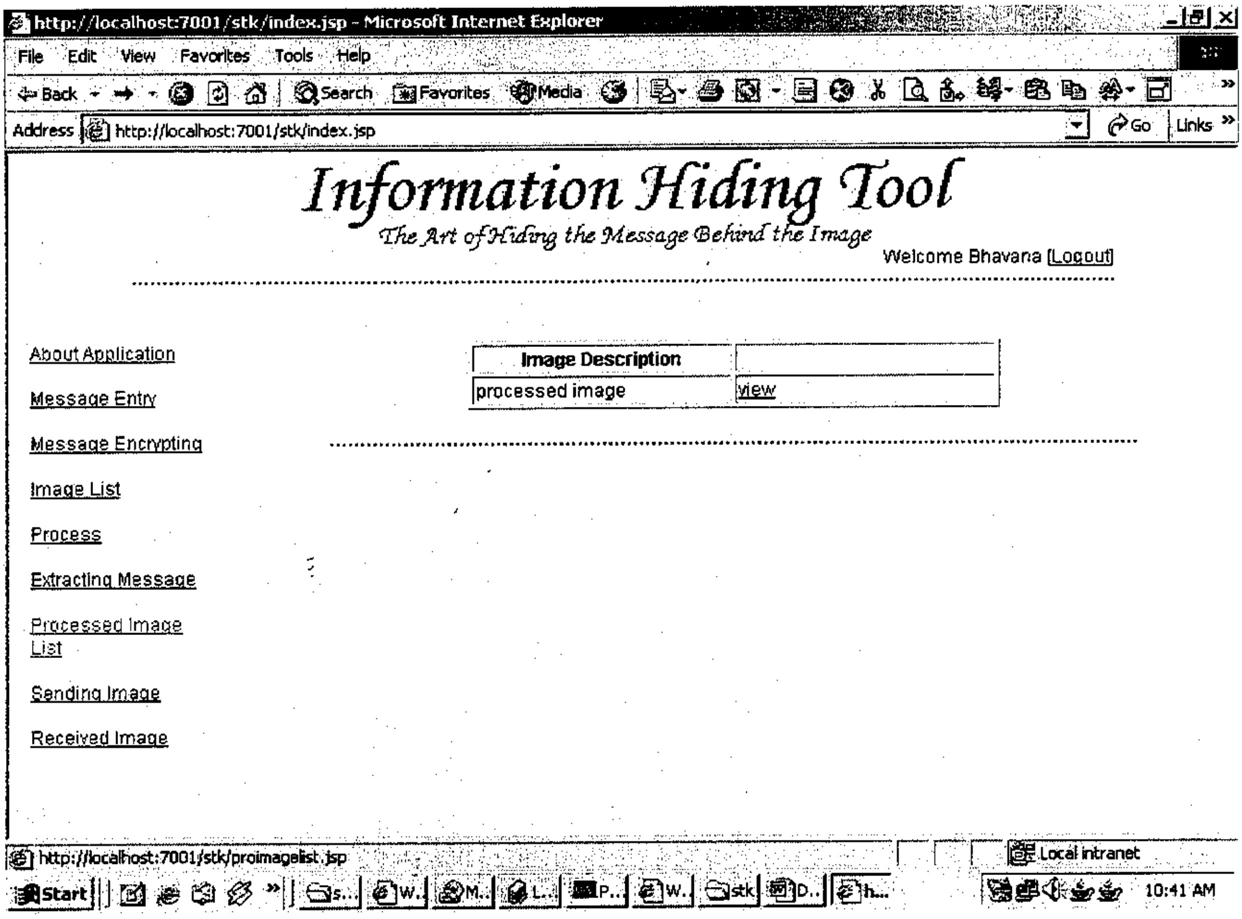
Welcome Bhavana [Logout]

About Application
Message Entry
Message Encrypting
Image List
Process
Extracting Message
Processed Image List
Sending Image
Received Image

Select the Processed image for Extracting the Message

processed image

The Message extracted form the Image is



http://localhost:7001/stk/index.jsp - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost:7001/stk/index.jsp
Go Links

Information Hiding Tool

The Art of Hiding the Message Behind the Image

Welcome Bhavana [Logout]

- About Application
- Message Entry
- Message Encrypting
- Image List
- Process
- Extracting Message
- Processed Image List
- Sending Image
- Received Image

Image Description	
processed image	view

http://localhost:7001/stk/proimagelist.jsp
Local intranet
Start
10:41 AM