FINGERPRINT RECOGNITION SYSTEM

PROJECT REPORT

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE OF

M.Sc (APPLIED SCIENCE - COMPUTER TECHNOLOGY)

OF BHARATHIAR UNIVERSITY

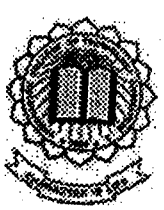
Submitted by

V.C.Komathi

Reg. No – 0137Q0041

Guided by

Mr. M.Ramasubramaniam, M.C.A



Department of Computer Science and Engineering

Kumaraguru College of Technology
(Affiliated to Anna University)

Coimbatore – 641 006

APRIL 2003

KUMARAGURU COLLEGE OF TECHNOLOGY

(Affiliated to Anna University)
Department of Computer Science and Engineering

Coimbatore – 641006

CERTIFICATE

This is to certify that the project work entitled

"FINGERPRINT RECOGNITION SYSTEM"

Done by

V.C.Komathi

Reg. No – 0137Q0041

Submitted in partial fulfillment of the requirement for the award of the degree of M.Sc (Applied science - Computer Technology) of Bharathiar University.

Head of Department

Internal Guide

Submitted to University Examination held on 10-5-2003

Internal Examiner
ap/cse/kct (10-5-03)

External Examiner

DECLARATION

I here by declare that the project work entitled
"FINGER PRINT RECOGNITION SYSTEM"

Done at

SARVA SHRADDHA BUSINESS (I) SOLUTIONS LIMITED
CHENNAI

And submitted to

KUMARAGURU COLLEGE OF TECHNOLOGY
(Affiliated to Anna University)

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

M.Sc (APPLIED SCIENCE - COMPUTER TECHNOLGY)

is a report of work done by me during my period of study in
Kumaraguru College of Technology, Coimbatore – 641 006.

Under the supervision of
Mr. M.Ramasubramaniam, M.C.A , Dept. of CSE

Name of the candidate	Register Number	Signature of the candidate
V.C.KOMATHI	0137Q0041	V. Kothi

Date: 10-5-2003

SARVA SHRADDHA BUSINESS SOLUTIONS (I) LTD.
Ist Floor, Gowtham Arcade, 208, T.V. Samy Road (E), R.S. Puram, Coimbatore - 641 002.
Ph : 0422-540566 E-mail : ssbsil@eth.net

April 7, 2003

PROJECT COMPLETION CERTIFICATE

This is to certify that **Ms. V. C. Komathi**, a student of Kumaraguru College of Technology, Coimbatore has successfully completed the Live Project titled **"Finger Print Recognition System"** using **C** and **Networking** at our Project Development Center. The Project commenced from January 2003 and completed on April 6 2003. The performance of the student with regard to the above-mentioned project was good.

For Sarva Shraddha Business Solutions (I) Limited

A. Giridhar
Director

M. Subramaniam
Project Manager

ACKNOWLEDGEMENTS

ACKNOWLEDGEMENTS

An endeavor over a long period can be successful only with the advice and support of many well wishers. We take this opportunity to express our gratitude and appreciation to all of them.

We, the students of Kumaraguru College of Technology are really proud in doing our project at SSBIL,Coimbatore.

We are bound to express our gratitude to **Dr.K.K.Padmanaban Phd,** Principal, Kumaraguru College of Technology, for his constant encouragement throughout our course.

We wish to thank **Dr.S.Thangasamy** H.O.D of Computer Science & Engineering Department for constantly encouraging us to pursue new goals and ideas.

We thank our Course coordinator **Mr.R.Dinesh B.E,M.S,** for guiding us throughout the project.

We admit our heart felt thanks to our internal project guide **Mr.K.Ramasubramanian M.C.A**, faculty member in Computer Science Department for being supportive throughout the project.

We owe much to **Mr.K.K.Venkataraman M.C.A and Mr.M.Subramaniam M.C.A** for their inspiring advice, immense help, and wholehearted support and constant encouragement throughout the tenure of this project work at their esteemed organization.

We express our gratitude to the **Mr.G.Rajagopal** of SSBIL for giving us a project in satisfying their needs.

We wish to thank all our friends and our family members who were showing their contributions in many subtle ways and indeed instrumental in achieving final results.

SYNOPSIS

SYNOPSIS

The main objective of our project is to provide unique GIFS (Graphical Interchange Format) for each and every user in order to provide a secure method of logging into the system. The Finger Print Recognition System is being designed in such a fashion that the centralized server will have a collection of fingerprints stored in it. While working in the node the users fingerprint is being checked with the server and the same is used for entering into the system.

To achieve all the above said concepts we need the system to be networked with a centralized server for safety accessing of the Finger Print Recognition System, because the entire project revolves around the server connected through TCP/IP. Under this mechanism, the Administrator has entire power for the application present in the Software. Further, the administrator reserves the rights to distribute application powers for the users.

CONTENTS

CONTENTS

PURPOSE

1.1 PURPOSE

Sarva Shraddha Business Solutions (I) Ltd

Sarva Shraddha Business Solutions (I) Ltd (SSBSIL) has been in the field of Software Development, Networking and Web designing business for 2 years.SSBSIL is fast and steadily growing software company based at Coimbatore started by enthusiastic, deterministic and dynamic entrepreneurs. Since inception they have created over 20 successful projects.

They have a reputation of delivering the projects in time and to the specification provided. They handle projects in html web page design, application projects, java scripting, networking projects or a complete customized database.

SHRADDHA, The Sanskrit word indicates "Perfection". Keeping up to the motto, the group has been pioneers in the field of Financial Services, and leaders in Computer Training, Software Development and Manpower recruitment for overseas corporations.

Sarva Shraddha Business Solutions(I) Ltd, The development division of the group, involved in development of Customized solutions for its corporate clients and its channel partners. This division is currently pursuing its projects in the field of Financial Services, Banking, Manufacturing and Trading. The group has currently forayed its activity in Man power recruitment for its overseas clients. The group acts as a Technical Evaluation partner for M/s.Exalt Interactive, a division of M/s.Lancesoft Inc, Virginia. SSBS(I)L, acts as Indian Representative for companies at Ireland and United States of America, for its man power requirement.

SCOPE

1.2 SCOPE

The main objective of our project is to provide unique GIFS (Graphical Interchange Format) for each and every user in order to provide a secure method of logging into the system. The Finger Print Recognition System is being designed in such a fashion that the centralized server will have a collection of fingerprints stored in it. While working in the node the users fingerprint is being checked with the server and the same is used for entering into the system.

This system utilizes the category of Login for usage of the application, which is categorized Administrator. The mechanism would be a strip down version of authorization of powers to users. Here the user has to enter the selected gifs name in the encrypted format to login to the system instead of the password mechanism of logging onto the system. Each users own fingerprint is provided or assigned to the user by the administrator.

To achieve all the above said concepts we need the system to be networked with a centralized server for safety accessing of the Finger Print Recognition System, because the entire project revolves around the server connected through TCP/IP. Under this mechanism, the Administrator has entire power for the application present in the Software. Further, the administrator reserves the rights to distribute application powers for the users.

DEFINITIONS, ACRONYMS, ABBREVIATIONS

1.3 DEFINITIONS

Ports

Port is the memory address to which information is transferred. It is the communication that allows devices to be physically attached. Logical port specified by a 16-bit number, which is port of TCP/IP uniquely, identifies the application running on that computer.

Sockets

A socket is a communication mechanism. A socket is normally identified by a small integer, which may be called the socket descriptor. It is the fundamental Internet network-programming interface. Sockets achieve sending and receiving data.

Protocol

Protocols are rules required to help entities, Communicate or understand Each other's protocol can be one rule or complete set of rules and standards that allow different devices to hold conversation. The protocol that has been used in this project is TCP/IP.

Interrupt Request

Serial port information resides at specific memory addresses and **interrupt requests** (**IRQs**.) An IRQ is a request-for-attention signal that can be passed by either hardware or software to a computer's microprocessor.

Hosts

A host is essentially anything on the network that is capable of receiving and transmitting IP packets on the network, such as a workstation or a router.

Server

A server is a program that provides some service. It runs continuously waiting for a client to connect to it. Server programs listen for incoming connections. When incoming connection is detected the server program can accept the connection, after which the i/p, o/p can occur

Client

A client is a program that connects to a server program to perform some services .A client program is run only when the service is needed.

1.3 ACRONYMS&ABBREVIATIONS

TCP/IP- Transmission Control Protocol/Internet Protocol

IRQ- Interrupt Request

ARP- Address Resolution Protocol

ICMP-Internet Control Message Protocol

IPX-Internet Packet Exchange

DOD-Department of Defense

GIF- Graphical Interchange Format

REFERENCES

1.4 REFERENCES

The head of Sarva Shraddha Business (I) India Solutions Mr.G.Rajagopal allotted us the project entitled "Fingerprint Recognition System" and directed us to our guide in SSBIL.

Our external guides Mr.K.K.Venkataraman and Mr.M.Subramaniam gave us immense help, wholehearted support and constant encouragement throughout the tenure of this project work at their esteemed organization.

Our internal guide Mr.K.Ramasubramanian helped as by sharing his ideas and views of developing a networking project using c language.

OVERVIEW

1.5 OVERVIEW

The system has to be networked with a centralized server for safety accessing of the Finger Print Recognition Software, because the entire project revolves around the server connected through TCP/IP. Here the users finger print is taken by using the scanner and is stored in the gif format. The server has the collection of fingerprint gifs stored in it. Each and every user is assigned a unique fingerprint GIF by the administrator. If the administrator assigns an already allotted GIF to another user then the administrator will be indicated that the fingerprint GIF was already assigned. On the client side the user enters the user name and the fingerprint GIFs name assigned by the administrator in the encrypted format.

Once the user gives the name of the fingerprint GIF on the client side then it searches for that particular GIF from the collection of fingerprint GIFS that is stored in the server. The fingerprint GIF that is assigned to the user is displayed in a palette on the client machine. The fingerprint GIF that is selected by the user is checked with the fingerprint that is stored in the server assigned by the administrator for that user. If the user enters a GIFS name that wasn't assigned by the administrator then an error message will be given to the user stating that the user has typed a GIFS name that wasn't assigned. If the fingerprint matches then the user is allowed to access the desktop else the access to the desktop is denied.

The Fingerprint Recognition System is a tool, which can be used even in the intelligence department to find out the criminal by matching the fingerprints of the criminal

GENERAL DESCRIPTION

2 GENERAL DESCRIPTION

2.1 PRODUCT PERSPECTIVE

LOGIN SETUP

The Fingerprint Recognition system provides a secure way of logging into the system .The server has a collection of fingerprints stored in it. When the user enters the username and the name of the gif assigned to the user by the administrator in an encrypted format a pixel-by-pixel comparison is done based on the pixel and spatial co-ordinate algorithm. If there is a match between the finger print given by the user on the client machine and the assigned fingerprint that is stored in the server for the username created for that user then the user will be allowed to access the desktop else the access is denied.

MENU SETUP

Menu Setup is used for accessing the Finger Print Recognition System with ease. But the restriction is maintained from the login setup. The entry can be made into the system when the fingerprint is matched. The each fingerprint is being recorded in file-formatted report.

The Finger Print Recognition System is being designed in such a fashion that the provision is being provided for logging into the system with security. In the menu setup on the server side provisions are given for creating a new user, modifying the username and deleting the already existing user. Each and every user is provided with a unique fingerprint gif, which is assigned by the administrator.

The Help Menu is provided for easy access and to maintain the stability. It gives information on how to use the tool with ease.

PRODUCT FUNCTIONS

2.2 PRODUCT FUNCTIONS

The user's fingerprint logging onto the system from local node matches the Fingerprint in the server via TCP/IP Client - Server Architecture. Once the connection between the server and client is being established, the node tracks the address of the same routes the link to the server fingerprint database and gets logged to the System.

The Project is done for security purpose since some password misuse is being made with out the notice of the administrator. So a safety system is planned for effective usage of the system. Through this project the administrator has been vested all powers to restrict the anonymous user's logging into the system (i.e.) whose fingerprint gets matched will get logged into the system. The users fingerprint is scanned and is stored in the server. The administrator creates a new user and assigns a unique fingerprint gif to that user. If suppose the fingerprint which is assigned to one user is assigned to an another user then an error message will be given to the administrator that the GIF has been already allotted.

USER CHARACTERISTICS

2.3 USER CHARACTERISTICS

The project is characterized in such a way that it is very user friendly and shortcut keys is provided for easy access of the Fingerprint Recognition System. The User screens are maintained in a secured manner, each and every user has a separate unique username and a scanned fingerprint gif that cannot be edited by the user, since the gif's are stored in a centralized server. The administrator assigns the unique fingerprint gif and the user name to the user.

Whenever a fingerprint is to be changed, the user should contact the administrator for changing the gifs. The user has to enter the username and the unique gifs name in encrypted format assigned by the administrator on the client side. The fingerprint that corresponds to that username will be searched from the collection of finger prints stored in the server and will be displayed on the client screen. A comparison of the fingerprint is made with that stored in the server assigned for that particular username. If a match is found between the fingerprints then the user is allowed to access the desktop else the access is denied. This tool can also be used in the intelligence department to compare the fingerprints of the criminal.

GENERAL CONSTRAINTS

2.4 GENERAL CONSTRAINTS

The administrator assigns the username and the users fingerprint gif for each and every user. The user has to enter the user name and the fingerprint gifs name in an encrypted format to login to the system. A search is made on the collection of fingerprints that is stored in the server and that particular gif corresponding to the name given by the user is displayed in a palette on the client machine. The gif that is placed in the client machine is compared with that stored in the server assigned by the administrator for that particular username.

If the administrator assigns an already allotted GIF to a user then an error message will be given to the administrator that the GIF has already been allotted. The user cannot edit the scanned fingerprint GIF that is assigned by the administrator since the fingerprint GIFS are stored in a centralized server. If the user has to make any changes due to any injury then the user has to consult the administrator

SPECIFIC REQUIREMENTS

3 SPECIFIC REQUIREMENTS

3.1 FUNCTIONAL REQUIREMENTS

3.1.1 LIST OF INPUTS

Input design is a process of converting user-organized input into Computer-based format. To enter the various data captured through the paper forms into the system, screens are designed. The elements are shown in the screen by which any user can easily follow. The input to the system was designed such that the required information can be collected and corrected quickly.

The goal of input design is to make data entry easier, logical and free from errors.

The decisions made during input design are:

- To provide cost effective methods of input.
- To achieve the highest possible level of accuracy.
- To ensure that input is understood by user.

Input data of a system may not necessarily be raw data captured into the system. These can also be output of another system or subsystem. The design of input covers all phases of input from the creation of initial data to actual entering of data into the system for processing. It involves identifying the data need, specification the characteristics of each data item, ensuring correctness of data.

The users fingerprint gif is given as input to the system, which is routed, to the server via TCP/IP architecture. The user selected fingerprint gif is checked with the gif stored in server. If a match of the fingerprint gifs are found then the user is allowed to access the desktop else the access is denied.

3.1.2 INFORMATION PROCESSING REQUIRED

The administrator assigns the username and the unique fingerprint gif for each and every user. On the client side the user has to enter the username and the unique finger print gifs name in encrypted format to login to the system. A search is made on the collection of fingerprints stored in the server and that particular fingerprint will be displayed on the palette in the client machine. If there is a match found between the fingerprints that is placed on the client machine and the one that is stored in the server assigned by the administrator for that user name then the user is allowed to access the desktop

3.2 PERFORMANCE REQUIREMENTS

3.2.1 SECURITY

Good security involves careful planning of a security policy, which should include access control and authentication mechanisms. These security strategies and procedures can range from a very simple password policy to complex encryption schemes with gifs usage. The Security is maintained from the Operating System that the users use. The Normal Mode of Internet Security is through the TCP/IP Layers of Protocols, which is being used in this project.

Gif level of entry into the system for any company can be an important security method and provides one of the most basic security services in a network authentication exchange.

There are several encryption techniques available on the market, using several kinds of algorithms, but the two main ones are the ones using keys and those not relying on keys at all.

Encryption techniques not using any keys are very simple and they work by transforming, scrambling, and the information being

encrypted. For instance, we could encrypt a message written in English text by just adding a number to the ASCII value of each letter, which could give a result. Although apparently secure, this sort of algorithm is not so secure. Actually, they are very easy to decipher. Once we learn the algorithm we will be able to decipher the encrypted information.

With private key gif entry algorithms, only one gif exists. The same gif position is used for both encryption and decryption. In order to ensure security, we must protect this gif and only we should know it. Another characteristic of private gif encryption is that the gifs used are usually small, making its algorithms computation relatively fast and easier then asynchronous ones.

One of the main limitations of using private gif encryption is when distributing it to everyone (users) who needs it, especially because the distribution itself must be secure. Otherwise we could expose and compromise the gif and therefore, all the information encrypted with it. Thus, it becomes necessary for us to change your private gif encryption every so often.

3.2.2 AVAILABILITY

The Fingerprint Recognition System works in the windows NT environment.

WINDOWS NT OPERATING SYSTEM

Windows NT was designed to scale to business needs: huge capacity to accommodate large, growing applications; portability across multiple hardware architectures; and the ability to add processing power as the system and applications demand it.

INTEGRATED FEATURES FOR ENTERPRISE SOLUTIONS

Windows NT includes key features built into the operating system that make client-server solutions easier to deploy:

- ✓ Integrated networking for basic file and print sharing and easy access to enterprise resources.
- ✓ A single user version of Windows NT Remote Access Service allows users to access their system and the network remotely. A complete, multi-user version is included with the Windows NT Advanced Server.
- ✓ Built-in workgroup features, including electronic mail and group scheduling, enhance workgroup productivity.
- ✓ Graphical administration tools, including performance monitor and event viewer, make it easy to optimize Windows NT platforms anywhere on the network.

3.2.3 CAPACITY

Software Capacity and validation is achieved through a series of tests that demonstrate conformity with the requirement. A test plan outlines the classes to test to be conducted and a test procedure defines specific test cases that will be used to demonstrate conformity with the requirements. Both, the planned the procedures are designed to ensure that all functional requirements are archived, documentation is correct and other requirements are met. After each software test case has been conducted, one of the two possible conditions exists.

They are:

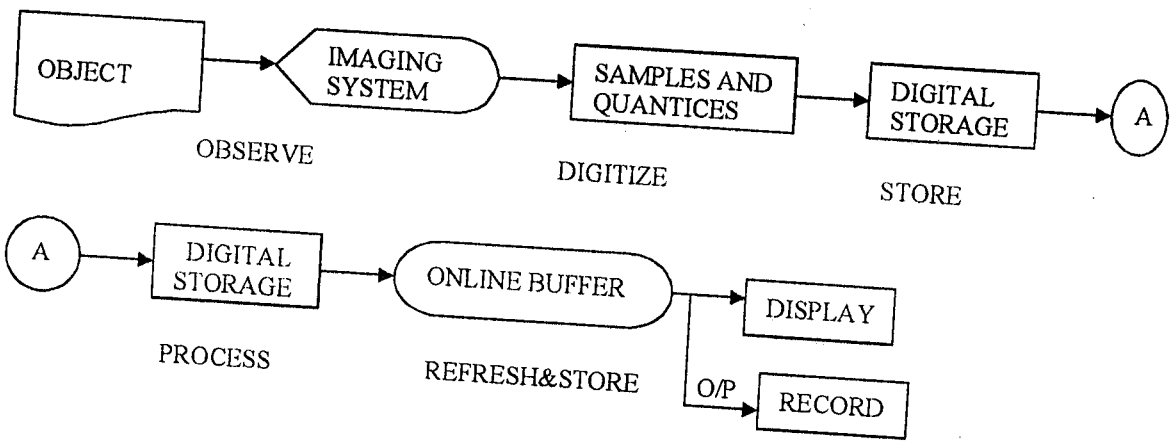
The function or performance characteristics conform to the specification and are accepted.

A deviation from specification is uncovered and a deficiency list is created.

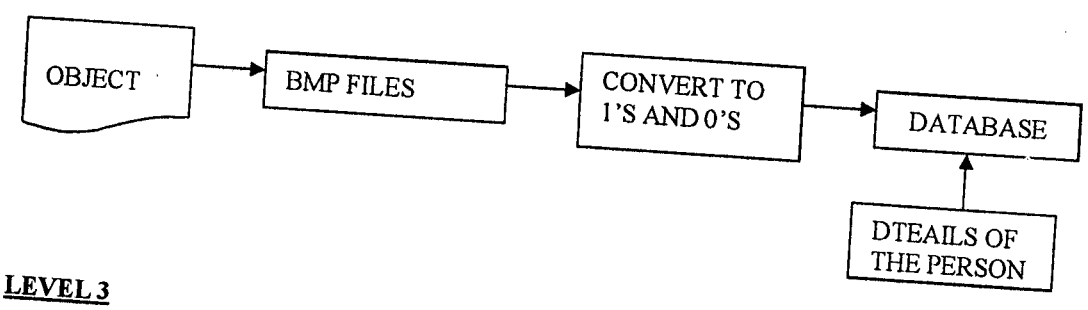
This project is validated under different test conditions. The requirements as per the specification are met. The performance is tested at full capacity of users, accessing, saving and modifying the user details.

OOAD

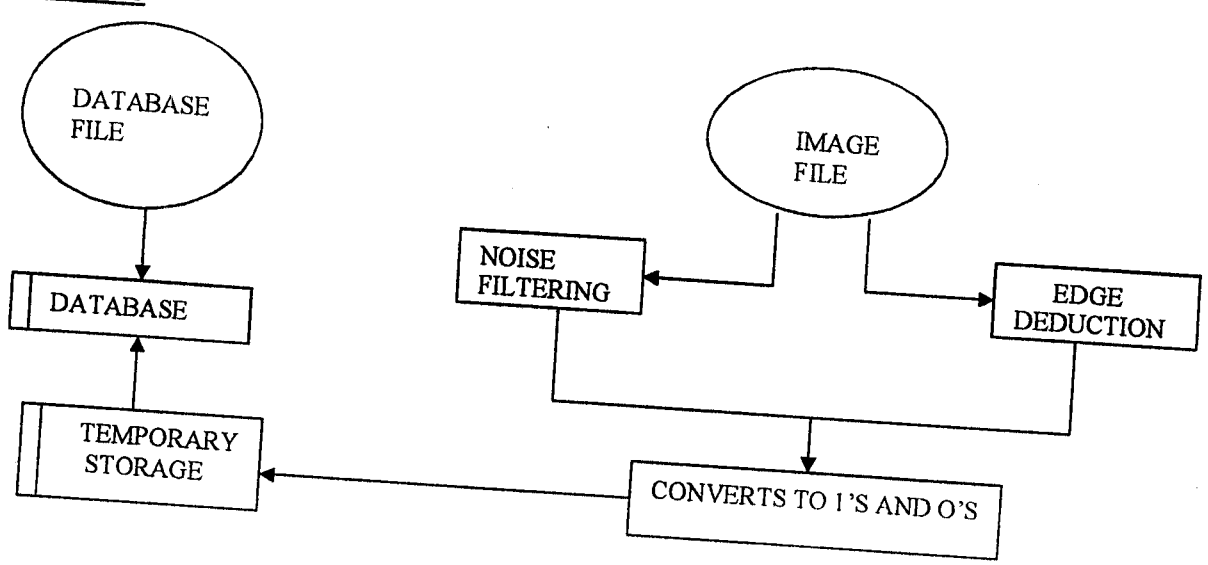
LEVEL 1



LEVEL 2



LEVEL 3



DESIGN CONSTRAINTS

3.3.1 SOFTWARE & HARDWARE REQUIREMENTS

HARDWARE REQUIREMENTS

Processor	: Pentium III
RAM	: 128 MB
HDD	: 20 GB
FDD	: 1.44" floppy drive
Monitor	: 17" Color monitor
Pointing Device	: Three-button Mouse
Keyboard	: 132 keys

SOFTWARE REQUIREMENTS

Platform	: Microsoft Windows 98/NT/2000
Language	: C Language
Database	: C File Systems
Network Architecture	: TCP/IP

PACKAGE SELECTED

C LANGUAGE

The C programming language was devised in the early 1970s as a system implementation language for the nascent Unix operating system. Derived from the type less language BCPL, it evolved a type structure; created on a tiny machine as a tool to improve a meager programming environment, it has become one of the dominant languages of today. C is much more flexible and freewheeling. This freedom gives C much more power that experienced users can employ.

CHARACTERISTICS OF C

Some of C's characteristics that define the language and also have lead to its popularity as a programming language.

- Small size
- Extensive use of function calls
- Loose typing -- unlike PASCAL
- Structured language
- Low level (Bit Wise) programming readily available
- Pointer implementation - extensive use of pointers for memory, array, structures and functions.

C has now become a widely used professional language for various reasons.

- It has high-level constructs.
- It can handle low-level activities.
- It produces efficient programs.
- It can be compiled on a variety of computers.

In recent years, there has been a major trend towards the use of C among serious programmers.

- ✓ C is flexible, high-level, structured programming language.
- ✓ C includes certain low-level features that are normally available Only in Assembly or Machine Language.
- ✓ C is largely machine-independent.

C is a general-purpose, structured programming language. Its instructions consists of terms that resembles algebraic expressions, augmented by certain English keywords such as if, else, for, do, while.

C compilers are commonly available for computers of all sizes and C interpreters are becoming increasingly common. The compilers are usually compact and they generate objects programs that are small and highly efficient when compared with programs compiled from other high-level languages. The interpreters are less efficient. Though they are easier to use when developing a new program.

Another important characteristics of c are that its program is highly portable. Most C programs can be processed on many different computers with little or no alteration.

NETWORKING

Networking is the sharing of information and services. Networking is possible when individuals of groups have information or abilities that they wish to share with others.

Computer networking technologies have developed because of the requirement of the following computing models:

- ✓ Centralized computing
- ✓ Distributed computing
- ✓ Collaborative computing

Computer networks are often classified by size, distance covered or structure. The following describes the same.

LAN, Wan, Man

Computer networks are often classified as one of the following two types

1. **Peer-peer**
2. **Server-centric.**

PROTOCOLS

Protocols are rules required to help entities, Communicate or understand Each other's protocol can be one rule or complete set of rules and standards that allow different devices to hold conversation. The protocol that has been used in this project is TCP/IP.

TCP and IP were developed by a Department of Defense (DOD) research project to connect a number different networks designed by different vendors into a network of networks (the "Internet"). It was initially successful because it delivered a few basic services that everyone needs (file transfer, electronic mail, remote logon) across a very large number of client and server systems. Several computers in a small department can use TCP/IP (along with other protocols) on a single LAN. The IP component provides routing from the department to the enterprise network, then to regional networks, and finally to the global Internet. On the battlefield a communications network will sustain damage, so the DOD designed TCP/IP to be robust and automatically recover from any node or phone line failure. This design allows the construction of very large networks with less central management. However, because of the automatic recovery, network problems can go undiagnosed and uncorrected for long periods of time.

TRANSMISSION CONTROL PROTOCOL

The TCP provides reliable transmission of data in an IP environment. TCP corresponds to the transport layer (Layer 4) of the OSI reference model. Among the services TCP provides are stream data transfer, reliability, efficient flow control, full-duplex operation, and multiplexing.

With stream data transfer, TCP delivers an unstructured stream of bytes identified by sequence numbers. This service benefits applications because they do not have to chop data into blocks before handing it off to TCP. Instead, TCP groups bytes into segments and passes them to IP for delivery.

TCP offers reliability by providing connection-oriented, end-to-end reliable packet delivery through an Internet work. It does this by sequencing bytes with a forwarding acknowledgment number that indicates to the destination the next byte the source expects to receive. Bytes not acknowledged within a specified time period are retransmitted. The reliability mechanism of TCP allows devices to deal with lost, delayed, duplicate, or misread packets. A time-out mechanism allows devices to detect lost packets and request retransmission.

TCP offers efficient flow control, which means that, when sending acknowledgments back to the source, the receiving TCP process indicates the highest sequence number it can receive without overflowing its internal buffers.

Full-duplex operation means that TCP processes can both send and receive at the same time.

Finally, TCP's multiplexing means that numerous simultaneous upper-layer conversations can be multiplexed over a single connection.

TCP CONNECTION ESTABLISHMENT

To use reliable transport services, TCP hosts must establish a connection-oriented session with one another. Using a "three-way handshake" mechanism the connection is established.

A three-way handshake synchronizes both ends of a connection by allowing both sides to agree upon initial sequence numbers. This mechanism also guarantees that both sides are ready to transmit data and know that the other side is ready to transmit as well. This is necessary so that packets are not transmitted or retransmitted during session establishment or after session termination. Each host randomly chooses a sequence number used to track bytes within the stream it is sending and receiving. Then, the three-way handshake proceeds in the following manner:

The first host (Host A) initiates a connection by sending a packet with the initial sequence number (X) and SYN bit set to indicate a connection request. The second host (Host B) receives the SYN, records the sequence number X, and replies by acknowledging the SYN (with an ACK = X + 1). Host B includes its own initial sequence number (SEQ = Y). An ACK = 20 means the host has received bytes 0 through 19 and expects byte 20 next. This technique is called *forward acknowledgment*. Host A then acknowledges all bytes Host B sent with a forward acknowledgment indicating the next byte Host A expects to receive (ACK = Y + 1). Data transfer then can begin.

TCP FIELD DESCRIPTIONS

- *Source Port* and *Destination Port*—Identifies points at which upper-layer source and destination processes receive TCP services.
- *Sequence Number*—Usually specifies the number assigned to the first byte of data in the current message. In the connection-establishment phase, this field also can be used to identify an initial sequence number to be used in an upcoming transmission.
- *Acknowledgment Number*—Contains the sequence number of the next byte of data the sender of the packet expects to receive.
- *Data Offset*—Indicates the number of 32-bit words in the TCP header.
- *Reserved*—Remains reserved for future use.
- *Flags*—Carries a variety of control information, including the SYN and ACK bits used for connection establishment, and the FIN bit used for connection termination.
- *Window*—Specifies the size of the sender's receive window (that is, the buffer space available for incoming data).
- *Checksum*—Indicates whether the header was damaged in transit.
- *Urgent Pointer*—Points to the first urgent data byte in the packet.
- *Options*—Specifies various TCP options.
- *Data*—Contains upper-layer information.

THE LAYERS OF TCP/IP PROTOCOL SUITE

The first, the link layer, is responsible for communicating with the actual network hardware (e.g., the Ethernet card). Data it receives off the network wire it hands to the network layer; data it receives from the network layer it puts on the network wire. This is where device drivers for different interfaces reside.

The second, the network layer, is responsible for figuring out how to get data to its destination. Making no guarantee about whether data will reach its destination, it just decides where the data should be sent.

The third, the transport layer, provides data flows for the application layer. It is at the transport layer where guarantees of reliability may be made.

The fourth, the application layer, is where users typically interact with the network. This is where telnet, ftp, email, IRC, etc. reside.

Packets are the basic unit of transmission on the Internet. They contain both data and header information. Simply put, headers generally consist of some combination of checksums, protocol identifiers, destination and source addresses, and state information. Each layer may add its own header information, so it can interpret the data the lower layer is handing it. This is the product of a packet, which has gone from that application layer all the way to the link layer. Each layer takes the previous layer's packet, viewing almost all of it as data, and puts its own header on it.

INTERNET PROTOCOL

The Internet Protocol (IP) is a network-layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be routed. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols. IP has two primary responsibilities: providing connectionless, best-effort delivery of data grams through an internet work; and providing fragmentation and reassembly of data grams to support data links with different maximum-transmission unit (MTU) sizes.

IP - is responsible for moving packet of data from node to node. IP forwards each packet based on a four-byte destination address (the IP number). The Internet authorities assign ranges of numbers to different organizations. The organizations assign groups of their numbers to departments. IP operates on gateway machines that move data from department to organization to region and then around the world.

TCP sends each of these data grams to IP. Of course it has to tell IP the Internet address of the computer at the other end. IP doesn't care about what is in the data gram, or even in the TCP header. IP's job is simply to find a route for the data gram and get it to the other end. In order to allow gateways or other intermediate systems to forward the data gram, it adds its own header. The main things in this header are the source and destination Internet address (32-bit addresses, like 128.6.4.194), the protocol number, and another checksum. The source Internet address is simply the address of your machine. The destination Internet address is the address of the other

machine. The protocol number tells IP at the other end to send the data gram to TCP.

Finally, the checksum allows IP at the other end to verify that the header wasn't damaged in transit. TCP and IP have separate checksums. IP needs to be able to verify that the header didn't get damaged in transit, or it could send a message to the wrong place.

IP PACKET FORMAT

IP packet format consists of fourteen fields

- *Version*—Indicates the version of IP currently used.
- *IP Header Length* (IHL)—Indicates the data gram header length in 32-bit words.
- *Type-of-Service*—Specifies how an upper-layer protocol would like a current data gram to be handled, and assigns data grams various levels of importance.
- *Total Length*—Specifies the length, in bytes, of the entire IP packet, including the data and header.
- *Identification*—Contains an integer that identifies the current data gram. This field is used to help piece together data gram fragments.
- *Flags*—Consists of a 3-bit field of which the two low-order (least-significant) bits control fragmentation. The low-order bit specifies whether the packet can be fragmented. The middle bit specifies whether the packet is the last fragment in a series of fragmented packets. The third or high-order bit is not used.

- *Fragment Offset*—Indicates the position of the fragment's data relative to the beginning of the data in the original data gram, which allows the destination IP process to properly reconstruct the original data gram.

- *Time-to-Live*—Maintains a counter that gradually decrements down to zero, at which point the data gram is discarded. This keeps packets from looping endlessly.

- *Protocol*—Indicates which upper-layer protocol receives incoming packets after IP processing is complete.

- *Header Checksum*—Helps ensure IP header integrity.

- *Source Address*—Specifies the sending node.

- *Destination Address*—Specifies the receiving node.

- *Options*—Allows IP to support various options, such as security.

- *Data*—Contains upper-layer information.

IP ADDRESSING

IP addressing is based on the concept of hosts and networks. A host is essentially anything on the network that is capable of receiving and transmitting IP packets on the network, such as a workstation or a router.

The hosts are connected together by one or more networks. The IP address of any host consists of its network address plus its own host address on the network. IP addressing, unlike, say, IPX addressing, uses one address containing both network and host address. How much of the address is used for the network portion and how much for the host portion varies from network to network.

An IP address is 32 bits wide, and as discussed, it is composed of two parts: the network number, and the host number [1, 2, 3]. By convention, it is expressed as four decimal numbers separated by periods, such as "200.1.2.3" representing the decimal value of each of the four bytes. Valid addresses thus range from 0.0.0.0 to 255.255.255.255, a total of about 4.3 billion addresses. The first few bits of the address indicate the Class that the address belongs to.

IP addresses are hierarchical for routing purposes and are subdivided into two sub fields. The Network Identifier (NET_ID) sub field identifies the TCP/IP sub network connected to the Internet. The NET_ID is used for high-level routing between networks, much the same way as the country code, city code, or area code is used in the telephone network. The Host Identifier (HOST_ID) sub field indicates the specific host within a sub network. To accommodate different size networks, IP defines several *address classes*. Classes A, B, and C are used for host addressing and the only difference between the classes is the length of the NET_ID sub field.

A Class A address has an 8-bit NET_ID and 24-bit HOST_ID. Class A addresses are intended for very large networks and can address up to 16,777,216 (2^{24}) hosts per network. The first digit of a Class A addresses will be a number between 1 and 126. Only about 90 or so Class A addresses have been assigned.

A Class B address has a 16-bit NET_ID and 16-bit HOST_ID. Class B addresses are intended for moderate sized networks and can address up to 65,536 (2^{16}) hosts per network. The first digit of a Class B address will be a number between 128 and 191. The Class B address space has long been threatened with being used up and it is has been very difficult to get a new Class B address for some time.

A Class C address has a 24-bit NET_ID and 8-bit HOST_ID. These addresses are intended for small networks and can address only up to

254 (2^8-2) hosts per network. The first digit of a Class C address will be a number between 192 and 223. Most addresses assigned to networks today are Class C.

The remaining two address classes are used for special functions only and are not commonly assigned to individual hosts. Class D addresses may begin with a value between 224 and 239, and are used for IP multicasting (i.e., sending a single data gram to multiple hosts). The class E addresses begin with a value between 240 and 255, and are reserved for experimental use.

PORTS

It is the memory address to which information is transferred. It provides the communication for devices to be attached. A port identifier in TCP/UDP messages refers to higher-layer applications. The port identifier and IP address together form a *socket*, and the end-to-end communication between two hosts is uniquely identified on the Internet by the four-tuple (source port, source address, destination port, destination address).

A 16-bit number specifies the port number. Port numbers in the range 0-1023 are called *Well Known Ports*. These port numbers are assigned to the server side of an application and, on most systems, can only be used by processes with a high level of privilege (such as root or administrator). Port numbers in the range 1024-49151 are called *Registered Ports*, and these are numbers that have been publicly defined as a convenience for the Internet community to avoid vendor conflicts. Server or client applications can use the port numbers in this range. The remaining port numbers, in the range 49152-65535, are called *Dynamic and/or Private Ports* and can be used freely by any client or server. There are two types of ports namely serial and parallel. Normally a machine is equipped with a single parallel port and two serial ports.

The serial or communications port (COM port) located on the back of our PC is one of computer's gateways to the outside world. The COM port lets our computer "talk," or interface, with peripherals such as a mouse or modem. The PC can recognize up to four serial ports while the typical computer contains only two, designated as COM1 and COM2. The serial port is sometimes called the RS-232 because it uses the RS-232C standard of the Electronics Industry Association (EIA).

Serial port information resides at specific memory addresses and **interrupt requests (IRQs.)** An IRQ is a request-for-attention signal that can be passed by either hardware or software to a computer's microprocessor. Only one device can reside at a single interrupt and address, and trying to put two devices at the same address is a common problem when we're adding new equipment or interface cards. When we do this, one serial device won't work.

SOCKETS

A socket is a communication mechanism. A socket is normally identified by a small integer, which may be called the socket descriptor. It is the fundamental Internet network-programming interface. The socket mechanism was first introduced in the 4.2 BSD UNIX systems in 1983 in conjunction with the TCP/IP protocols that first appeared in the 4.1 BSD UNIX systems in late 1981.

Formally a **socket** is defined by a group of four numbers, these are

- The remote host identification number or address
- The remote host port number
- The local host identification number or address
- The local host port number

Users of Internet applications are normally aware of all except the local port number, this is allocated when connection is established and is almost entirely arbitrary unlike the well-known port numbers associated with popular applications.

To the application programmer the socket mechanism is accessed via a number of functions. These are.

Socket ()	Create a socket
Bind ()	Associate a socket with a network address
Connect ()	Connect a socket to a remote network address
Listen ()	Wait for incoming connection attempts
Accept ()	Accept incoming connection attempts

In addition the functions setsockopt(), getsockopt(), fcntl() and ioctl() may be used to manipulate the properties of a socket, the function select() may be used to identify sockets with particular communication statuses. The function close () may be used to close a socket liaison.

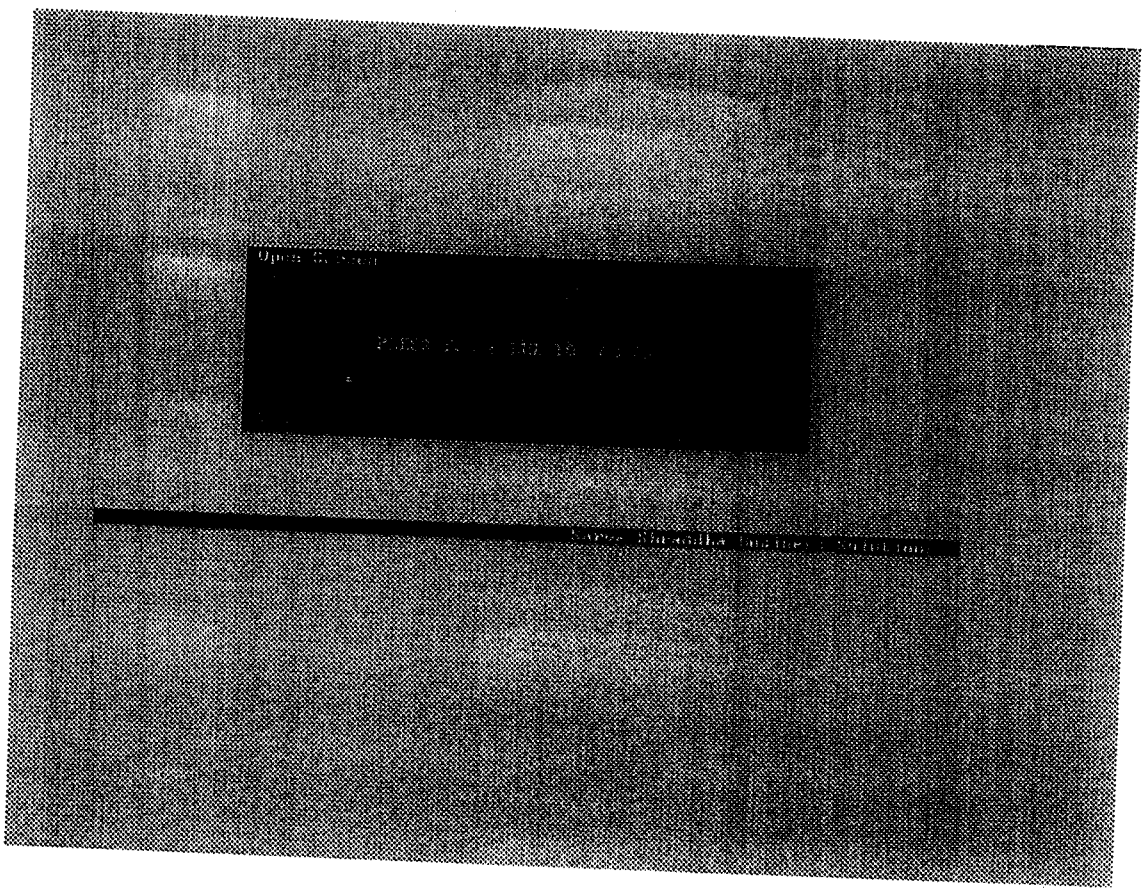
Data can be written to a socket using any of the functions write (), writev(), send(), sendto() and sendmsg(). Data can be read from a socket using any of the functions read (), readv(), recv(), recvfrom() and recvmsg()

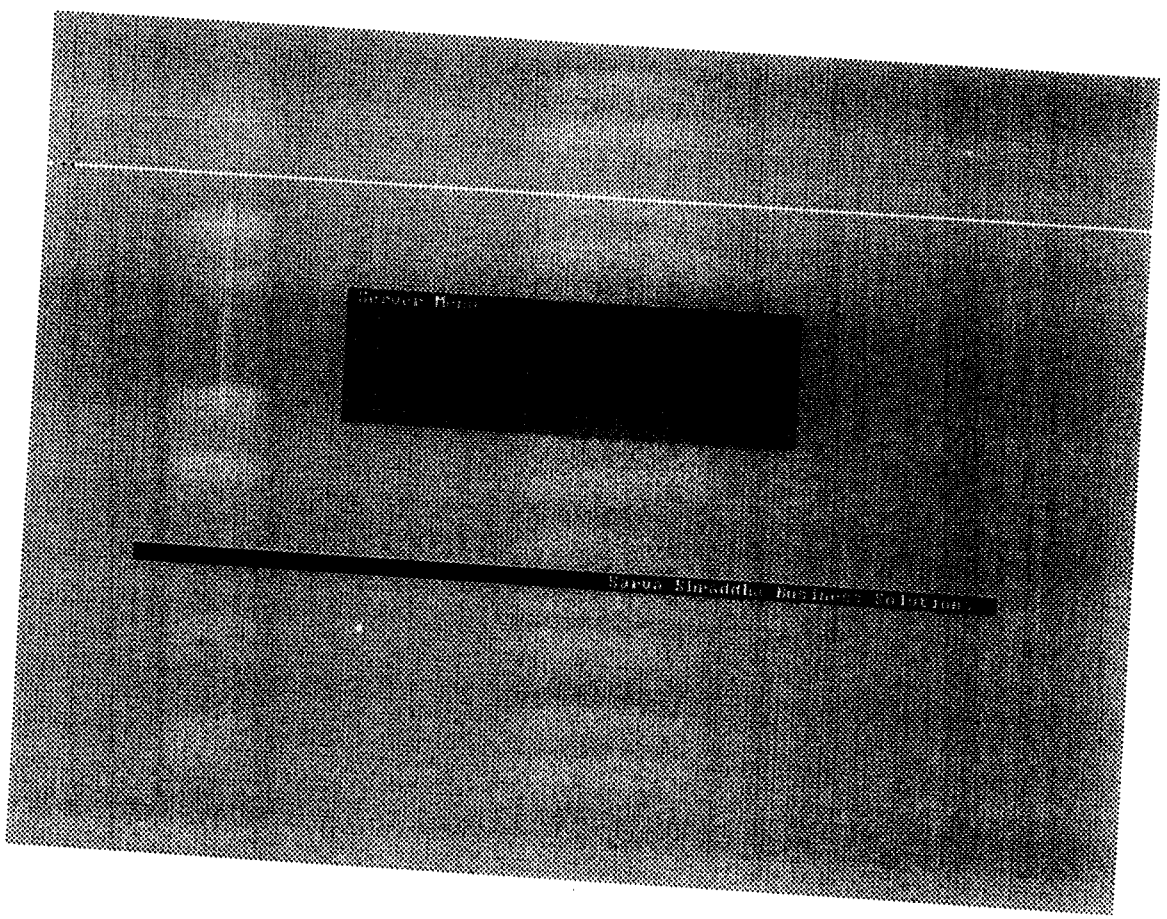
3.3.2 EXTERNAL INTERFACE REQUIREMENTS

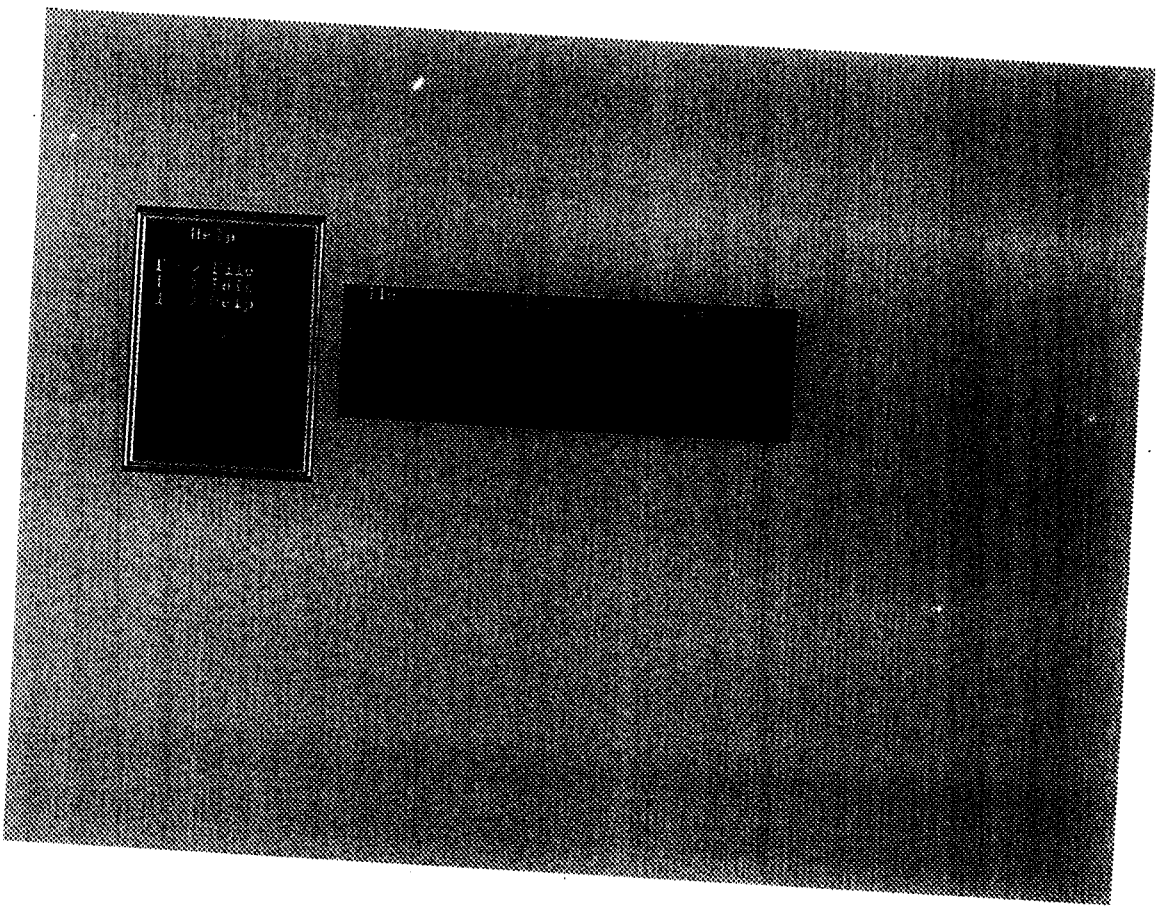
The Fingerprint GIF is a source from external interfaces like scanner for entering into the system. Since the Sensor is not been used it is sensed from the external interfaces like scanner and stored in the centralized server for safety use. This mechanism is similar to the one used in bank sectors where the signatures are sourced from account holders, scanned and stored in the server.

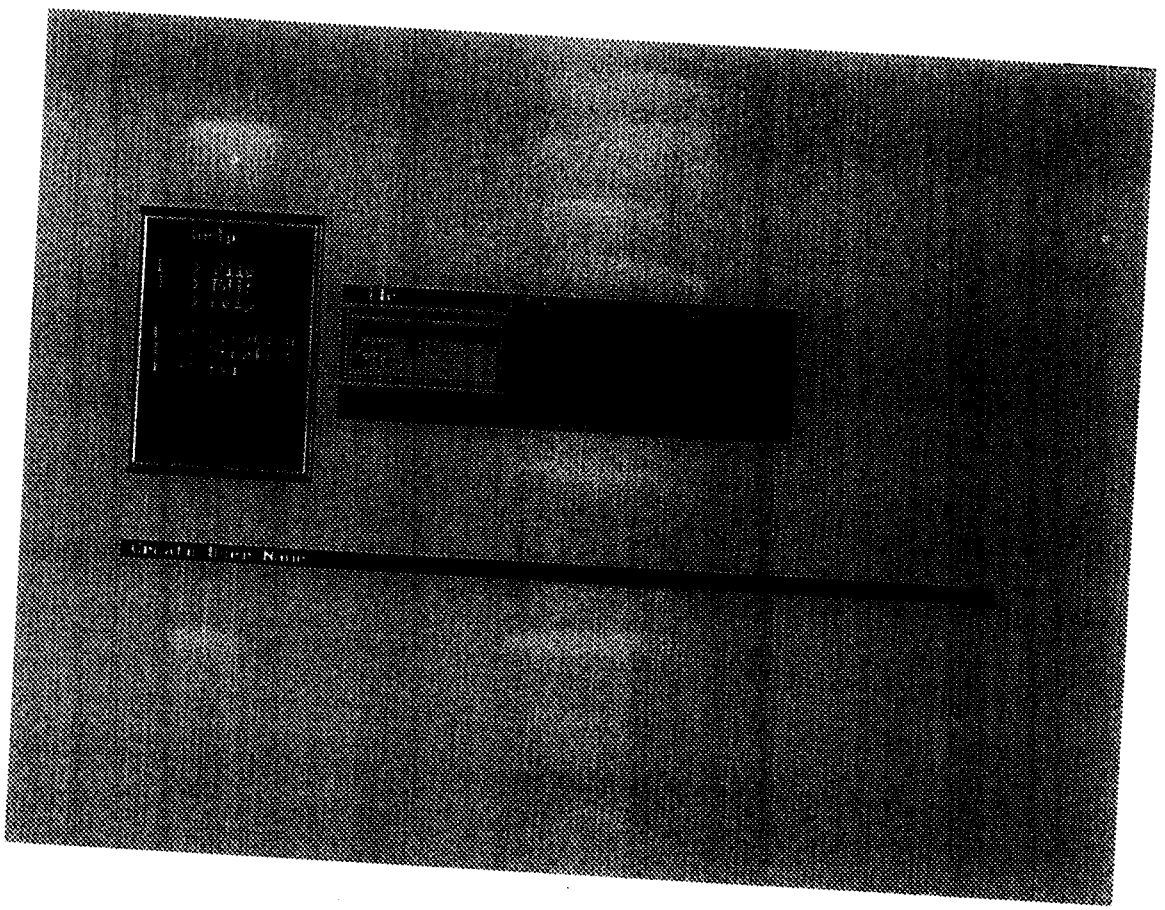
The Fingerprint gifs are stored in the form of files and are maintained in a unique algorithm so that others will not know the usage of the gifs. Since sensor is not been used we have to scan the fingerprint and store in the file for entry into the node with secured manner.

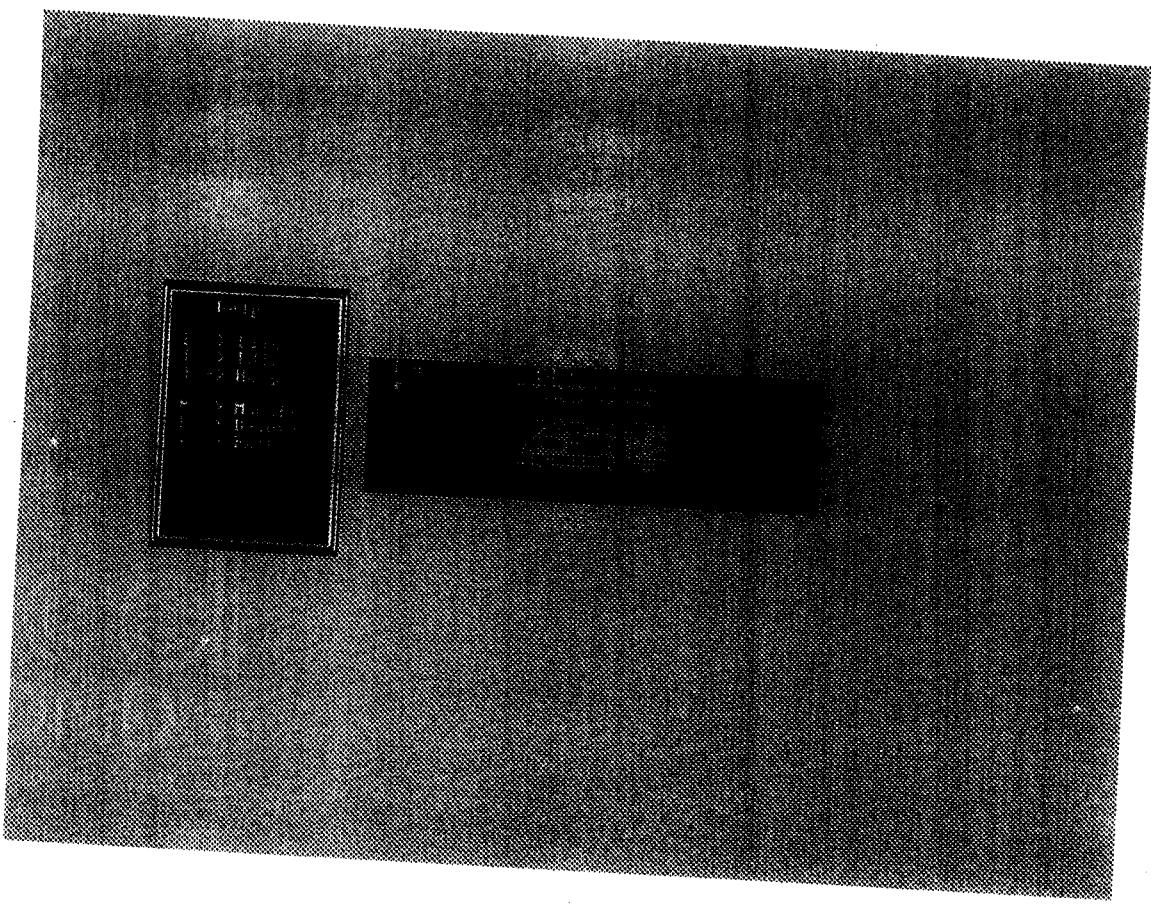
SCREEN FORMATS

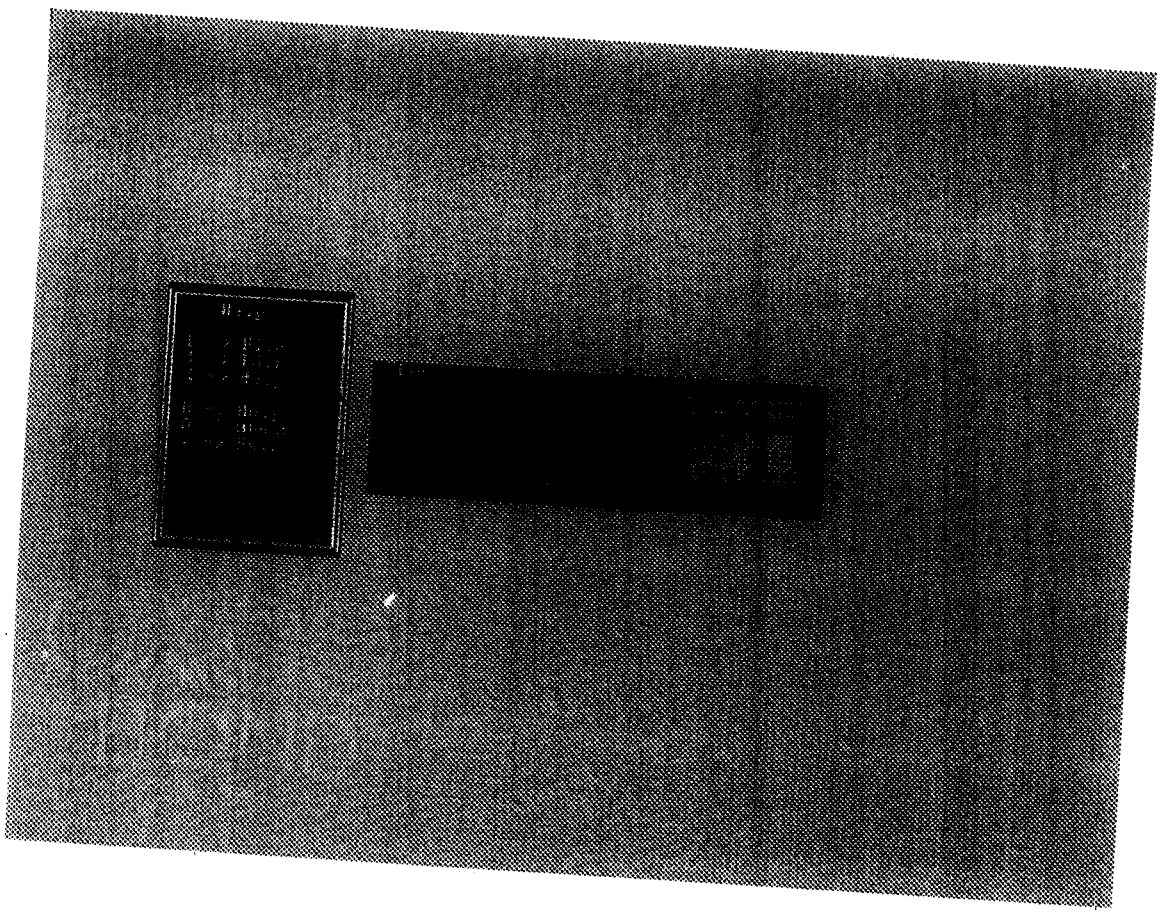


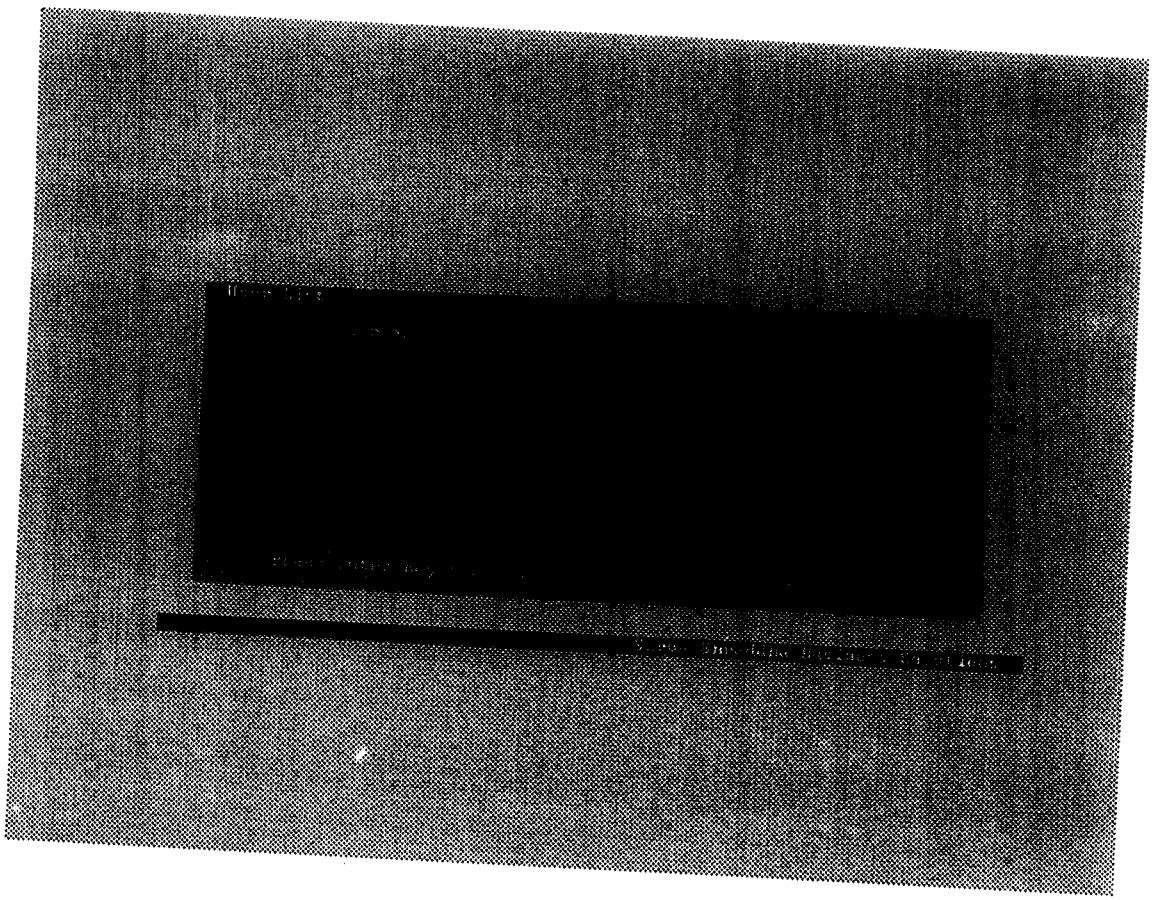


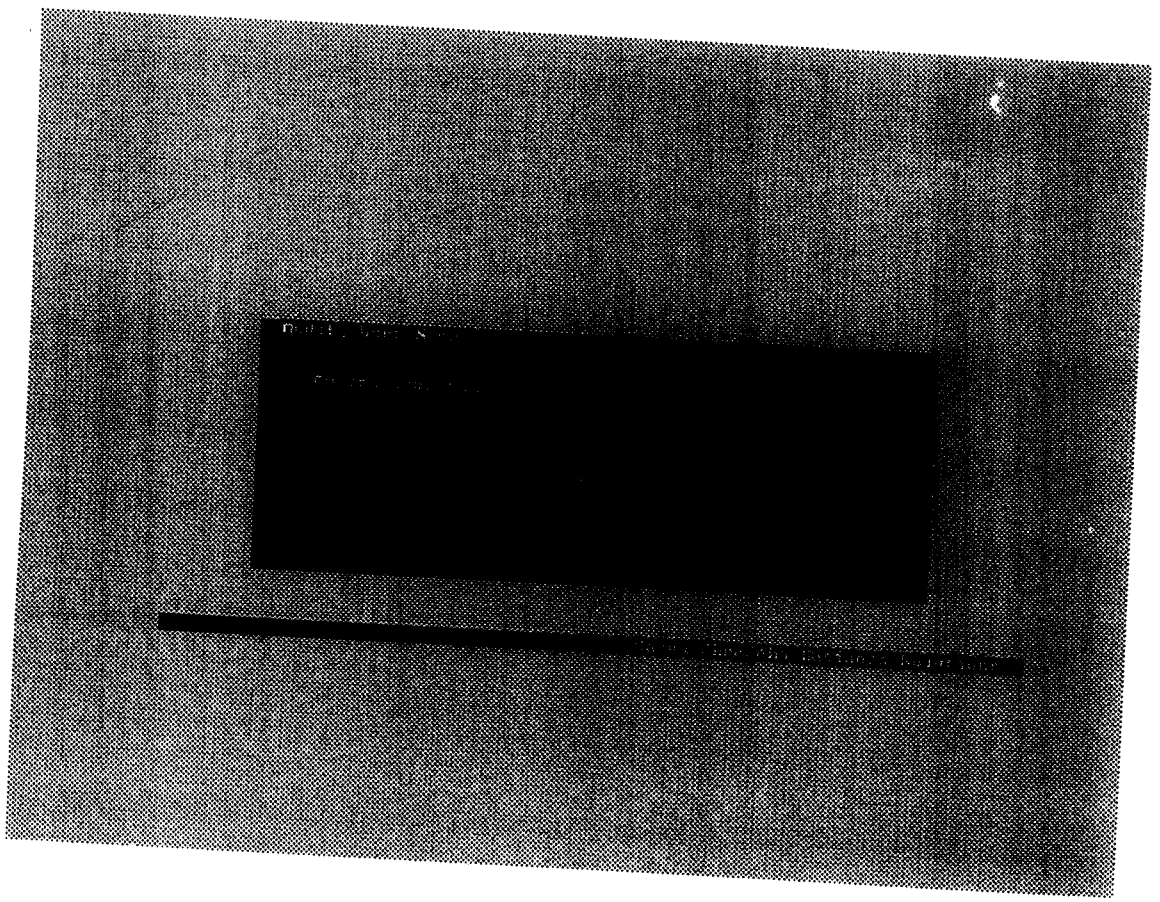


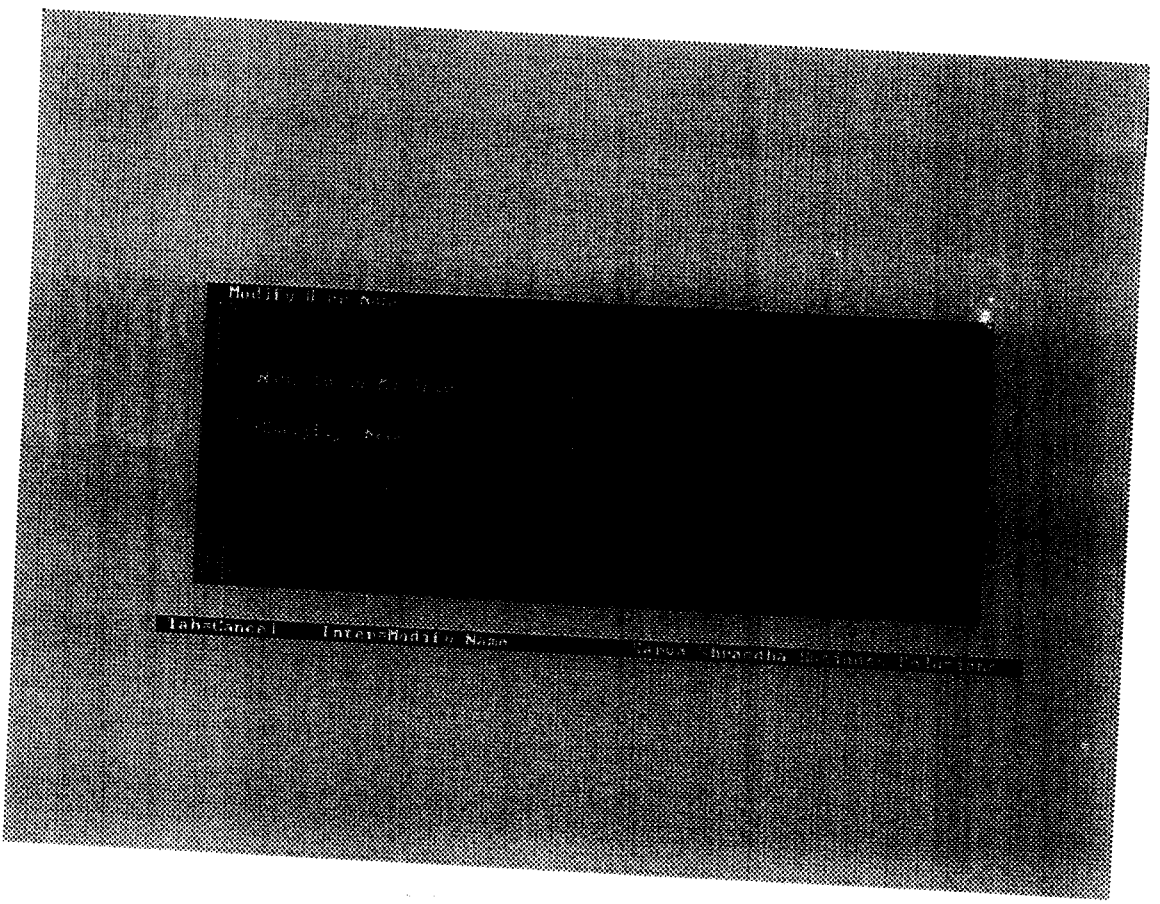


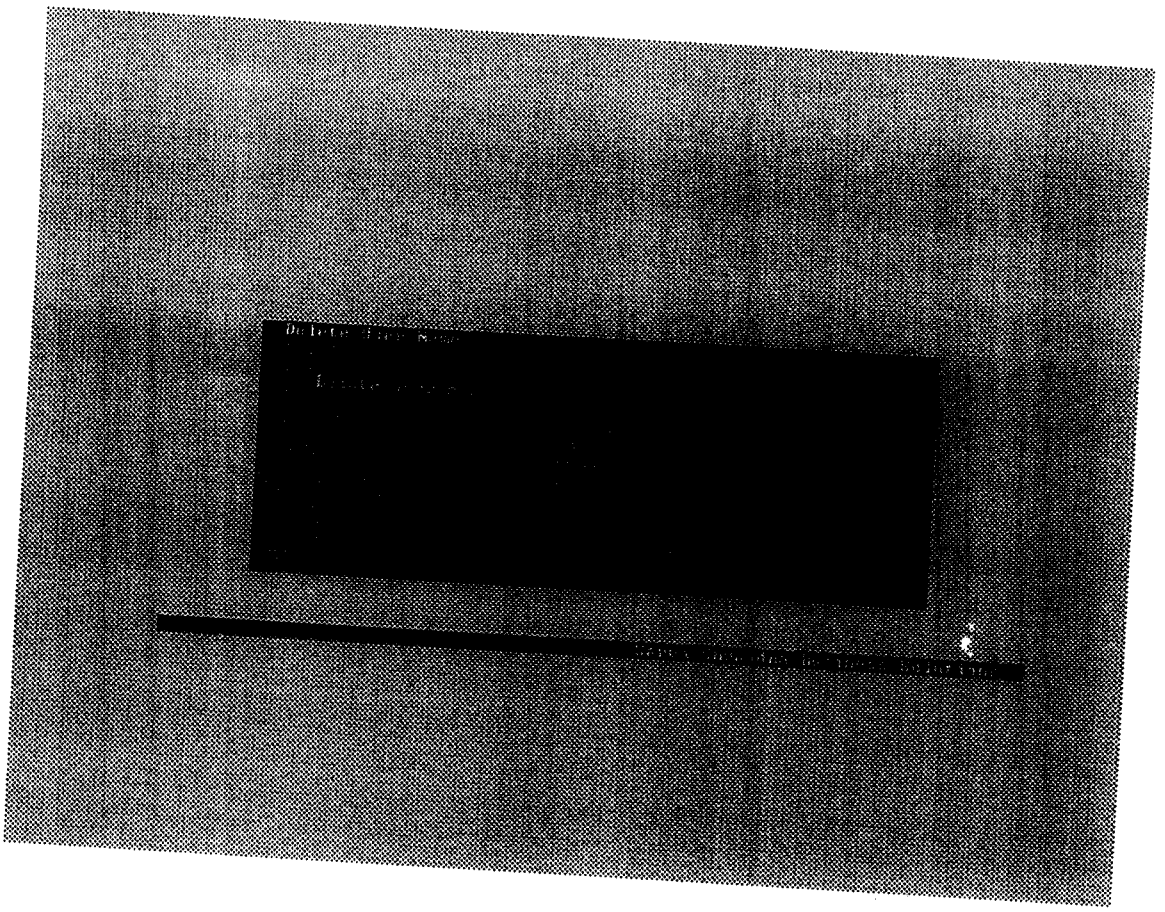


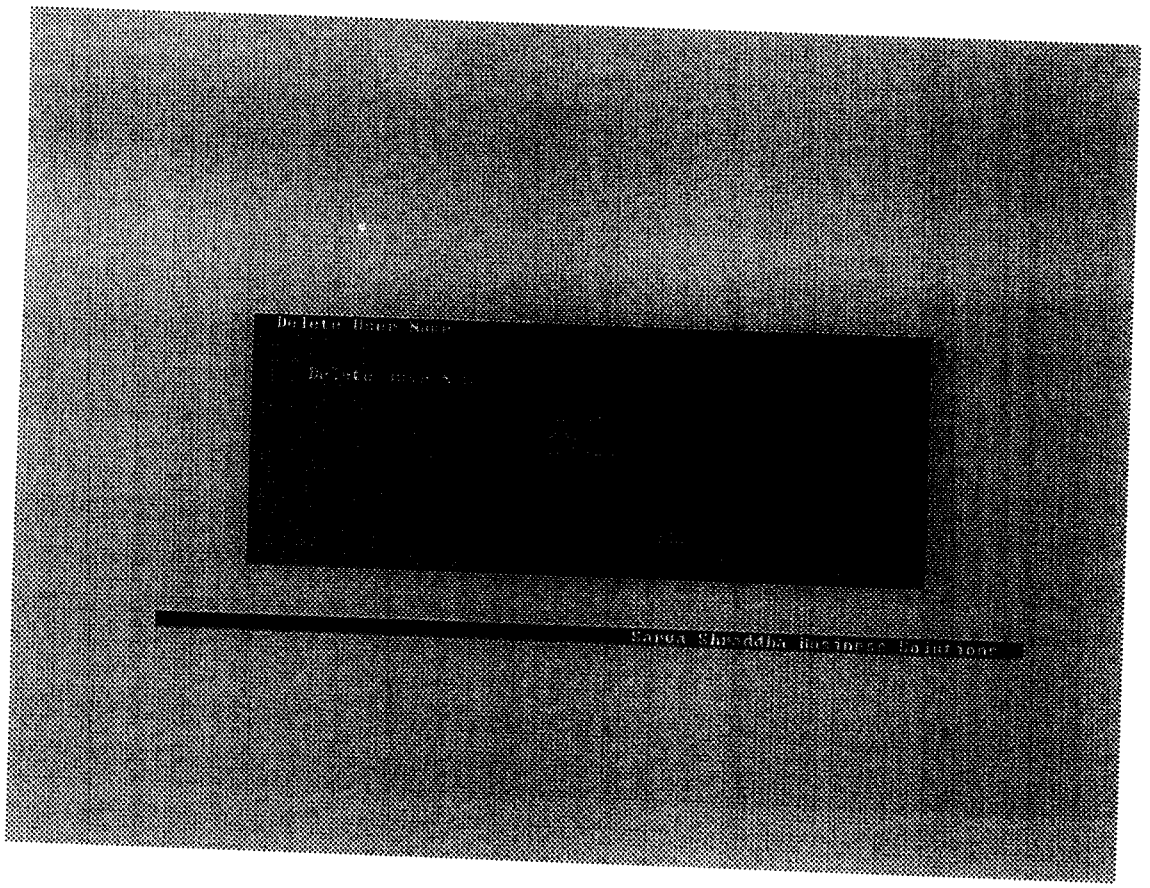


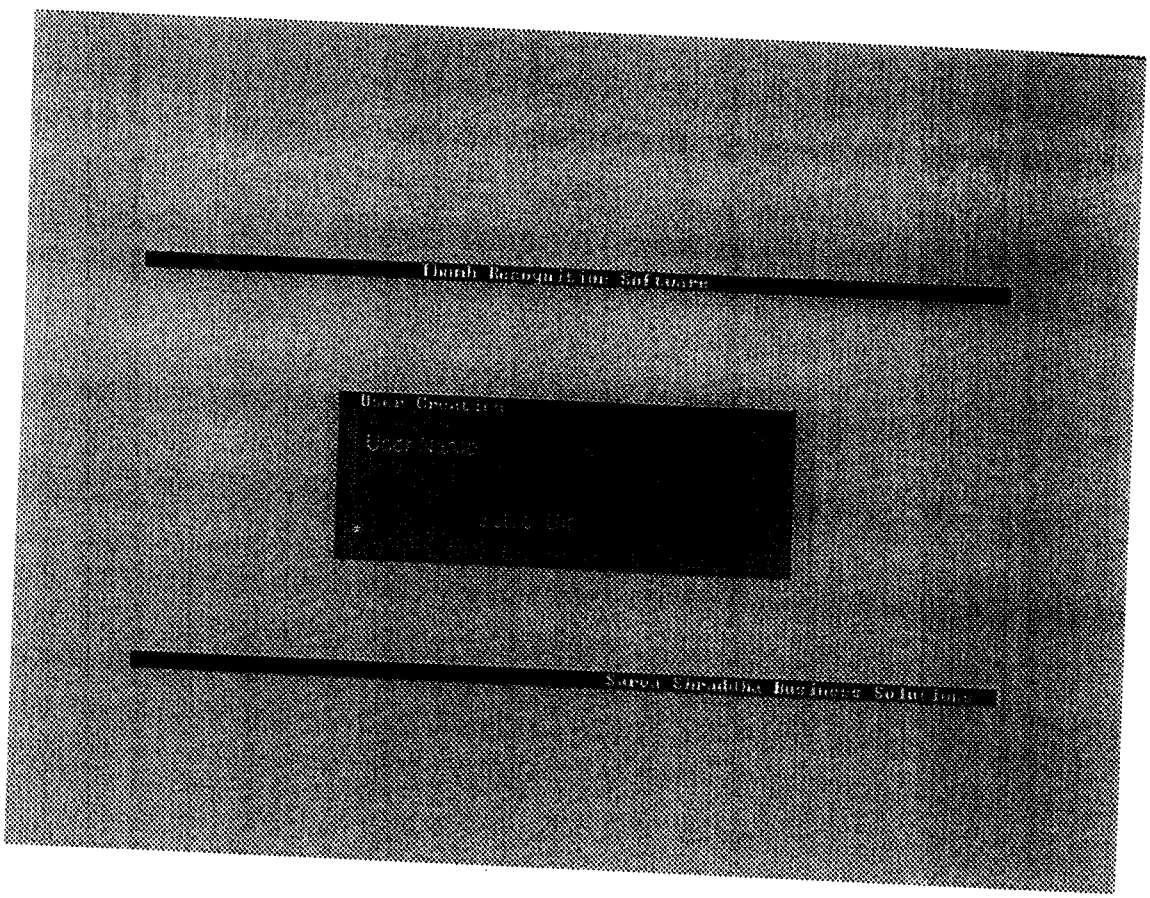


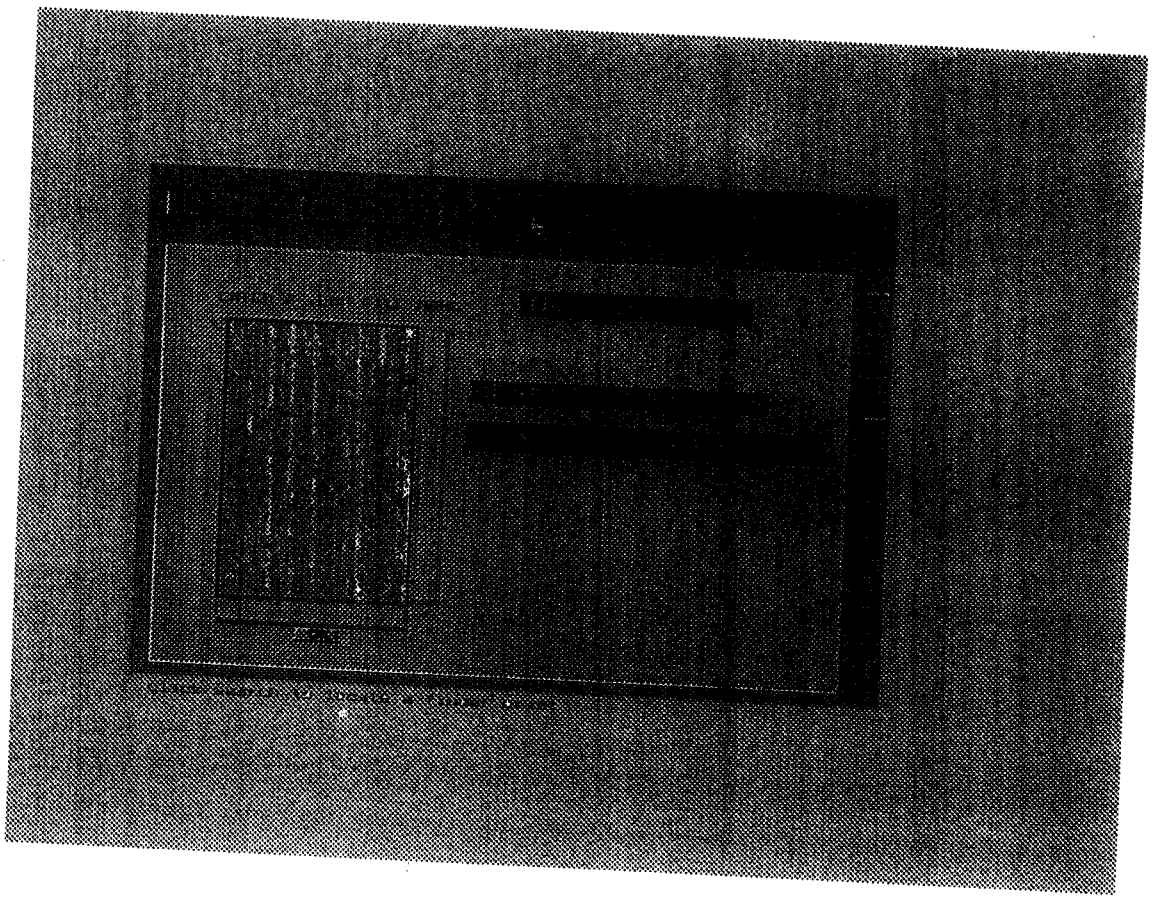


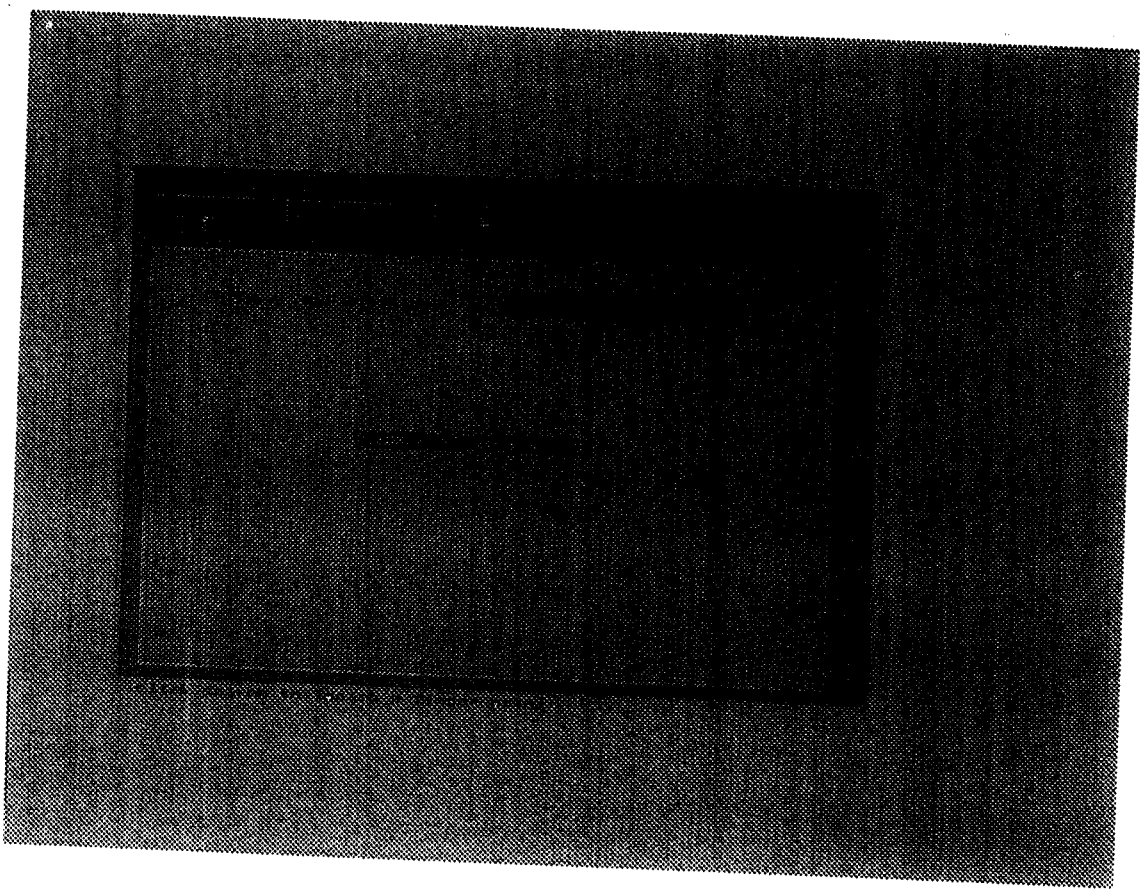


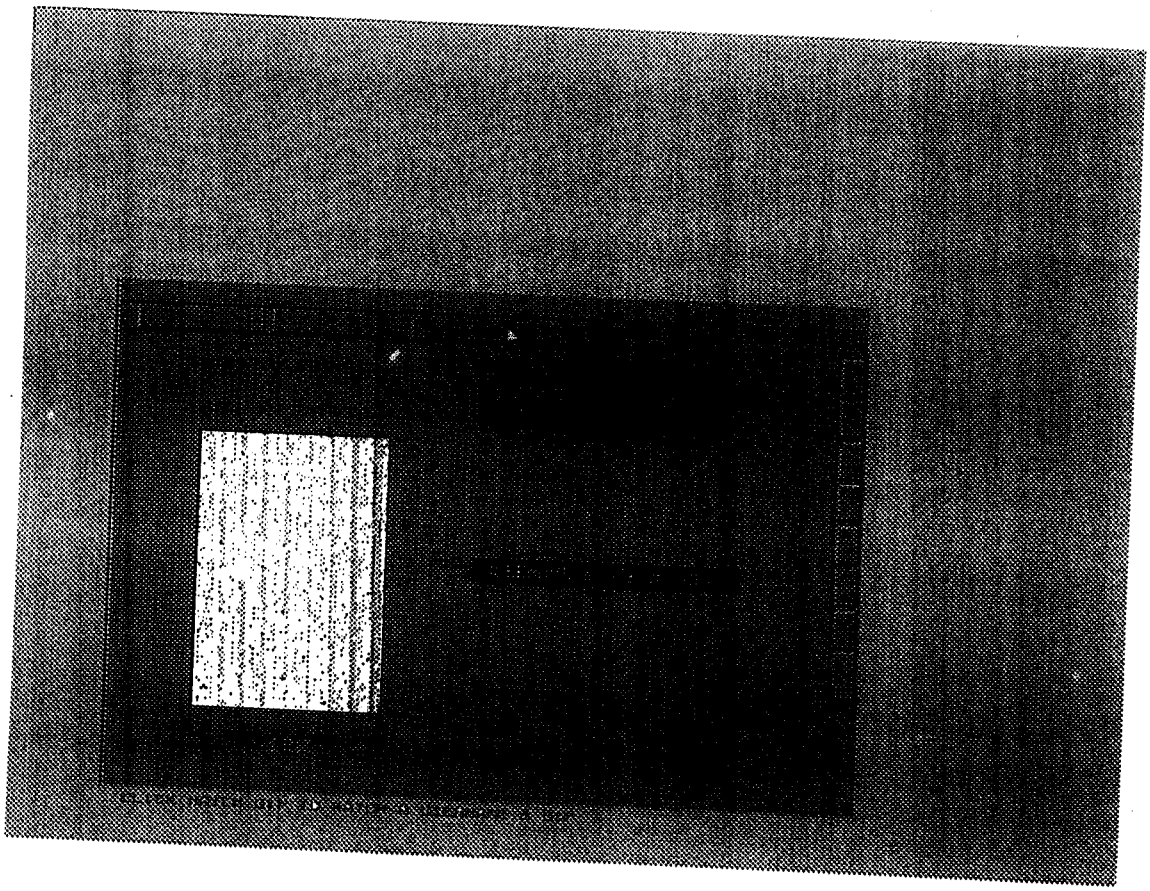












TESTING

3.6 TESTING

The Software testing process commences once the program is created and a working prototype with basic functionalities is available. Software testing is essential for correcting errors. A Project is set to be incomplete without proper testing.

TESTING OBJECTIVES

The testing objectives are summarized in the following three steps:
Testing is the process of executing a program with the intent of finding an error.

1. A good test case is one that has high probability of finding an as yet undiscovered error.
2. A successful test is one that uncovers an as-yet-undiscovered error.

For this Finger Print Recognition System needs four types of testing. They are

- Unit Testing
- Validation Testing
- Integration Testing
- Output Testing

UNIT TESTING

Unit testing comprises the set of tests performed by an individual programmer prior to the integration of the unit into the large system. A program unit is usually small enough that the programmer who developed the unit can test it. Then the unit is integrated into the large part of the

system. Unit testing is always white-box oriented and the step can be conducted in parallel for modules.

INTEGRATION TESTING

Bottom-up integration is the traditional strategy to integrate the components of the software system into the functional unit. Bottom-up integration consists of unit testing of the entire system.

Modules are tested in isolation from one another in an artificial environment, known as a "test harness", which consist of the driver programs and data necessary to exercise the modules.

Moreover integration testing addresses the issues associated with the dual problem of verification and program construction. After the application has been integrated a set of higher-order tests were conducted.

OUTPUT TESTING

The outputs are tested thoroughly by giving sample data, for which results are known. The outputs from the system are matched with that of the known values and the results are found to be accurate. Test data of about 50 Username are validated on the login form. The results were found to be accurate.

Testing is the process of executing test cases with the intention of exposing the errors.

TESTING PRINCIPLES

- All tests should be traceable to customer requirements.
- Tests should be planned long before testing begins, that is, the test planning can begin as soon as the requirement model is complete.
- Testing should begin "in the small" and progress towards testing " in the large". The focus of testing will shift progressively from programs, to individual modules and finally to the entire project.
- Exhaustive testing is not possible.

VALIDATION TESTING:

Software testing and validation is achieved through a series of black box tests that demonstrate conformity with the requirement. A test plan outlines the classes to test to be conducted and a test procedure defines specific test cases that will be used to demonstrate conformity with the requirements. Both, the planned the procedures are designed to ensure that all functional requirements are archived, documentation is correct and other requirements are met. After each validation test case has been conducted, one of the two possible conditions exists.

They are:

The function or performance characteristics conform to the specification and are accepted.

A deviation from specification is uncovered and a deficiency list is created.

This project is validated under different test conditions. The requirements as per the specification are met.

SYSTEM IMPLEMENTATION

3.7 SYSTEM IMPLEMENTATION

IMPLEMENTATION

Testing is an important phase in development in software development and application development. Testing will lead the error free application to the client.

SYSTEM IMPLEMENTATION

Implementation is the stage where the theoretical design is converted into working system. It consist of

- Testing and Debugging
- Error Correction
- Training the User
- Change over

Implementation includes equipment's installation and user training. For the system to begin operation, a sufficient number of users have been trained to the system. Several hours were scheduled for a number of users so that they were able to fully understand the new system and had an opportunity to familiarize themselves with the various input screens and generation of output.

The change over is another important aspect of the implementation process and had to be handled carefully. Data from the previous system, static contend is ported to the new system and the result produced is compared with that of the previous system. The new system is found to satisfy the user needs.

FUTURE ENHANCEMENTS

4.FUTURE ENHANCEMENTS

We here by conclude that we have completed our project "Fingerprint Recognition System" at SSBIL,coimbatore to the fulfillment of their requirements

We are proud that our project has been successfully implemented in the company. Using the sensor for direct comparison of the finger print impression rather than taking the scanned fingerprint GIF of the user for logging into the system can further enhance it

BIBLIOGRAPHY

5 REFERNCES

1. **Stevens**,W.R. TCP/IP Illustrated,Volume1.Wesley, Reading, Massachusetts, 1994.

2 Effective TCP/IP Programming - 44 Tips to Improve Your Network Programs

By **Jon C. Snader**

3. TCP/IP Explained

By **Philip Miller**, Published by Digital Press

4. Troubleshooting TCP/IP - Analyzing the Protocols of the Internet

By **Mark A. Miller.**

5. Using Turbo C

By **Herbert Schildt.**

6. Let us C

By **Yashvanth Kanethkar**