KUMARAGURU
COLLEGE OF TECHNOLOGY
Department of Computer Science and Engineering

ISO 9001:2000
Certified

TRANSCRYPTION & DIGITAL WATERMARKING

PROJECT WORK DONE AT
PELLUCID SYSTEMS
CHENNAI

PROJECT REPORT

SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE AWARD OF THE DEGREE OF
M.Sc APPLIED SCIENCE (SOFTWARE ENGINEERING)
OF BHARATHIAR UNIVERSITY, COIMBATORE.

SUBMITTED BY

K.VEERAKUMAR
REG NO: 0137S0058

Under the guidance of

INTERNAL GUIDE	EXTERNAL GUIDE
Mr. M. Manikantan, M.C.A., Dept. of Computer Science & Engineering, Kumaraguru College of Technology, Coimbatore.	Mr. Shankar Raman, M.C.A., Senior Software Engineer, Pellucid Systems, Chennai.

CERTIFICATE

KUMARAGURU
COLLEGE OF TECHNOLOGY
Department of Computer Science and Engineering

ISO 9001:2000 Certified

(Affiliated to Bharathiyar University)
Coimbatore - 641006
(JUNE-2004 TO OCTOBER -2004)

CERTIFICATE

This is to certify that the project entitled

"TRANSCRYPTION & DIGITAL WATERMARKING"
Done by

K.VEERAKUMAR
REG NO: 0137S0058

Submitted in partial fulfillment of the requirements for the award of the degree of M. Sc (Applied Science) Software Engineering of Bharathiyar University.

Professor and HOD **Internal Guide**

Submitted to University examination held on 30.09.04

Internal Examiner **External**

Examiner

Pellucid Systems
Technologies Refined

2004

TO WHOMSOEVER IT MAY CONCERN

This is to certify that Mr. VEERAKUMAR.K (RegNo.0137S0058) undergoing 4th year
. (Software Engineering) in Kumaraguru College of Technology, Coimbatore has
sfully completed the individual project titled

“TRANSCRYPTION & DIGITAL WATER MARKING”

s done the project from June 2004 to September 2004. During the period of his project
vith us, he was found to be hard working and sincere in his assignments. We wish him all
t in his future.

Chennai
15/09/2004

Signature of Issuing Authority

DECLARATION

I here by declare that the project entitled **"TRANSCRYPTION & DIGITAL WATER MARKING"**, submitted to **Kumaraguru College of Technology**, Coimbatore Affiliated to Bharathiyar University as the project work of **Master of Science in Applied Science Software Engineering,** is a record of original work done by me under the supervision and guidance of **Mr. Shankar Raman, M.C.A.,** Pellucid Systems., Chennai and **Mr. M.Manikantan. M.C.A.,** Lecturer of Kumaraguru College of Technology, Coimbatore and the project work has not found the basis for the award of any Degree/Diploma/Associate ship/Fellowship or similar title to any candidate of any University.

K. Veerakumar

Place: COIMBATORE **Signature of the student**

Date: 24.9.2004

Countersigned by

(Internal Guide) **(External Guide)**

ACKNOWLEDGEMENT

ACKNOWLEDGEMENT

I am immensely grateful to **Dr.K.K.Padmanabhan, B.Sc (Engg), M.Tech., Ph.D.,** Principal, Kumaraguru College of Technology for his valuable support to come out with this project.

I really feel delighted in expressing my heartful thanks to **Prof. Dr. S. Thangasamy, BE. (Hon's)., Ph.D.,** Head of the Department of Computer Science and Engineering for his endless encouragement in carrying out this project successfully.

My heartfelt thanks to our Course Coordinator **Mr. K.R. Baskaran, B.E., M.S.,** for his unfailing enthusiasm, encouragement and guidance that paved me to the completion of this project.

I am indent to express my heartiest thanks to **Mr. M.Manikantan M.C.A.,** Department of Computer Science and Engineering, my project guide who rendered his valuable guidance and support to do this project work extremely well.

I am greatly indebted to Senior Software Engineer, **PELLUCID SYSTEMS,** Chennai for getting me into his esteemed Institution. I also thank **Mr. Shankar Raman, M.C.A.,** my guide and he has helped me a lot in my project.

I am also thankful to all the faculty members of the Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore for their valuable guidance, support and encouragement during the course of my project work.

My humble gratitude and thanks to my parents who have supported to complete the project and to my friends for lending me valuable tips, support and cooperation through out my project work.

SYNOPSIS

SYNOPSIS

This project entitled ""**Transcryption and Digital Watermarking**" is a real time project done for " **PELLUCID SYSTEMS".**

Only registered users can use this software. Any new user can signup at the time of product Installation and start using the software after proper verification and authentication. This project contains an integrated environment for transcription, audio listening, encryption and digital watermarking. All related activities concerning transcription are clubbed into a single environment.

This project encrypts text files using well known and complicated encryption algorithms. Also there is facility for hiding information in an image. The algorithms used are exclusively developed for this project. The encrypted files can be compressed using the Huffman Algorithm. The keys (Passwords) generated for each file is stored in a database for easier retrieval. This project contains an ingenious method of concealing and embedding information in an image file even it is a plain image. This project has been created keeping in mind the following benefits to the user:

1) To provide the client a user friendly integrated Medical Transcription Editor that is both simple and robust.
2) To provide the client different types of encryption methods so that he can select the method of his choice. And also dynamic encryption facility.
3) To provide the client encoding/hashing modules that encode the secret key.
4) To provide compression facility to compress the files.
5) To provide the client a unique Digital Water Marker, using which he can embed messages or files inside even a plain image.
6) To provide him an Image Browser to select the image of his choice to embed the message inside.
7) To provide facility for storing the generated keys in a database and for easy retrieval of the keys.

This project contains several modules all of which coalesce to form a wholesome and highly secure project.

1) Authentication Module
2) Transcription Editor Module
3) Common Encryption Techniques Module
4) Advanced Encryption Techniques Module
5) Image Browsing & Embedding Module
6) Data Compression Module
7) Database Storage Module
8) Help Module

CONTENTS

INTRODUCTION

1.0 INTRODUCTION

Since this project's main focus is on Cryptography, a clear understanding of the different forms of cryptography and methods of execution is essential. With this in mind I have presented here the fundamental details pertaining to the art of cryptography.

There are two basic kinds of mathematical operations used in encryption systems; transpositions and substitutions. Transpositions rearrange the symbols in the plaintext without changing the symbols themselves. Substitutions replace plaintext elements (symbols, pairs of symbols, etc.) with other symbols or groups of symbols without changing the sequence in which they occur.

The encryption modules contain either one or more of the following techniques.

1. Shuffle Technique
2. Linear Technique
3. Random Technique
4. Complex Technique

1)SHUFFLE means changing odd and even symbols in the string: ABCD == BADC.

2) LINEAR means simple substitution (A + B) mod C.

3) RANDOM is the same as LINEAR except (A+RN) mod C where RN is the random number.

4) COMPLEX is the combination of 1, 2, 3.

Cryptography

It is an art and science of preparing coded or protected communications intended to be intelligible only to the person possessing a key. Cryptography (Greek *kryptos,* "secret"; *graphos,* "writing") refers both to the process or skill of communicating in or deciphering secret writings (codes, or ciphers) and to the use of codes to convert computerized data so that only a specific recipient will be able to read it using a key. Cryptographers call an original communication the cleartext or plaintext. Once the original communication has been scrambled or enciphered, the result is known as the ciphertext or cryptogram. The enciphering process usually involves an algorithm and a key. An encryption algorithm is a particular method of scrambling—a computer program or a written set of instructions. The key specifies the actual scrambling process. The original communication may be a written or broadcast message or a set of digital data.

In its broadest sense, cryptography includes the use of concealed messages, ciphers, and codes. Concealed messages, such as those hidden in otherwise innocent text and those written in invisible ink, depend for their success on being unsuspected. Once they are discovered, they frequently are easy to decipher. Codes, in which predetermined words, numbers, or symbols represent words and phrases, are usually impossible to read without the key codebook. Cryptography also includes the use of computerized encryption to protect transmissions of data and messages.

Today most communication leaves some kind of recorded trail. For example, communications over telephone lines, including faxes and e-mail messages, produce a record of the telephone number called and the time it was called. Financial transactions, medical histories, choices of rental movies, and even food choices may be tracked by credit card receipts or insurance records. Every time a person uses the telephone or a credit card, the telephone company or financial institution keeps a record of the number called or the transaction amount, location, and date. In the future, as telephone networks become digital, even the actual conversations may be recorded and stored. All of this amounts to a great potential loss of privacy. Cryptography is one tool that will be able to ensure more privacy. The ability to encrypt data, communications, and other information gives individuals the power to restore personal privacy.

Cryptography is important for more than just privacy, however. Cryptography protects the world's banking systems as well. Many banks and other financial institutions conduct their business over open networks, such as the Internet. Without the ability to protect bank transactions and communications, criminals could interfere with the transactions and steal money without a trace.

TYPES OF CRYPTOGRAPHY

There are many types of cryptography, including codes, steganography (hidden or secret writing), and ciphers. Codes rely on codebooks. Steganography relies on different ways to hide or disguise writing. Ciphers include both computer-generated ciphers and those created by encryption methods. The different types of ciphers depend on alphabetical, numerical, computer-based, or other scrambling methods.

Codes and Codebooks

A well-constructed code can represent phrases and entire sentences with symbols, such as five-letter groups, and is often used more for economy than for secrecy. A properly constructed code can give a high degree of security, but the difficulty of printing and distributing codebooks—books of known codes—under conditions of absolute secrecy limits their use to places in which the books can be effectively guarded. In addition, the more a codebook is used, the less secure it becomes.

Imagine a codebook with two columns. In the first column is a list of all the words that a military commander could possibly need to use to communicate. For example, it contains all the possible geographic areas in a region, all possible times, and all military terms. In the other column is a list of plain words. To create a coded message, the encoder writes down the actual message. He then substitutes words in the codebook by finding matches in the second column for the words in the message and using the new words instead. For example, suppose the message is *Attack the hill at dawn* and the codebook contains the following word pairs: attack = bear, the = juice, hill = orange, at = calendar, and dawn = open. The encoded message would read *Bear juice orange calendar open*.

If the coded message fell into enemy hands, the enemy would know it was in code, but without the codebook the enemy would have no way to decrypt the message. Codebooks lose some of their value over time, however. For example, if the coded message fell into enemy hands and the next day the hill was attacked at dawn, the enemy could link the event to the coded message. If another message containing the word *orange* were captured, and the following day, something else happened on the hill, the enemy could assume that orange = hill is in the codebook. Over time, the enemy could put together more and more code word pairs, and eventually crack the code. For this reason, it is common to change codes often.

Steganography

Steganography is a method of hiding the existence of a message using tools such as invisible ink, microscopic writing, or hiding code words within sentences of a message (such as making every fifth word in a text part of the message). Cryptographers may apply steganography to electronic communications. This application is called transmission security.

Steganography, or secret writing, seems to have originated almost as early as writing itself did. Even in ancient Egypt, where writing itself was a mystery to the average person, two distinct forms of writing were used. Hieratic or sacred writing was used for secret communication by the priests, and demotic writing was used by other literate people. The ancient Greeks and Romans, as well as other civilizations that flourished at around the same time, used forms of steganography. The invention of the first shorthand system was presumably intended as a form of secret writing. It first came into wide use in ancient Rome, with *notae Tironianae* ("Tironian notes"), a system invented by Marcus Tullius Tiro in 63 BC.

Ciphers

Ease of use makes ciphers popular. There are two general types of ciphers. Substitution ciphers require a cipher alphabet to replace plaintext with other letters or symbols. Transposition ciphers use the shuffling of letters in a word to make the word incomprehensible.

Ciphers are the secret codes used to encrypt plaintext messages. Ciphers of various types have been devised, but all of them are either substitution or transposition ciphers. Computer ciphers are ciphers that are used for digital messages.

Computer ciphers differ from ordinary substitution and transposition ciphers in that a computer application performs the encryption of data. The term *cryptography* is sometimes restricted to the use of ciphers or to methods involving the substitution of other letters or symbols for the original letters of a message

Substitution Ciphers

In simple substitution ciphers, a particular letter or symbol is substituted for each letter. The letters are substituted in their normal order, usually with normal word divisions. Such ciphers are recognized by the occurrence of a set of normal letter frequencies attached to the wrong letters. They are solved by using frequency analysis and by noting the characteristics of particular letters, such as the tendency to form doubles, common word prefixes and suffixes, common first and last letters in words, and common combinations, such as *qu, th, er,* and *re.*

A substitution cipher is performed by reordering the letters in the alphabet. For example, a cipher devised long ago by Julius Caesar shifts all the letters in the alphabet by three places. Thus, when the letter *a* is needed, a *d* is used, and when a *b* is to be written, an *e* is used. The letters wrap around at the end of the alphabet. So, if a person wants to encipher a *z*, it is written as a *c*. Similarly, a *y* is written as a *b*. The entire cipher is represented by two rows of letters. These rows are called a lookup table.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

When someone wants to encrypt a word, he or she looks up the original letter in the top row and uses the corresponding cipher-text letter in the bottom row. So, for example, the word HELLO would be written as KHOOR. To decrypt the coded word, a person would search for the letter in the bottom row and write down the corresponding letter in the top row. So, KHOOR decrypts back to HELLO.

While the above substitution cipher is easy to remember, it is also easy to break. To make a substitution cipher more complex, multiple substitutions and sometimes even numbers are added to the cipher.

In multiple-substitution (poly-alphabetic) ciphers, a keyword or number is employed. The first message letter might be enciphered by adding to it the numerical value of the first letter of the keyword; the second message letter is enciphered similarly, using the second letter of the keyword, and so on, repeating the keyword as often as necessary to encipher the whole message. When adding the numerical value of a keyword letter to a message letter, one starts counting with the message letter. Thus, to encipher the word TODAY by the code word DIG, *t* becomes *w,* as *d* is the fourth letter of the alphabet (count *t, u, v, w*); *o* becomes *w,* as *i* is the ninth letter of the alphabet; and *d* becomes *j,* as *g* is the seventh letter of the alphabet. For the rest of the message the code word is repeated, and thus TODAY is coded WWJDG.

By using combinations of the basic types of ciphers, ciphers can be created to various degrees of complexity. The key, however, should be easy to remember or reproduce, for without it the cipher is no longer a message but a puzzle. Given sufficient time and material, most ciphers can be solved and their keys discovered, but for a particular purpose the complexity need be only so great as to obtain the level of security desired. Military orders that must be kept secret for only a few hours, for example, can be encrypted in a cipher that would be entirely unsuited for diplomatic reports using a cipher over an extended period of time.

Transposition Cipher

In a transposition cipher, the order of plaintext letters is changed to derive the ciphertext. The message is usually written without word divisions in rows of letters arranged in a rectangular block. The letters are then transposed in a prearranged order, such as by vertical columns, diagonals, or spirals, or by more complicated systems, such as the knight's tour, which is based on the move of the knight in chess. The arrangement of the letters in the enciphered message depends upon the size of the block of code words used and upon the route followed in inscribing and transposing the letters.

A cipher in which every pair of letters is swapped is an example of a transposition cipher. In this case, for example, the ciphertext for *elephant* would be *lepeahtn*. The first and second letters are swapped, then the third and fourth letters are swapped, and so on. Transposition ciphers may be combined with substitution ciphers to produce a more complex encoded message.

Breaking Simple Ciphers

Substitution and transposition ciphers appear to be difficult to break. However, if enough messages are encrypted with any cipher, the cipher is easily broken. Repetition of a series of letters may lead code breakers to the key of any cipher system. In a substitution cipher, once a letter is associated with another letter, a pattern emerges and the cipher is easily decrypted.

In order to make a cipher even more secure, a key word or number may be used. Transposition ciphers might be recognized by the letter frequencies (the number of times a common letter, such as *e*, is used compared to the number of times a less frequently used letter, such as *q*, appears) for the language used. Solution of such ciphers without the key is possible by rearranging the letters in various geometric designs and at the same time forming a new word by reordering the letters of the coded word or phrase (such as from *satin* to *stain*) until the method of encipherment is discovered.

Computers may be used to break simple ciphers. Techniques for encrypting data naturally took advantage of the power of computers. Today's modern cryptographic techniques are based entirely on a cryptographic key that is kept secret. The plaintext that is to be encrypted is converted to bits, or binary digits of 1s and 0s. Then complex substitutions and transpositions are performed on the plaintext, using the key as a guide. The transformation of the plaintext to ciphertext is entirely dependent on the key.

COMPUTER CIPHERS AND ENCRYPTION

Government agencies, banks, and many corporations now routinely send a great deal of confidential information from one computer to another. Such data are usually transmitted via telephone lines or other nonprivate channels, such as the Internet. Continuing development of secure computer systems and networks will ensure that confidential information can be securely transferred across computer networks.

In the early 1970s, Horst Feistel, a scientist at International Business Machines Corporation (IBM Corporation), developed LUCIFER, a computerized cryptosystem that used both substitution and transposition.

In 1977 the United States National Bureau of Standards (now the National Institute of Standards and Technology [NIST]) developed a cryptographic technique called the Data Encryption Standard (DES). DES was based on LUCIFER and made use of the computer binary code (converting plaintext to bits, or binary digits of 1s and 0s). DES transformed 64-bit segments of information into 64-bit segments of ciphertext using a key that was 56 bits in size. Each user randomly selected a key and revealed it only to those persons authorized to see the protected data. DES was broken in 1998.

In 1978 three American computer scientists, Ronald L. Rivest, Adi Shamir, and Leonard Adleman, who later founded the company RSA Data Security, created the Rivest-Shamir-Adleman (RSA) system. The RSA system uses two large prime numbers, p and q, multiplied to form a composite, n. The formula $n = pq$, capitalizes on the very difficult problem of factoring prime numbers.

As more and more information is transferred over computer networks, computer scientists continue to develop more secure, complex algorithms. In 1997 the NIST began coordinating development of a replacement for DES called Advanced Encryption Standard (AES). AES will use a more complex algorithm, based on a 128-bit encryption standard instead of the 64-bit standard of DES. This 128-bit algorithm will make AES impossible to decrypt with current technology.

Another encryption system based on 128-bit segments is called International Data Encryption Algorithm, or IDEA. The Swiss Federal Institute of Technology developed the IDEA standard in the 1990s. Computer scientists have also proposed alternatives such as public-key cryptosystems (PKCs), which use two types of keys, a public key and a private key. The public key encrypts data, and a corresponding private key decrypts it. The user gives the public key out to other users, and they can use the public key for encrypting messages to be sent to the user. The user keeps the private key secret and uses it to decrypt received messages. An example of a PKC is the RSA system, described above.

CRYPTANALYSIS

Cryptanalysis is the art of analyzing ciphertext to extract the plaintext or the key. In other words, cryptanalysis is the opposite of cryptography. It is the breaking of ciphers. Understanding the process of code breaking is very important when designing any encryption system. The science of cryptography has kept up with the technological explosion of the last half of the 20th century. Current systems require very powerful computer systems to encrypt and decrypt data..

Today's cryptanalysis is measured by the number and speed of computers available to the code breaker. Some cryptographers believe that the National Security Agency (NSA) of the United States has enormous, extremely powerful computers that are entirely devoted to cryptanalysis.

The substitution ciphers described above are easy to break. Before computers were available, expert cryptanalysts would look at ciphertext and make guesses as to which letters were substituted for which other letters. Early cryptanalysis techniques included computing the frequency with which letters occur in the language that is being intercepted. For example, in the English language, the letters *e, s, t, a, m,* and *n* occur much more frequently than do *q, z, x, y,* and *w*. So, cryptanalysts look at the ciphertext for the most frequently occurring letters and assign them as candidates to be *e, s, t, a, m,* and *n*. Cryptanalysts also know that certain combinations of letters are more common in the English language than others are. For example, *q* and *u* occur together, and so do *t* and *h*. The frequency and combinations of letters help cryptanalysts build a table of possible solution letters.

In modern cryptographic systems, too, the more ciphertext that is available to the code breaker, the better. For this reason, all systems require frequent changing of the key. Once the key is changed, no more ciphertext will be produced using the former key. Ciphertext that is produced using different keys—and frequently changed keys—makes the cryptanalyst's task of code breaking difficult.

I have included many different methods of encryption in this project so that the users can choose the type of method that best fits their need.

1.1 PROJECT OVERVIEW

Objectives of this project:

1) To provide the user with a Medical Transcription Editor with various integrated features.

2) To provide the client different types of encryption methods so that he can select the method of his choice.

3) To provide a Digital Watermarking of important files.

4) To provide the client a unique feature, using which he can embed messages or files inside an image.

5) To provide him a browser to select the image of his choice to embed the message inside.

6) To provide the client encoding modules that encode the secret key.

7) To provide compression facility to compress the files.

8) To provide facility for storing the generated keys in a database and for easy retrieval of the keys.

9) To provide the client a user friendly interface that is both simple and pleasing to eye as well as robust.

10) To provide a highly useful help module.

This project contains several modules all of that combine to form a wholesome and highly secure project.

- **Authentication Module**
- **Medical Transcription Editor Module**
- **Common Encryption Techniques Module**
- **Advanced Encryption Techniques Module**

- **Digital Watermarking Module**
- **Image Browsing & Embedding Module**
- **Data Compression Module**
- **Database Storage Module**
- **Help Module**

➢ Authentication Module:

This module contains a form that shows whenever this program is invoked. The user has to enter his Username and password in the boxes provided. Only when the authentication is verified and succeeded, the user is allowed to enter the main area.

➢ Medical Transcription Editor Module:

This module contains highly productive tools that help a transcriptionist immensely. It has a feature for adjusting the playback rate of the audio file. There is looping facility in the editor so that the user can repeatedly listen to the dictation file for a preset interval. There is facility for increasing and decreasing the speed of the dictation file. This will help the user to transcribe difficult-to-grasp dictation portions easily by slowing down a fast paced dictation file. There is also features for dynamic encryption of the transcribed files, auto-saving option, inbuilt medical dictionary, etc.

➢ Common Encryption Techniques Module:

This module contains different forms, each of which contains a simple but robust encryption technique. The user is allowed to open a file for encryption and then encrypt it. He has to provide a key for decrypting the file. Once a file is encrypted the resultant file is saved in the disk. The user then saves the password key of that particular file in a database. This module also contains an encoding method form which either creates a Hash Key or encodes a password. These forms contain provisions for visually check and inspect the encrypted files.

- **Advanced Encryption Techniques Module:**

The different forms of this module contain time-tested, robust encryption techniques. The algorithms presented here use transposition and substitution but in a rather intricate way.

- **Image Browsing and Embedding Module:**

This module contains three forms each of which does a different work. The image browsing form is used to select an image available in the user's system. The images are displayed as thumbnail images. The user can select an image and preview it in full size. Once he is satisfied with the image he can invoke the image encryption form and embed all the information inside the image. A key is automatically generated that can be stored as the file name of the new embedded message image. The user can decrypt the image and see the message it contains only when he provides the correct password.

- **Digital Watermarking Module:**

This module contains unique Digital Watermarking feature to insert any type of data whether it is text, image, or audio, inside an image. Messages can be embedded even in a plain image. First time implementation of an algorithm developed solely for this project.

- **Data Compression Module:**

This module contains the Huffman Algorithm for compression of large files. The user has to provide the file name and the path to store the new compressed file.

- **Database Storage Module:**

The password keys are stored in this module's form. A simple database system is used with ADODB connectivity. Microsoft's Access forms the backend of this module. The user can also all the keys entered by viewing it in the Password key browser form.

- **Help Module:**

This module contains the help files that instruct new users how to use the application. This module also contains an about form.

1.2 ORGANIZATION PROFILE

Pellucid Systems, Chennai is a reputed company dealing in audio products for the past 7 years. Started in the year 1997 with strength of 15 workers, the company has grown manifold over the years. Now with worker strength of over 120 in the Chennai Head office alone, the company has established many branches all over South India.

The company primarily deals in audio electronic items: both hardware and software. It has a vast client base including Digital Sound Studios, Entertainment industry, Television, Advertising, homes, schools, etc. The company has fulfilled the requirement of its client in a professional manner over the years and has earned a very good name. The company has extensive and continually updated expertise in real-time systems, on-line systems, embedded systems, image processing, audio processing, data communications, networking, e-commerce technologies etc.

VISION

The company's vision is to operate globally and bring the benefits of Information Technology to improve the productivity of their customers and quality of their products and services.

MISSION

Pellucid systems will constantly endeavor to delight its customers through excellence in service delivery and achieve worldwide recognition. People are pellucid systems strength, through staff empowerment, customer focus and Quality Management Systems, Pellucid will continuously improve its products and services to meet international standards of quality, cost and time.

SYSTEM STUDY AND ANALYSIS

2.0 SYSTEM STUDY AND ANALYSIS

System study is the main phase of the system development. Much care has to be taken while undergoing this phase. There should be a careful study of the existing system which may bring up and unwrap various activities and problems. This may also help a lot in proposing the new system and hence the development of the life cycle of the new system.

Why the company needs a new software system?

The client company is engaged in the business of MT (Medical Transcription) and BT (Business Transcription). The client's nature of work is such that it receives audio files from different countries through internet for converting into transcribed files. Once the audio files are downloaded, the transcribers working in the company transcribe the audio files by typing the matter dictated through the audio files. Once the transcription part is over, the client has to send the files through internet to its customers in other countries. It is while sending the transcribed text files through internet that a lot of things can go wrong. The matter transcribed may be of a highly confidential nature, and if by chance it falls into the hands of a rival company of our client's customer, then it will cause irreparable loss to our client's customer. When business secrets adopted by particular company are revealed to its rivals, then the company cannot survive for long. So to protect the interests of the customer's clients and also to protect the integrity and reputation of the client, a tamper-proof method is absolutely necessary. Also, in the case of Medical Transcription files, the matter dictated by foreign doctors contains highly personal details of their patients. If per chance they are fall into disreputable hands, then the privacy of such patients are lost. The patients may suffer irredeemable loss to their repute. When the patient happens to be a famous personality, a revelation of the private details could be very harmful. There are laws in foreign countries that prohibit doctors from revealing their patient's history to outsiders. If the patient feels that his/her personal health details are being made public, or are unnecessarily revealed to others, then he/she may sue the concerned doctor for compensation.

So privacy of personal details is of paramount importance in both the Medical Transcription and Business Transcription fields. Any disclosure will result in severe loss in terms of monetary loss, and loss of reputation etc. It is in this scenario that a highly secure encryption method becomes necessary for all the parties concerned. Besides the above, the company also receives medical images (Radiographic)and others. These images have to be processed and watermarked. So a very good digital embedding/watermarking tool is necessary. Also, the company is in need of an IDE that contains all the required features.

2.1 EXISTING SYSTEM

The existing system suffers from many defects. The foremost being an absolutely insecure system that the client company is following. At present, the client company transcribes Medical and Business audio files and sends the transcribed files changing only the file's extension. For example, if the transcribed file is named Margaret.txt, then the file is renamed as Margaret.abc. The client company naively hopes that in the case of the record being fallen into the hands of others, then those who got the records may not know how to open the files. What the client company does not know is that it is a very simple matter to open the files in any text editor to read the contents.

The next defect is that the client's customers are from many different countries. They want their transcribed documents encrypted using well known methods and algorithms. Since the client company does not have any specific method for encryption of documents, they have to install a software that contains different methods. Otherwise, they will lose their customers and their business will be spoiled.

The next defect is that the size of the transcribed file. If the file size is large, then the uploading and downloading time will be more, which will cause severe problems like disconnection in the middle of file transfer, heavy data traffic, etc. Besides the abovementioned defects the other shortcomings in the existing system are as follows:

1. In the existing system there is no integrated environment for transcription, audio listening, encryption and digital watermarking.
2. In the existing system, the user has to switch between the editor and the audio player frequently. This results in wastage of time, resources, and productivity.
3. There is no separate medical terminology compilation in the existing system. Because of this, whenever a difficult medical terminology is dictated the user is more prone to commit mistakes.
4. There is no automatic correction option in the existing editor.
5. There is no automatic save option in the existing editor.
6. Dynamic Encryption technique has not been implemented in the existing system.
7. There is no feature for adjusting the playback rate of the audio file.
8. There is no audio looping facility in the editor so that the user can repeatedly listen to the dictation file for a preset interval.
9. There is no facility for increasing and decreasing the speed of the dictation file to help the user to transcribe difficult-to-grasp dictation portions easily by slowing down a fast paced dictation file.
10. There is no Digital Watermarking feature.
11. Algorithms present in the existing system are defective.
12. Key Encoding/Hashing feature is absent.
13. No database to store the keys
14. Absence of an Image browser.

2.2 PROPOSED SYSTEM:

In designing the proposed system, I first made a systematic requirement of the needs of the client company. Then I adopted a strategy to include as many different types of encryption methods as possible. And also in the proposed system, there is facility for generating hashing code for password keys. The proposed system also contains an ingenious system to embed text matter inside an image selected by the client company. The proposed system contains a method to compress the files to smaller size. For proper maintenance and record keeping, there is also a database facility for the storage of password keys. Because of all these features the proposed system can safely and beneficently replace the existing system.

Proposed system outline:

1. Secure Encryption:

The proposed system contains several encryption methods to encrypt different types of files and password keys. Since all the encrypted methods are created using reputed and time-tested algorithms, there is a very remote chance of the files being decrypted.

2. Processing speed:

In the new system, the speed of encryption of files is very high. Each method of encryption is optimized to use the processor's maximum capacity. This feature has resulted in the reduction of execution time.

3. Correctness:

The new project does the exact operation needed by the organization and also helps to achieve the objective of the organization.

4. Faster Information Retrieval:

The proposed system uses a database management system to retrieve password information immediately.

5. Security and Privacy:

Data access is only by the authorized users and hence there is high security.

6. Memory and Maintainability:

A large amount of data can be stored and retrieved using only very low amount of memory. The proposed system has been designed in such a manner, that it is very easy to maintain it efficiently.

Advantages of the Proposed System:

- Infallible because of its secure encryption methods
- Accurate decryption by only those who are holding the password keys
- Highly productive Transcription Editor containing useful features
- Unique Digital Watermarking algorithm
- Key encoding feature implemented
- Less expensive to create and maintain the software
- Faster in operation
- Automatic coding
- Minimum manpower
- Flexibility – the software can adopt to different needs
- Easier generation of encrypted files
- Backup facility is provided
- Storage and retrieval of data is easier because of a secure database system
- Easy maintenance
- Latest and secure technological approach to the problems.

Comparison of the Existing System and the Proposed System:

In the existing system there is no integrated environment for transcription, audio listening, encryption and digital watermarking. However, in the proposed system all related activities concerning transcription are clubbed into a single environment.

In the existing system, the user has to switch between the editor and the audio player frequently. This results in wastage of time, resources, and productivity. The proposed system has no such drawback since the audio player has been inbuilt in the editor itself, the user need not alternate between different programs.

There is no separate medical terminology compilation in the existing system. Because of this, whenever a difficult medical terminology is dictated the user is more prone to commit mistakes. This drawback has been overcome in the proposed system by the implementation of Dynamic Medical Terminology database in the editor itself.

There is no automatic correction option in the existing editor. This has been implemented in the proposed system.

There is no automatic save option in the existing editor. The proposed system has an automatic saving feature.

Dynamic Encryption technique has been implemented for the first time in the proposed system. The matter typed will be simultaneously encrypted so that the user can actually see the encrypted form of the transcription file while typing. This feature will help the user to choose different encryption techniques that suit his need. Also, the time taken to convert a transcription file is minimized.

The proposed system has a feature for adjusting the playback rate of the audio file. There is looping facility in the editor so that the user can repeatedly listen to the dictation file for a preset interval.

There is facility for increasing and decreasing the speed of the dictation file. This will help the user to transcribe difficult-to-grasp dictation portions easily by slowing down a fast paced dictation file.

A Unique feature of DWM

The proposed system has digital water marking methodology that has never been attempted before. Using this methodology the user can hide or watermark a file without causing perceptible changes to the image. Even a very plain image file can be made to hold a large data without any changes to its appearance.

PROGRAMMING ENVIRONMENT

3.0 Programming Environment

3.1 HARDWARE SPECIFICATION

SERVER:

- INTEL PENTIUM III,650 MHz
- A REPUTED COMPANY'S MOTHERBOARD
- 128 MB RAM
- 256 MB VIRTUAL MEMORY
- 40 GB HARD DISK
- 15 INCH VGA COLOR MONITOR
- MULTIMEDIA KEYBOARD
- SCROLL MOUSE (Either 2 button or 3 button)
- SOUNDCARD (Either in-built or separate)
- EARPHONES
- SPEAKERS
- WEB SERVER
- MODEM (Either external or internal)
- INTERNET CONNECTION
- PRINTER
- BACKUP MEDIA (Either a Zip Drive or a CD Writer)

CLIENT:

- WINDOWS 95/98/2000/XP / WINDOWS NT
- VGA MONITOR

3.2 SOFTWARE REQUIREMENTS:

- WINDOWS 95/98/2000/XP/WINDOWS NT
- MICROSOFT VISUAL BASIC 6.0 Enterprise Edition

SYSTEM DESIGN AND DEVELOPMENT

4.0 SYSTEM DESIGN & DEVELOPMENT

FEASIBILITY ANALYSIS

Feasibility analysis helps the system to truly meet the user expectations, feasibility analysis involves

(i) Technical feasibility

(ii) Behavioral feasibility

TECHNICAL FEASIBILITY

This centers on the existing computer system and to what extent it can support the proposed system. The existing computer system has enough capacity to support the proposed system.

BEHAVIOURAL FEASIBILITY

This is an estimate of how strong a reaction the user staff is likely to have toward the development of a computerized system.

4.1 INPUT DESIGN

Input is one of the expensive phases of the operation of a computerized system. The input data are the lifeblood of a system and has to be analyzed and designed with utmost care and consideration. Input system design features can ensure the reliability of the system and generated correct reports from the accurate data. It also determines whether the user can interact efficiently with the new system. Different types of problems occurring in the system can usually be traced back to faulty input design method. The input data is validated, edited, organized in an acceptable from by the system before being processed.

Error message are displayed in the screen when any invalid data was given as input in the system. While entering data, the user needs to know the following:

Type of file to be encrypted.

A basic knowledge about the different image types for digital watermarking.

The sequence of operations required to perform a particular task.

A thorough understanding of how the software functions.

4.2 OUTPUT DESIGN

Computer output is most important and is a direct source of information to the user. Efficient and intelligible output design should improve the system's relationship with the user and help in decision making. The nature of processing and procedures related to the system were classified and verification whether they give the expected results as output.

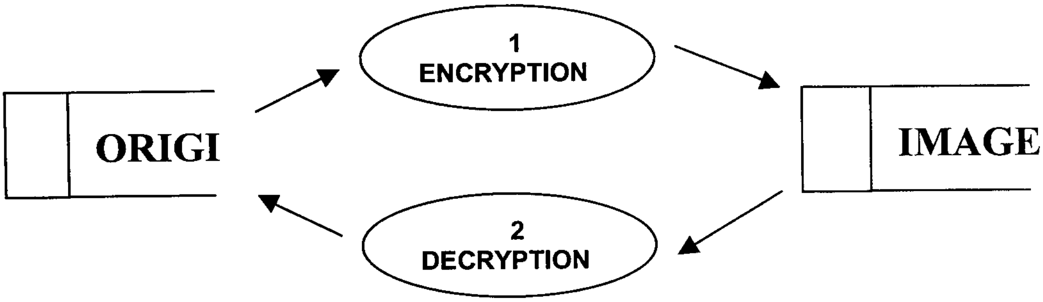
Output from the computer system are required primarily to communicate the result of processing and provide permanent copy of these results for later consultation. While designing the output, the type of the output, concerning format, frequency, responses etc have been taken into consideration. The encrypted files and also the digital watermarking files play an important role in the output design.

4.3CODE DESIGN

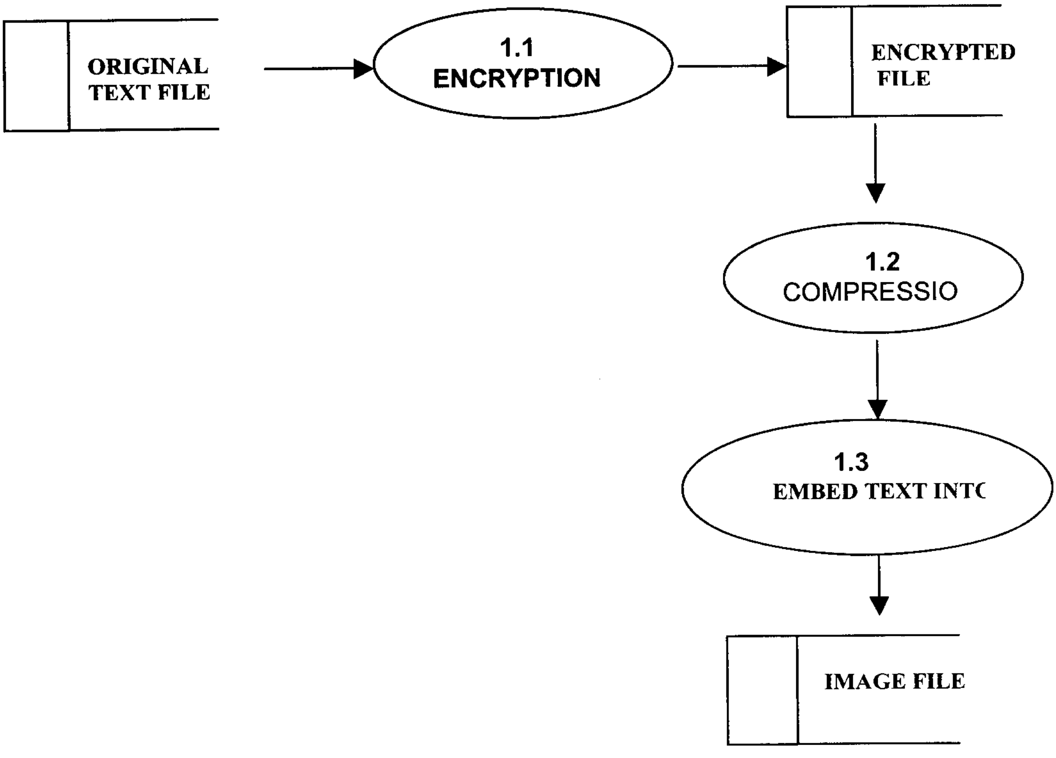
The purpose of the code is to facilitate the identification and retrieval of items of information. A code is an ordered collection of symbols designed to provide unique identification of an entity or attributes. In the system design phase, code design has an important role. The coding system are used to reduce the input, control errors and speed up the entire process. So coding system are methods in which conditions, words, idea or relationship are expressed by a code. The code designed for this project offers uniqueness, expandability, conciseness, uniformity, simplicity, versatility, meaningfulness and operability.

4.4DATA FLOW DIAGRAM

DFD LEVEL 0



DFD LEVEL 1



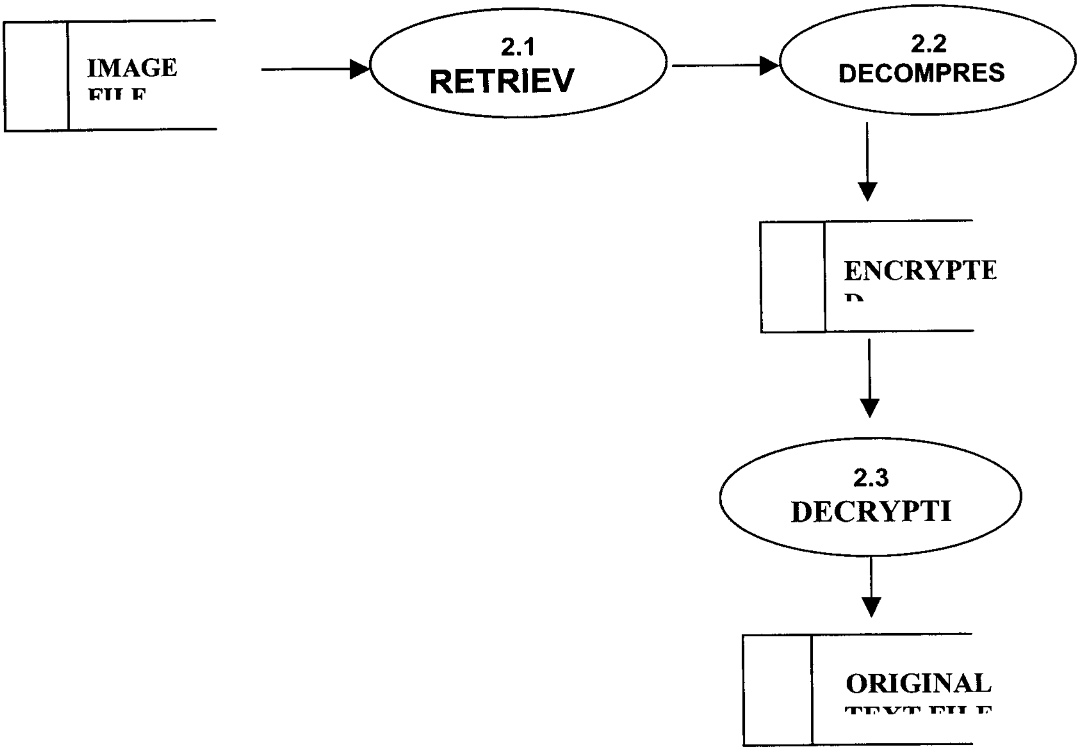
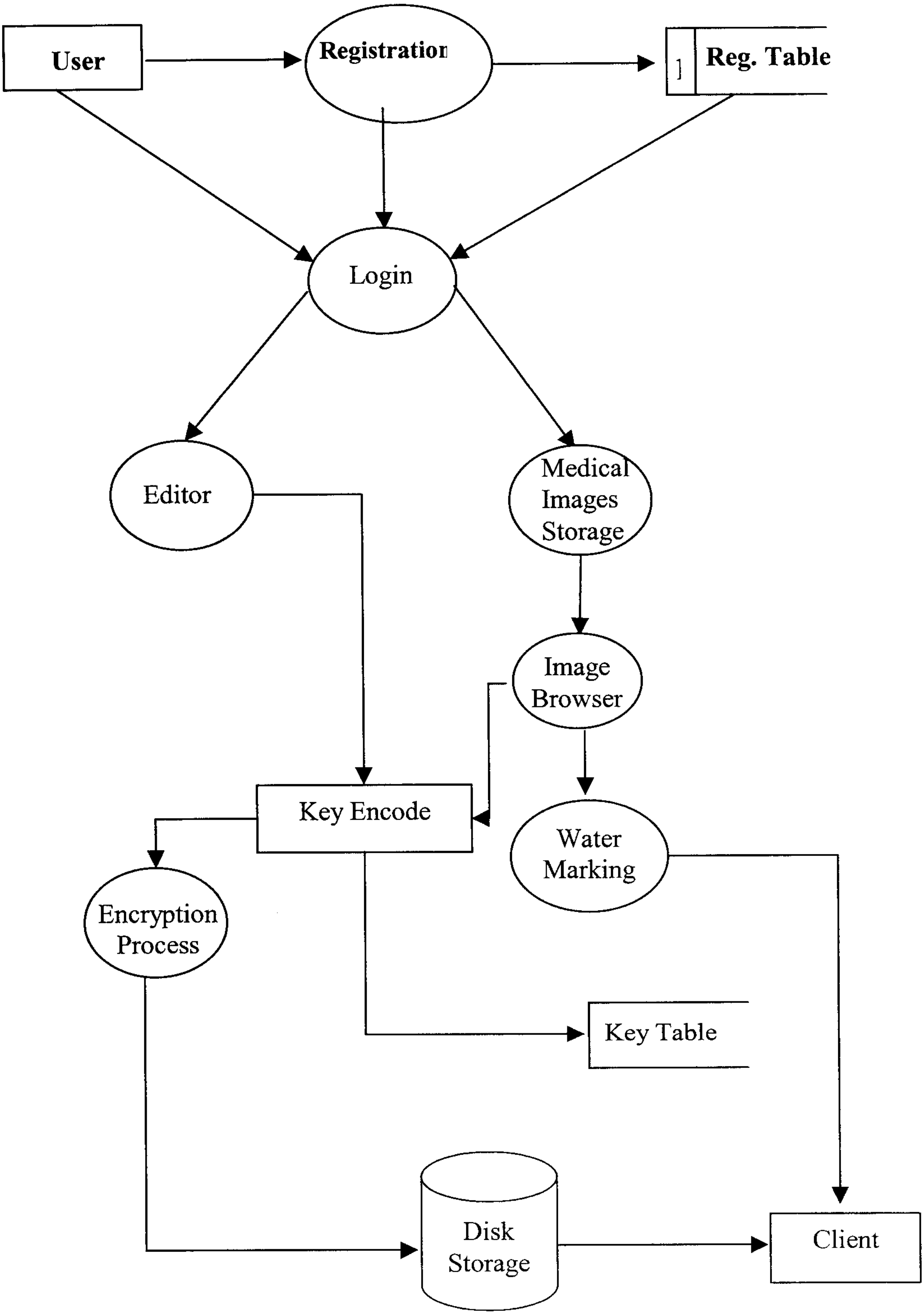


IMAGE
FILE
2.1
RETRIEV
2.2
DECOMPRES
ENCRYPTE
D
2.3
DECRYPTI
ORIGINAL
TEXT FILE

DATA FLOW DIAGRAM:



System Testing & Implementation

5.0 SYSTEM IMPLEMENTATION & TESTING

5.1 SYSTEM IMPLEMENTATION

It is an important stage in any system development life cycle process. Testing is a process of executing a program with respect to software quality. Software testing is a critical element of software quality assurance and represents the ultimate review of specification, design and coding. Different test conditions should be thoroughly checked and the bugs deleted should be fixed. To do this there are many ways of testing the system reliability, completeness, correctness and maintainability.

5.2 SYSTEM TESTING

Testing is the process of exercising of evaluating a system or system components by manual or automated means to verify that it satisfies specified requirements. Testing is also a process of executing a program with the intent of finding errors. A good test case is one that has a high probability of finding an error. A successful test case is one that detects an as-yet-undiscovered error

Software testing can be looked upon as one among the many processes an organization performs that provides the last opportunity to correct any errors in the developed system. Software testing includes selecting tests and test data that have more probability of finding errors.

The first step in system testing is to develop a plan that tests all aspects of the system. Completeness, correctness, reliability and maintainability of the software are to be tested for best quality assurance – an assurance that the system meets the specifications and requirements for its intended use and performance. System testing is the most practical process of executing a program with the explicit intention of finding errors that make the programs fail.

Testing was done in following 3 steps:

- The function performance of all individual modules.
- The interface system
- The user requirement specification. Individual document is provided for the user and management

A test plan entails the following activities: -

- Preparation of test plans
- We specify conditions for user acceptance testing
- Then we prepare test data for program testing
- Also we prepare test data for transaction path testing
- Then we plan user training
- The programs were compiled / assembled
- Finally operational documents are prepared.

The different types of testing adopted in this project are:

UNIT TESTING

Unit testing concentrates on each unit of the software as implemented in source code. Initially test focuses in each module individually, assuring that if functions properly as unit test makes heavy use of while box testing , exerting specific paths in a modules control to ensure complete coverage and maximum error deduction. In each phase unit test has done to review the performance of each module and the bugs are removed and time study is also done and it is minimized.

INTERGRATION TESTING:

Integration tasting is a systematic technical for constructing the program structure while conduction tests to uncover errors associated with interfacing. The objective is to take unit tested modules and build a program structure that has been dictated by design. The system functions well after integrating the active modules.

VALIDATION TESTING:

Validation testing refers to a different set of activities that ensure that the software that has been will is traceable to customer requirements. Data entered by the customer should be validated properly and finally moved to the server. The validation is done to the client size and was found satisfactory to the client as well as administration.

OUTPUT TESTING:

The output testing is used to uncover errors and it is conducted at the developer's site buy a customer. The software is used in a natural setting with the developer "looking over the shoulder " of the user and recording errors and usage problems. Output tests are conducted in a controlled environment.

USER ACCEPTANCE TESTING:

The user acceptance test is conducted at one or more customer sites by the end users of the software. Unlike output testing the developer is generally not present. Therefore the user acceptance test is a "live" application of the software in an environment that cannot be controlled by are encountered during the user acceptance testing and reports these to the developer of regular intervals. As a result of problems reported during user acceptance tests, the software developer makes modification and then prepares for release of the software product to the entire customer base.

TESTS PERFORMED REGARDING THIS SOFTWARE

A number of experiments are conducted to test the software for bugs. These experiments are listed below. The experiments are classified depending on the inputs that the user has to specify and the computations and processing that are done with the code.

OPERATING SYSTEM & HARDWARE:

Any software needs memory to run and also the processor utilization for the software is also very important. We have tested our software under different processor speeds and on different operating system platforms. The test is also extended by checking the memory utilization by running the same software by varying the RAM capacities. We have also noted the effects of different sound cards, microphones, and speakers and their impact on the ultimate analysis of sounds.

The results are as follows:

These are the results that occurred on testing the software under different operating systems.

Windows Platforms

Microsoft Windows 95	Works fine
Microsoft Windows 98	Works fine
Microsoft Windows ME	Works fine
Microsoft Windows XP	Works fine

Processor Speed

Pentium I 166 MHz . Works Well (With 16/32 Mb SDRam)

Pentium II 233 MHz. Works Well (With 32 Mb SDRam)

Pentium II 500 MHz. Works Well (With 32 Mb SDRam)

Pentium III 500 MHz. Works Well (With 64 Mb SDRam)

Pentium III 833 MHz. Works Well (With128 Mb SDRam)

Pentium VI 1.4 GHz. Works Well (With 128 Mb SDRam)

We came to the conclusion that any Hardware and OS fulfilling the above criteria works fine for this software.

MODULE TESTING

Each individual program module was tested for any possible logical effort. They were also tested for specifications to see if they are working as per what the program is supported to do and how it should perform under various conditions.

VOLUME TESTING

The user has provided the test data for this kind of test. This was made to check whether the hardware and software are functioning correctly when large amount of data is supplied.

USABILITY AND DOCUMENT TESTS

This is to verify the user-friendliness of the system developed. Normal operating and effort handling procedures are related to this. Accuracy and completeness of documentation is checked here.

PROGRAM TESTING

This test is used to check the errors in syntax and logic. To detect errors, the actual output is compared with the expected output. When a mismatch occurs the instruction sequence is traced to detect the error.

STRING TESTING

Here each portion of the system is tested against the entire module with the test data provided by the user. This is done because programs are related to one another and they interact in a total system.

QUALITY ASSURANCE

Quality assurance is the review of software and related documentation for correctness, accuracy, reliability, maintainability and expandability. This also includes assurances that the system meets the specification and the requirements for its intended use and performance.

MAINTENANCE ISSUES

The maintenance activities are:

The first maintenance activity occurs since it is unreasonable to assume that testing will uncover all errors in a large system. The process of including the diagnosis and correction of one or more errors is called corrective maintenance.

The second activity that contributes a definition of maintenance occurs since rapid change is encountered in every aspect of computing.

The third activity involves recommendations for new capabilities, modifications to the existing functions and general enhancements when the software is used.

Software is changed to improve future maintainability or reliability. This is called as preventive maintenance.

Maintenance Characteristics

Structured and unstructured maintenance

The only available elements of a software configuration are source code; maintenance activity begins with an evolution of the code, often complicated by poor internal documentation. The suitable characteristics such as program structure, global data structure, system interfaces, performance and design constraints or difficult to handle and are often misinterpreted.

Maintenance Cost

The cost of software maintenance has increased steadily during the past several years. One intangible cost of software maintenance is the development opportunity that is postponed or lost since the available resources must be channeled to maintenance tasks.

Problems

Most of the problems associated with software maintenance can be traced. The problems are

It is often difficult or impossible to trace the evaluation of the software was created.

It is difficult to understand some one else the program.

The maintenance has not been viewed as glamorous work. Much of these perceptions come from the high frustrations level associated with maintenance work.

Maintainability

Maintainability can be defined as the case with which software can be, corrected, adopted and enhanced.

Controlling Features

Availability of qualified software staff.

Understandable system structure.

Easy of system handling.

Use of standardized programming languages.

Use of standardized operating system.

Standardized structure of documentation.

CONCLUSION

6.0 CONCLUSION

After some extended debugging, all the methods successively hid the data so that it was unnoticeable,and successfully decoded the data requested. This software was also tested by several medical professionals (doctors, medical imaging technologists). They indicated confidence in what they saw evenwith data embedded into the image. They felt the changes did notchange the perception of the image or the diagnosis. Most thought the need for patient security was important and my first attempt at this was valid.This project provided me with the oppurtunity to learn and implement all the different techniques in the steganography area. Some new algrithms were created for this project to embed information in a plain image. A user friendly IDE was developed containing different features of the Medical Transcription field. Given enough time, this project could be extended to cover other areas like embedding Ultrasound, CT, MRI that have been saved as an AVI file.

SCOPE FOR FUTURE DEVELOPMENT

7.0 SCOPE FOR FUTURE DEVELOPMENT

In future, algorithms for encoding and decoding and embedding the following three formats could be developed:

z

1) AVI format
2) WAV format
3) DICOM format (It is a common medical imaging format)

An AVI editor could be built in the project to obviate the need for viewing the AVI file frames in a separate external editor. Similarly, a sound editor could be included and used to analyze the encoded wave files. A DICOM editor could also be built to see if all required patient info had been encrypted.

BIBLIOGRAPHY

8.0 BIBLIOGRAPHY

Books:

- **Elias M.Award,**“System Analysis and Design”, Galgotia Publications, Second Edition, 1995.
- **Cole,Eric. Hiding in Plain Sight** .” Steganography and the Art of Covert Communication.” San Francisco:Wiley Publishing,Third Edition ,2003.
- **Lee,**“Introducing System Analysis and Design”,Galgotia Book Source,1980.
- **Roger S.Pressman,**“Software Engineering-A Practioners Approach”, McGraw Hill International Editions, Fouth Edition, 1990.

Web sites

www.cryptography.com

www.dimag.com

www.astalavista.box.sk

CD-ROM:

Singh, Simon. “The Code Book on CD-ROM. CD-ROM”. Virtual Image, 2002.

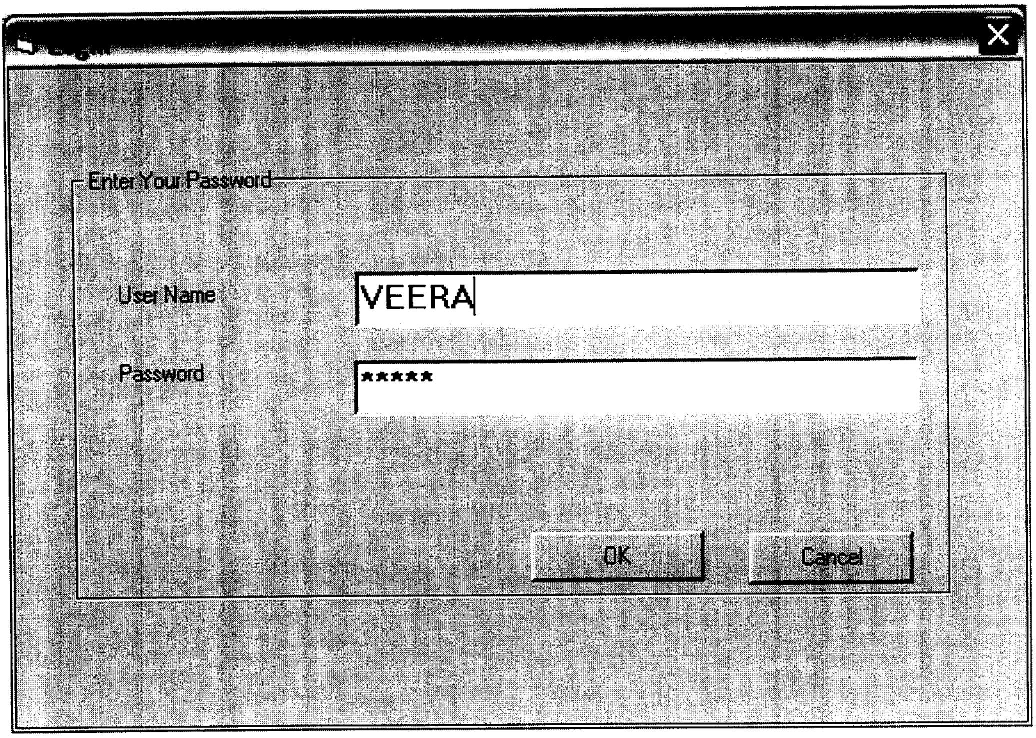
Magazine:

D. Ananad and U.C. Niranjan, “Watermarking Medical Images with Patient Information” in proc. IEEE/EMBS Conference, Hong Kong, China, Oct 1998, pp. 703-706

APPENDIX

9.0 APPENDIX

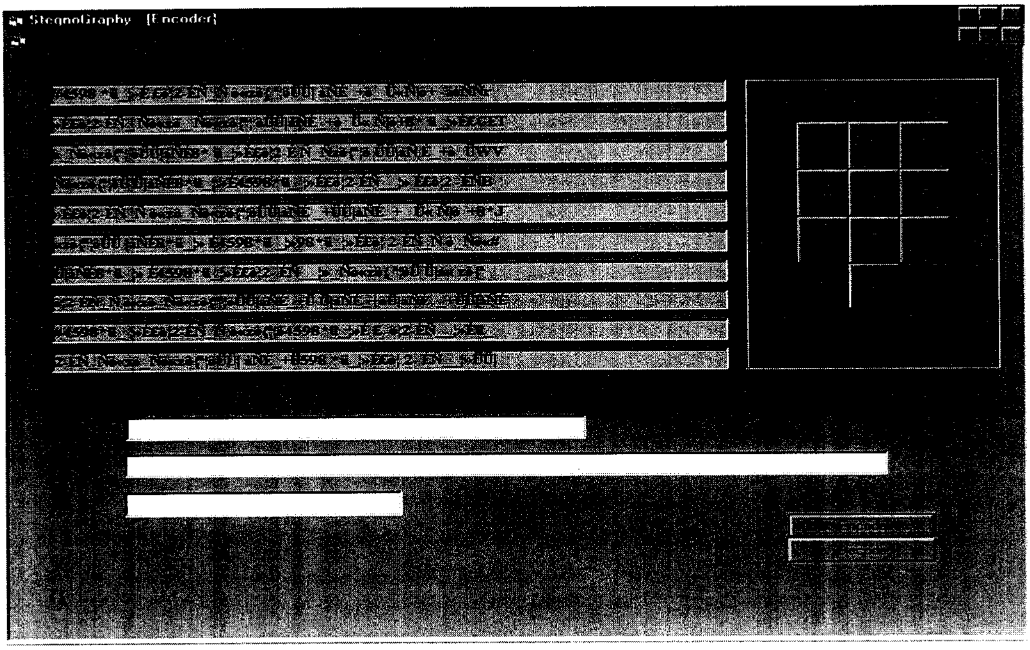
9.1 Sample Screen

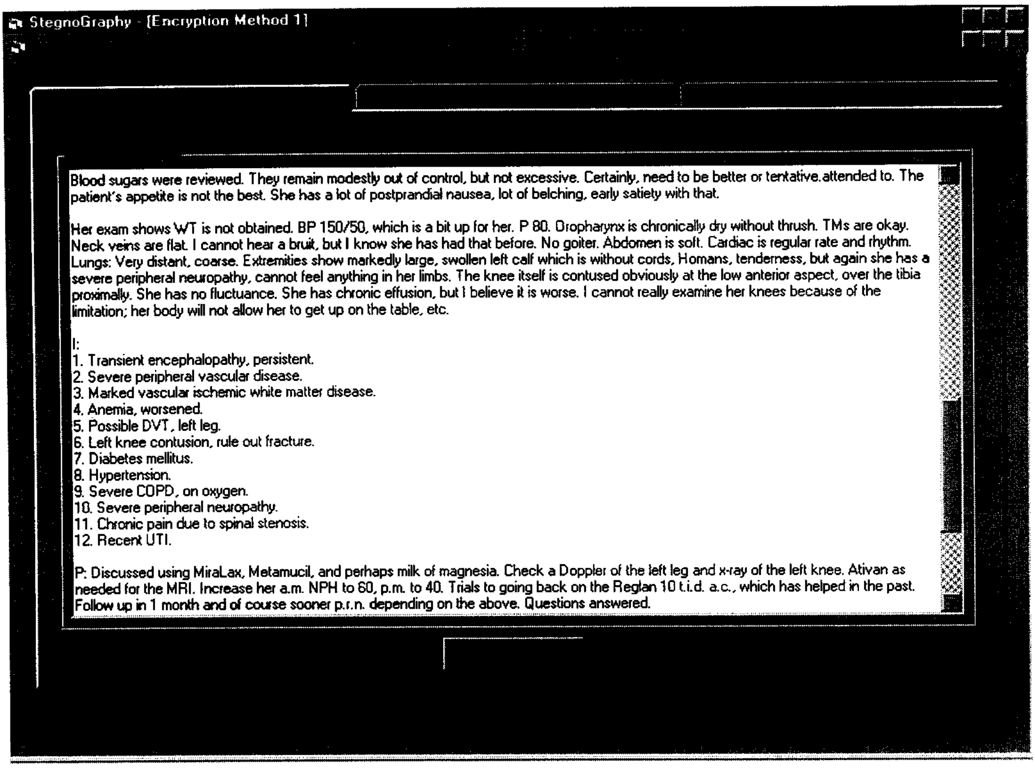


Enter Your Password

User Name: VEERA

Password: *****



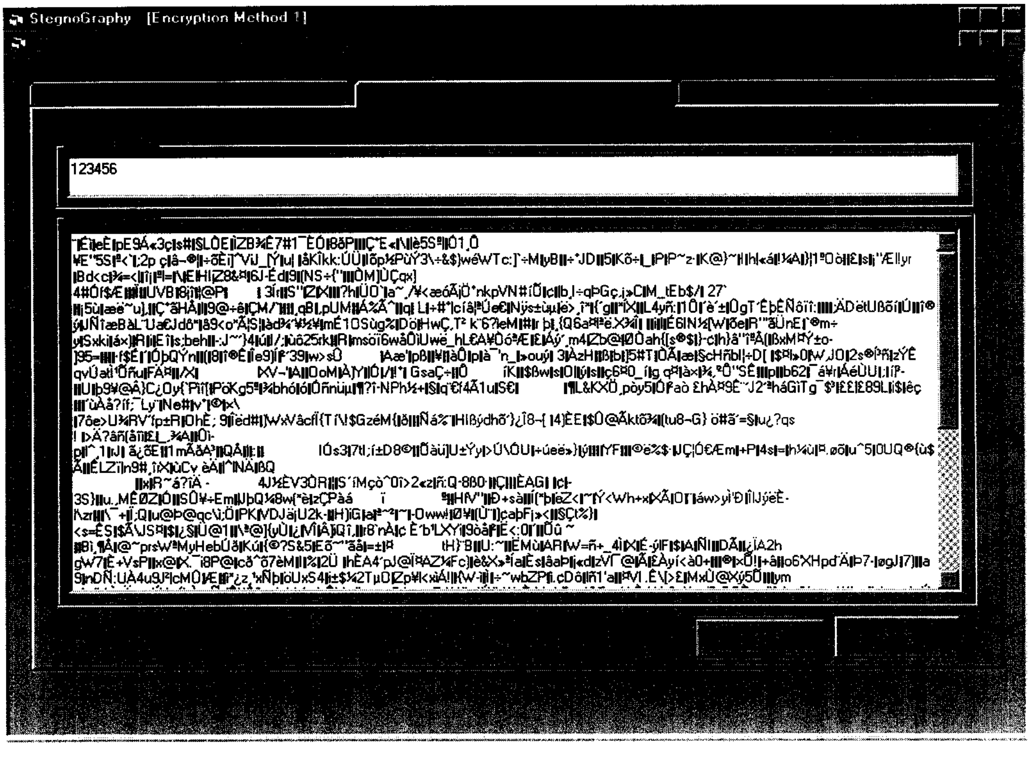


Blood sugars were reviewed. They remain modestly out of control, but not excessive. Certainly, need to be better or tentative.attended to. The patient's appetite is not the best. She has a lot of postprandial nausea, lot of belching, early satiety with that.

Her exam shows WT is not obtained. BP 150/50, which is a bit up for her. P 80. Oropharynx is chronically dry without thrush. TMs are okay. Neck veins are flat. I cannot hear a bruit, but I know she has had that before. No goiter. Abdomen is soft. Cardiac is regular rate and rhythm. Lungs: Very distant, coarse. Extremities show markedly large, swollen left calf which is without cords, Homans, tenderness, but again she has a severe peripheral neuropathy, cannot feel anything in her limbs. The knee itself is contused obviously at the low anterior aspect, over the tibia proximally. She has no fluctuance. She has chronic effusion, but I believe it is worse. I cannot really examine her knees because of the limitation; her body will not allow her to get up on the table, etc.

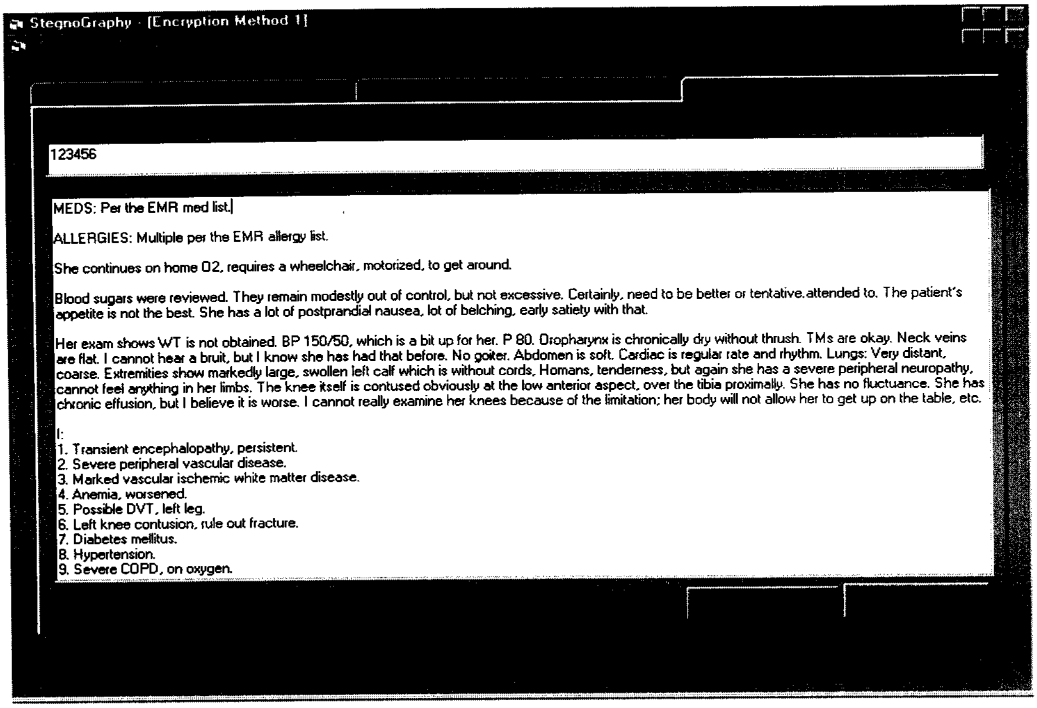
I:
1. Transient encephalopathy, persistent.
2. Severe peripheral vascular disease.
3. Marked vascular ischemic white matter disease.
4. Anemia, worsened.
5. Possible DVT, left leg.
6. Left knee contusion, rule out fracture.
7. Diabetes mellitus.
8. Hypertension.
9. Severe COPD, on oxygen.
10. Severe peripheral neuropathy.
11. Chronic pain due to spinal stenosis.
12. Recent UTI.

P: Discussed using MiraLax, Metamucil, and perhaps milk of magnesia. Check a Doppler of the left leg and x-ray of the left knee. Ativan as needed for the MRI. Increase her a.m. NPH to 60, p.m. to 40. Trials to going back on the Reglan 10 t.i.d. a.c., which has helped in the past. Follow up in 1 month and of course sooner p.r.n. depending on the above. Questions answered.



123456

```
¨ÉìeÈ|pE9Á«3ç|s#|§LÒE|ÌZB¾Ê7#1¯ÈÓ|ßðP||Ç*E«|\|è5S²|Ó1¸Ô
¥E"5S|ª<`|;2p ç|â–®||÷õÈi]^ViJ_[Ý|u| |åKÎkk:ÚÙ||õp¾PùÝ3\÷&$)wéWTc:]`÷M|yB||÷*JD||5|Kõ÷|_|P|P~z·|K@}~|||h|«á|!¼A|}|1ºOò||£|s|¡"Æ||yr
|Bd<c|¾=<||î¡|ª|=|\|E|H|Z8&¤|6J-Éd|9|[NS÷{"|||ÒM]ÙÇqx]
4#Óf$Æ|||||UVB|8¡î|@P|      | 3ír||S"|Z|X|||?h|ÙÒ`|a~./¥<æóÃjÖ*nkpVN#íÕ|c||b¸|÷qÞGç¸j»C|M_tEb$/| 27`
||¡5ù|aeë~u],||Ç*ãHÅ||9@÷ê|ÇM/"|||,qB|,pUM||Á%Ã^||q| L|÷#*|cíâ|ªÚe€|Nýs±ùµ|é>¸î*|{´g||*ÍX||L4yñ:|1Ô|`è´±|ÓgT´ÉþÉÑôïî:||||:ÄDètUßõî|Ú||î®
ýJÑîaeBàL¨Ua€Jdô"|â9<o*Ã|S¦|àd¾´¥½¥|mÉ1OSùg%|DöHwÇ,T² k¨6?|eM|#|r þ|¸{Q6aª|ªë.X¾î| ||||||É6IN½[W|õe|R'"ãÙnE|`®m÷
y|Sxki|áx)|R||È î|s;beh||-:J~"}4|ú||/;|ùô25rk||R|msöï6wåÔìUwè_hL€A¥Òó²Æ|£|Áý´.m4|Zb@|ØÒah{[s®$|}-c|h}â"î²Å(|ßxM¤Ý±o-
]95=|||·f$É|´|ÓþQÝn||(8|î®É|îe9)|f´39|w>sÛ        |Aæ'|pß||¥||àÔ|p|à¯'n_|»ouý| 3|ÀzH||ß|b|]5#T|ÒÃ|aæ|§cHñb||÷D[ |$¤|»0|W,JO|2s®|ªñ|zÝÊ
qvÙatì'ÕñuIFÄ¤||/X|          |XV–'|A||OoM|À]Y||Ó|/|!*| GsaÇ÷||Ô       íK||$ßw|s|O||ý|s||ç6¤0_í|g q¤|àx|¾,²Ô"SÉ|||p||b62|¯á¥r|ÁéÙÙI;IíP-
||U|b9¥@Â}C¿Oy{`Pìî||PöKg5ª|¾bhó|ó|Ôñnùµ|¶?î-NPh½+|§|q¨€f4Ã1u|S€|          |¶L&KXÖ¸pòy5|Ó|ªaò £hÀ¤9È¨J2²háGìTg¯$ª|££|£89L|i$|éç
|||´ùÀå?íf;¯Ly¨|Ne#|v*|©|x\
|7ôe>U¾RV´fp±R|OhÈ; 9|îèd#|)WxVâcfÏ{TíN!$GzéM{|ð|||Ñá%¨|H|ßýdhõ´}¿Î8¬{ |4}ÈE|$Ù@Ãktõ¾|(tu8¬G} ö#ã´=§|u¿?qs
! |>Ä?ãñ(åîî£|_¾A||Ôì-
p||^¸1||J| ã¿õE||1mÃðA³||QÅ|||:||          |Ós3|7t|;í±D8©||Õàü]U±Ýy|>Ú\ÓU|÷úeë»}|ý|||YF|||©ë%$·|JÇ|Ó€Æm|+P|4s|=|h¼ù|¤.øõ|u^5|OUQ®{ù$
Ã||ÉLZï|n9#¸îX|ùCv èÄ||^|NÄ|ßQ
             ||x|R~á?îÄ -             4J½ÈV3ÒR||S´íMçò^0î>2«z|ñ:Q-8ß0·||Ç|||ÈAG| |c|-
3S}||u.,MÉØZ|Ó||SÛ¥÷Em||JþQ¼8w{*è|zÇPàá        ï              ¶||HÍV"||Ð+sà||í(*þ|éZ<|~|Ý<Wh+x|XÃ|O|`|áw>yì'Ð|î|JýèÈ-
Ñzr|||\¯+|Ï;Q|u@Þ@qc\i;Ö|PK|VDJäjU2k-||H)iG|a|ª~²|~|-Oww!|Ø¥|(Ù¨|]çabFj»<||§Çt%)|
<s=£S|$Ã\JS¤|$|¿§|Ù@1||\ª@]{yÙ|¿M|Â]Qî,||r8`nÀ|c È´b'LXY|9òå|ªÉ<:O|´||Õû ~
||8ì,¶Å|@~prsW²MyHebÚð|Kú|{©?S&5|Eõ~"ãå|=±|¤            tH}¨B||U:~||ÈMù|AR|W=ñ+_4ì|X|É-ýlF|$|A|Ñ|||DÃ||¿ÏA2h
gW7|È+VsP||x@|X.¯î8P@|cð^õ7èM||%|2Ü |hÈA4´pJ@Ï¤AZ¼Fc)|è&X»ª|a|È s|âaÞ|¡«d|zV|¯@|Ã|£Àyí<à0+|||®|xÕ!|+â||o6XHpd'Ä|Þ7-|øgJ|7)|||a
9|nDÑ:UÀ4u9J²|cMÒ|Æ||i*¿z¸'xÑþ|öUx54|¡±$¾2TµD|Zp¥|<xiÁ!||{W-i|||÷~wbZP¶.çDô||ñ1'a||¤V| .Ê\[>£|MxÙ@Xý5Õ|||ym
```



123456

MEDS: Per the EMR med list.

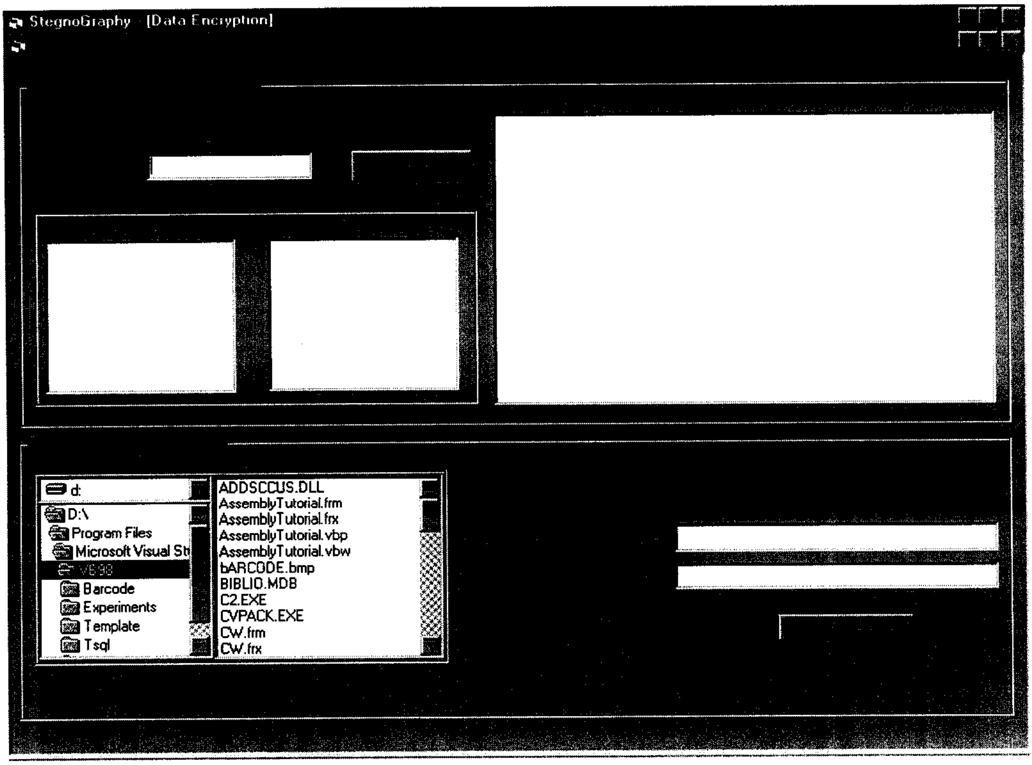
ALLERGIES: Multiple per the EMR allergy list.

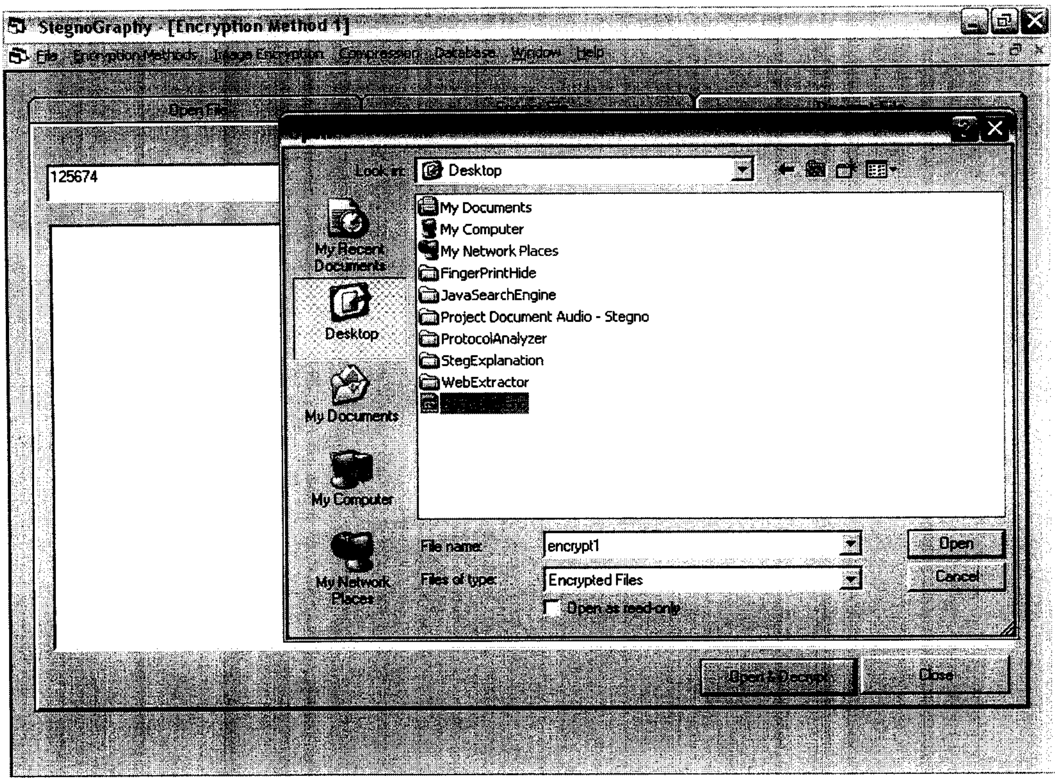
She continues on home O2, requires a wheelchair, motorized, to get around.

Blood sugars were reviewed. They remain modestly out of control, but not excessive. Certainly, need to be better or tentative.attended to. The patient's appetite is not the best. She has a lot of postprandial nausea, lot of belching, early satiety with that.

Her exam shows WT is not obtained. BP 150/50, which is a bit up for her. P 80. Oropharynx is chronically dry without thrush. TMs are okay. Neck veins are flat. I cannot hear a bruit, but I know she has had that before. No goiter. Abdomen is soft. Cardiac is regular rate and rhythm. Lungs: Very distant, coarse. Extremities show markedly large, swollen left calf which is without cords, Homans, tenderness, but again she has a severe peripheral neuropathy, cannot feel anything in her limbs. The knee itself is contused obviously at the low anterior aspect, over the tibia proximally. She has no fluctuance. She has chronic effusion, but I believe it is worse. I cannot really examine her knees because of the limitation; her body will not allow her to get up on the table, etc.

I:
1. Transient encephalopathy, persistent.
2. Severe peripheral vascular disease.
3. Marked vascular ischemic white matter disease.
4. Anemia, worsened.
5. Possible DVT, left leg.
6. Left knee contusion, rule out fracture.
7. Diabetes mellitus.
8. Hypertension.
9. Severe COPD, on oxygen.





125674

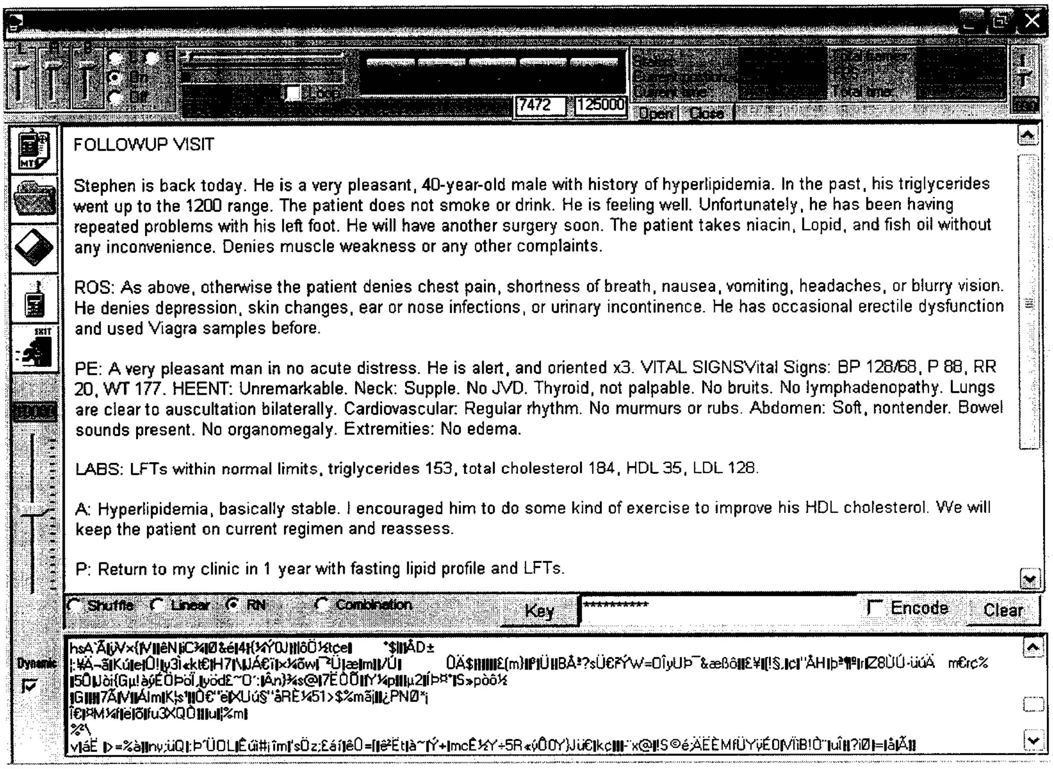
Look in: Desktop

- My Documents
- My Computer
- My Network Places
- FingerPrintHide
- JavaSearchEngine
- Project Document Audio - Stegno
- ProtocolAnalyzer
- StegExplanation
- WebExtractor
- [redacted]

File name: encrypt1

Files of type: Encrypted Files

□ Open as read-only



7472 125000

FOLLOWUP VISIT

Stephen is back today. He is a very pleasant, 40-year-old male with history of hyperlipidemia. In the past, his triglycerides went up to the 1200 range. The patient does not smoke or drink. He is feeling well. Unfortunately, he has been having repeated problems with his left foot. He will have another surgery soon. The patient takes niacin, Lopid, and fish oil without any inconvenience. Denies muscle weakness or any other complaints.

ROS: As above, otherwise the patient denies chest pain, shortness of breath, nausea, vomiting, headaches, or blurry vision. He denies depression, skin changes, ear or nose infections, or urinary incontinence. He has occasional erectile dysfunction and used Viagra samples before.

PE: A very pleasant man in no acute distress. He is alert, and oriented x3. VITAL SIGNSVital Signs: BP 128/68, P 88, RR 20, WT 177. HEENT: Unremarkable. Neck: Supple. No JVD. Thyroid, not palpable. No bruits. No lymphadenopathy. Lungs are clear to auscultation bilaterally. Cardiovascular: Regular rhythm. No murmurs or rubs. Abdomen: Soft, nontender. Bowel sounds present. No organomegaly. Extremities: No edema.

LABS: LFTs within normal limits, triglycerides 153, total cholesterol 184, HDL 35, LDL 128.

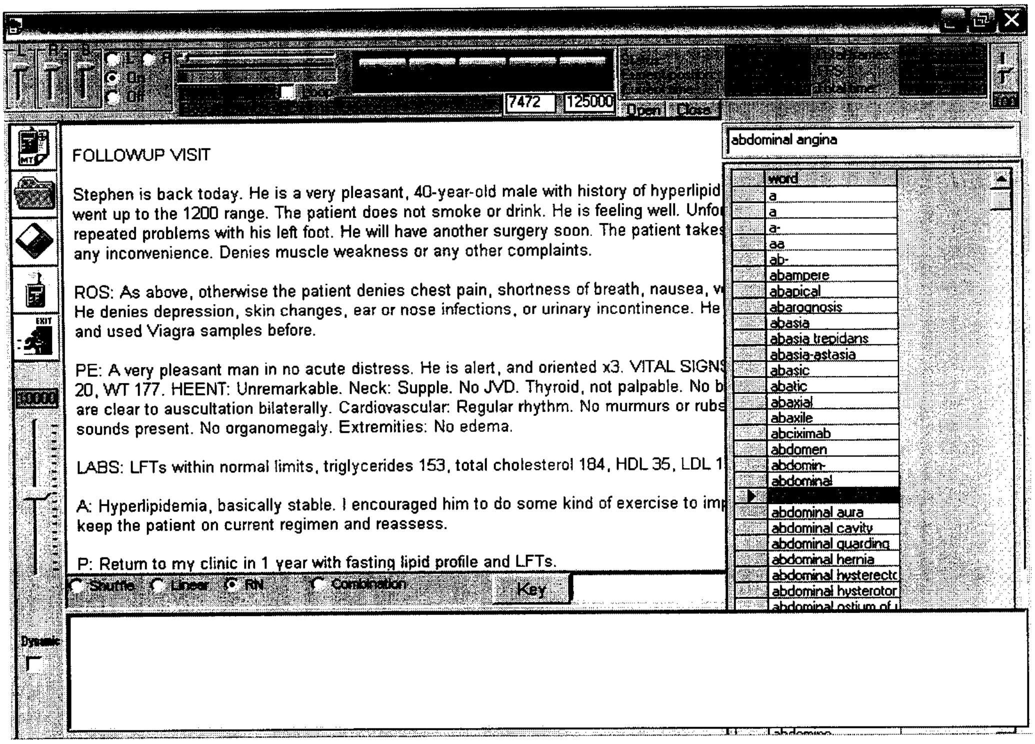
A: Hyperlipidemia, basically stable. I encouraged him to do some kind of exercise to improve his HDL cholesterol. We will keep the patient on current regimen and reassess.

P: Return to my clinic in 1 year with fasting lipid profile and LFTs.

○ Shuffle ○ Linear ● RN ○ Combination Key *********** □ Encode Clear

☑ Dynamic

```
hsA`ÃlyVx{fVlleNlC¾lØ&él4l{¼ÝOJlllôÖ½tçel      *$lllÅD±
|;¥Ä–ãlKúlelÖ!ly3ì«ktЀlH7lNJÁ€ïl×¼õwl¯²Ülæ|ml/Úl         ÖÄ$lllll£(m)lPlÜllBÅ²?sÜ€ªÝW=0ÎyUÞ¯&æßôll£¥l[!§,lcl'ÅHlþ³¶ºlrlZ8ÙÚ·üúÄ   m€rç%
l5ÔlJòí{Gµ!àýÉÖÞöÏ,lyòd£~0´:lÂn}¾s@l7ËÖÕllY¼plllµ2lÍÞ¤*lS»pòô½
lGlll7ÃlVlÁlmlK¦s'llÒ€"ëlXUú§"åRÈ¼51>$%mãlll¿PNØ*¡
Î€l¤M¼fleló|fu3XQÒlllull%ml
%^\
vlâË l>=%àllny;üQl:Þ'ÜDLlÊúi#¡îmlsÖz;£áïlêÖ=ll颲Ëtlà~lÝ+lmcÊ½Y÷5R«ýÔ0Y}Jü€lkçlll-¨x@l!S©é;ÄËÈMfÜYÿÉ0lVïB!Ö¨luîll?iØl=låÌÃll
```



FOLLOWUP VISIT

Stephen is back today. He is a very pleasant, 40-year-old male with history of hyperlipid
went up to the 1200 range. The patient does not smoke or drink. He is feeling well. Unfo
repeated problems with his left foot. He will have another surgery soon. The patient take
any inconvenience. Denies muscle weakness or any other complaints.

ROS: As above, otherwise the patient denies chest pain, shortness of breath, nausea, v
He denies depression, skin changes, ear or nose infections, or urinary incontinence. He
and used Viagra samples before.

PE: A very pleasant man in no acute distress. He is alert, and oriented x3. VITAL SIGN
20, WT 177. HEENT: Unremarkable. Neck: Supple. No JVD. Thyroid, not palpable. No b
are clear to auscultation bilaterally. Cardiovascular: Regular rhythm. No murmurs or rub
sounds present. No organomegaly. Extremities: No edema.

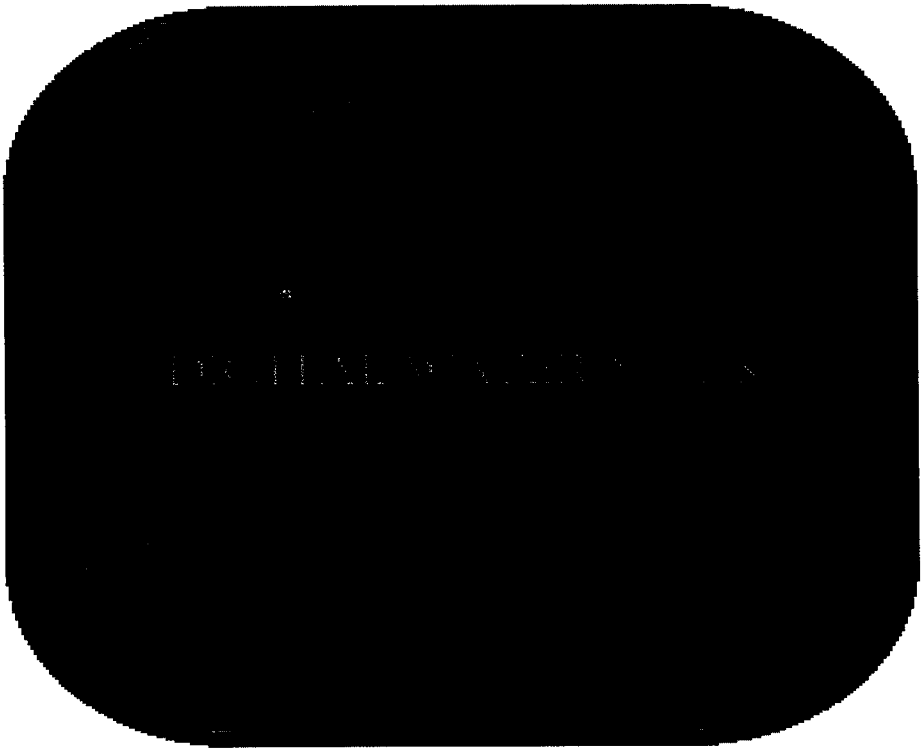
LABS: LFTs within normal limits, triglycerides 153, total cholesterol 184, HDL 35, LDL 1

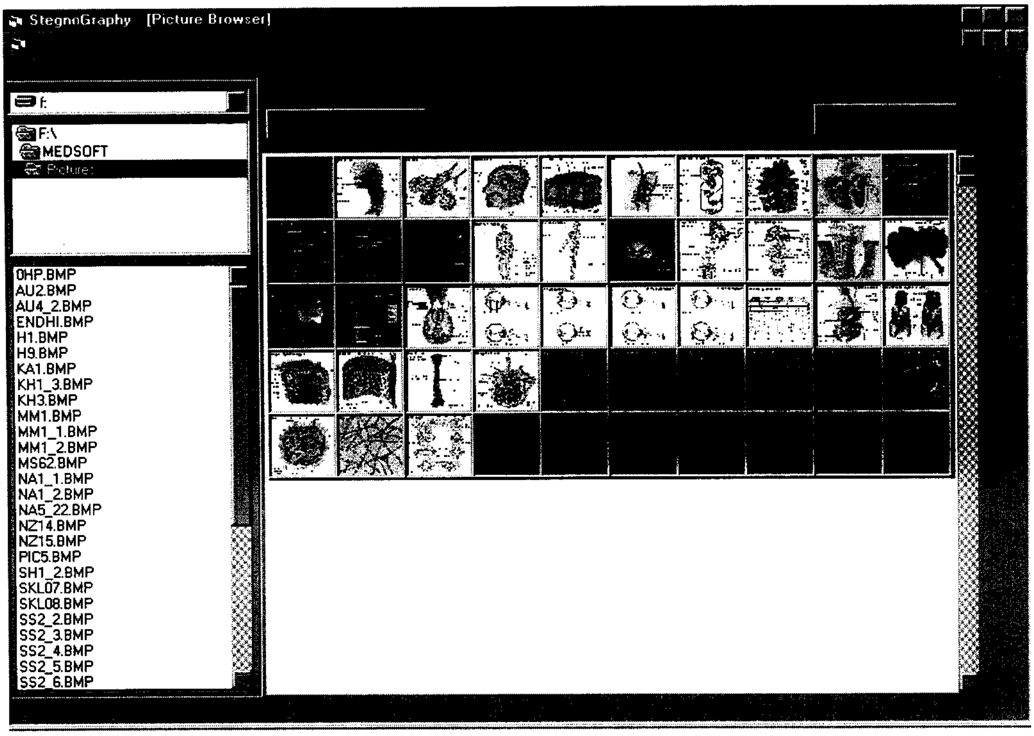
A: Hyperlipidemia, basically stable. I encouraged him to do some kind of exercise to im
keep the patient on current regimen and reassess.

P: Return to my clinic in 1 year with fasting lipid profile and LFTs.

○ Shuffle ○ Linear ● RN ○ Combination

	word
	a
	a
	a-
	aa
	ab-
	abampere
	abapical
	abarognosis
	abasia
	abasia trepidans
	abasia-astasia
	abasic
	abatic
	abaxial
	abaxile
	abciximab
	abdomen
	abdomin-
	abdominal
▶	
	abdominal aura
	abdominal cavity
	abdominal guarding
	abdominal hernia
	abdominal hysterectc
	abdominal hysterotor
	abdominal ostium of i



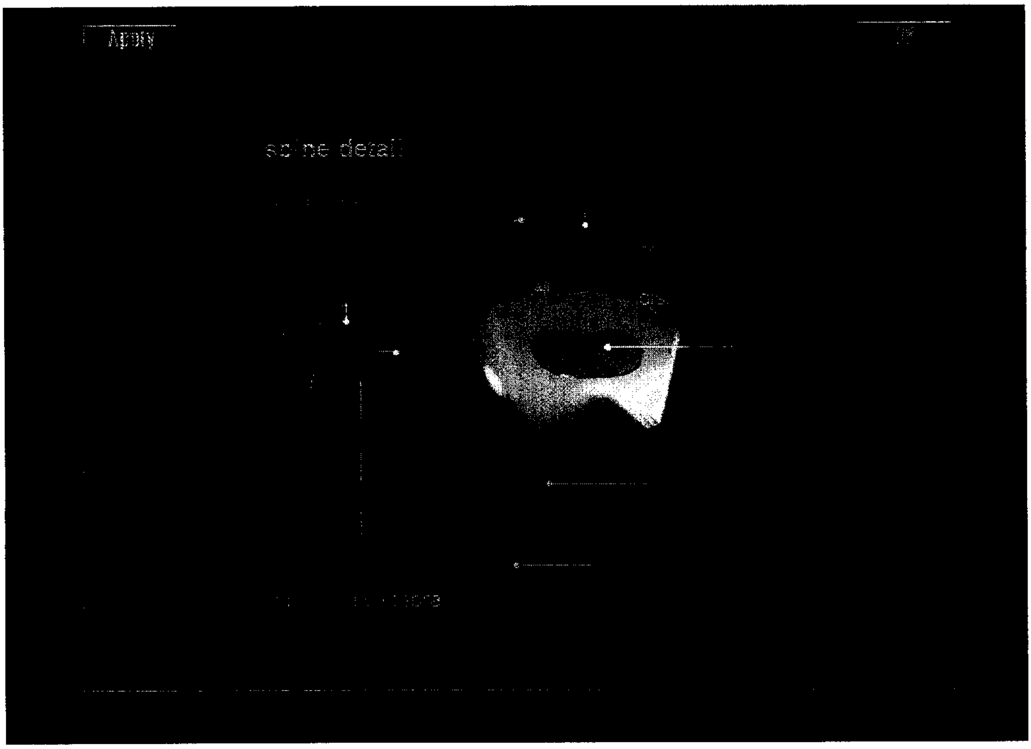


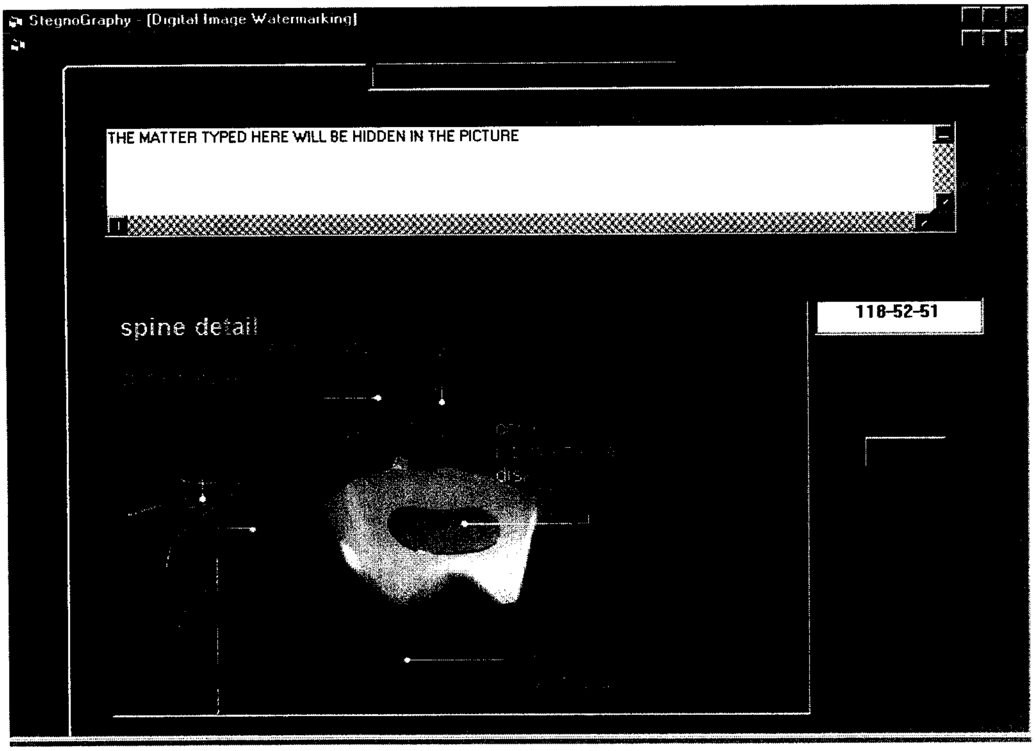
StegnoGraphy [Picture Browser]

f:

F:\
MEDSOFT
Picture

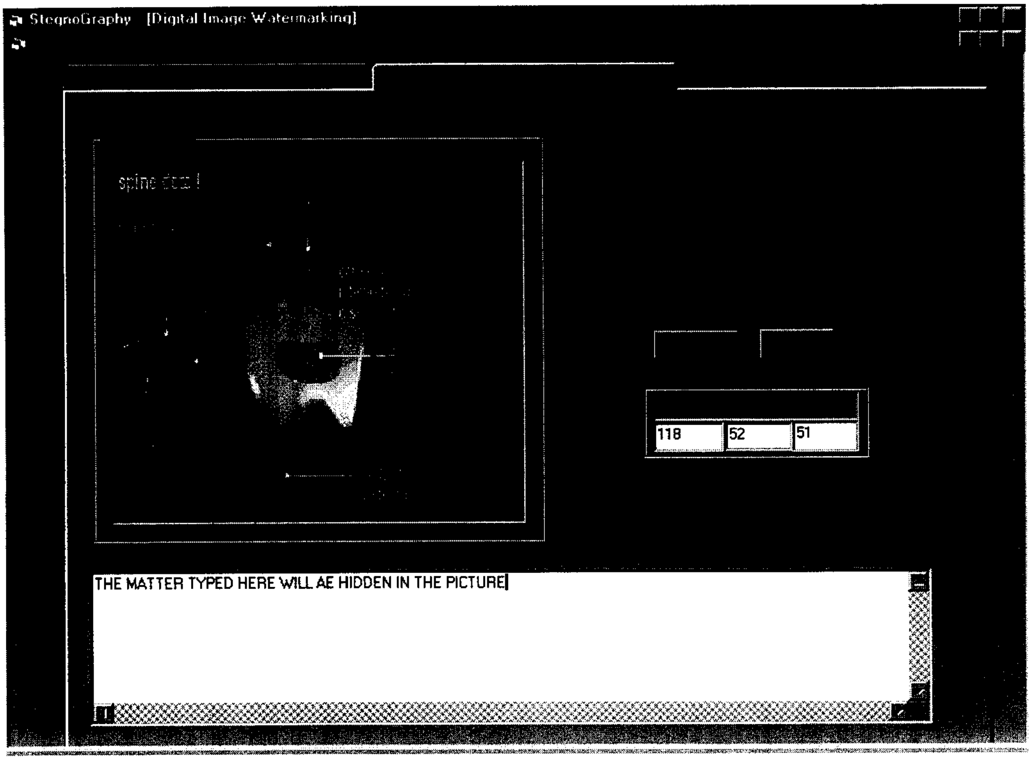
OHP.BMP
AU2.BMP
AU4_2.BMP
ENDHI.BMP
H1.BMP
H9.BMP
KA1.BMP
KH1_3.BMP
KH3.BMP
MM1.BMP
MM1_1.BMP
MM1_2.BMP
MS62.BMP
NA1_1.BMP
NA1_2.BMP
NA5_22.BMP
NZ14.BMP
NZ15.BMP
PIC5.BMP
SH1_2.BMP
SKL07.BMP
SKL08.BMP
SS2_2.BMP
SS2_3.BMP
SS2_4.BMP
SS2_5.BMP
SS2_6.BMP





THE MATTER TYPED HERE WILL BE HIDDEN IN THE PICTURE

118-52-51



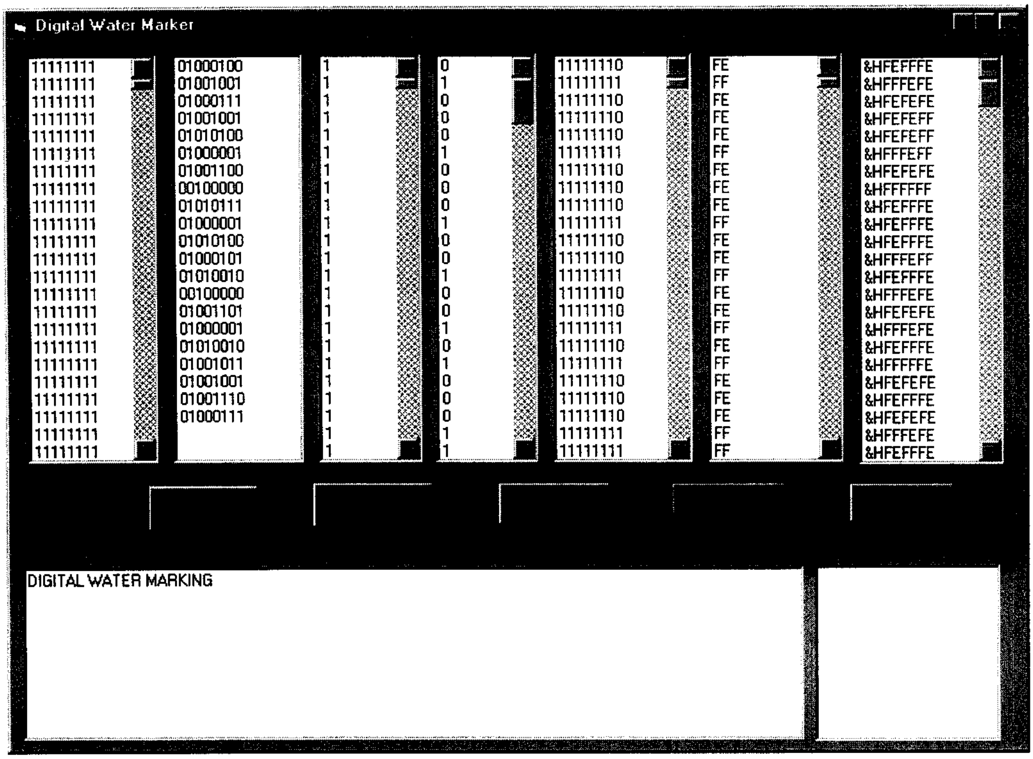
118	52	51

THE MATTER TYPED HERE WILL AE HIDDEN IN THE PICTURE

9.2 SAMPLE CODING:

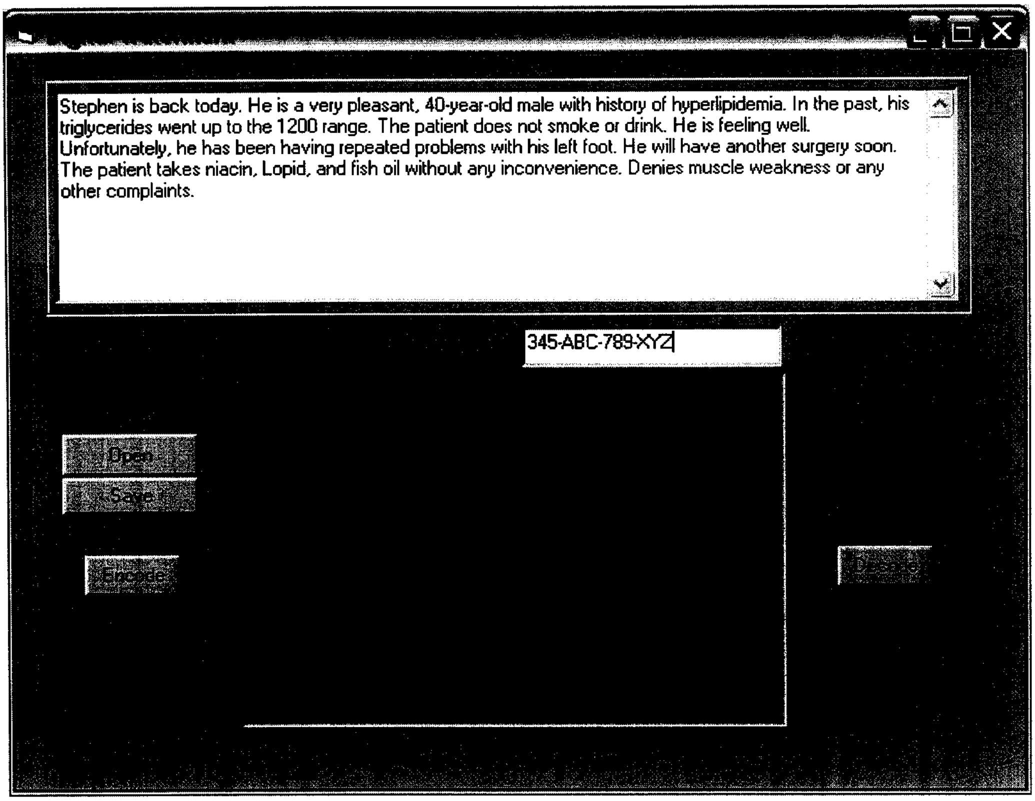
```
Private Declare Function GetPixel Lib "gdi32" (ByVal hdc As Long, ByVal x As Long,
ByVal y As Long) As Long
Private Declare Function SetPixel Lib "gdi32" (ByVal hdc As Long, ByVal x As Long,
ByVal y As Long, ByVal crColor As Long) As Long

Private Type BITMAPFILEHEADER
      bfType As Integer
      bfSize As Long
      bfReserved1 As Integer
      bfReserved2 As Integer
      bfOffBits As Long
End Type
Private Type BITMAPINFOHEADER '40 bytes
      biSize As Long
      biWidth As Long
      biHeight As Long
      biPlanes As Integer
      biBitCount As Integer
      biCompression As Long
      biSizeImage As Long
      biXPelsPerMeter As Long
      biYPelsPerMeter As Long
      biClrUsed As Long
      biClrImportant As Long
End Type
Dim h1 As BITMAPFILEHEADER
Dim h2 As BITMAPINFOHEADER
Dim pix As String * 1
Dim rgbentry As String * 3
Dim pic()
Dim ba() As String * 8
Dim rv, gv, bv
Dim bin As String
Dim hexval As String
Private Sub Command1_Click()
Dim a As String
Dim c As String
Dim i As Integer
a = Text1.text
For i = 1 To Len(a)
b = Hex(Asc(Mid$(a, i, 1)))
LUT (CStr(b))
List2.AddItem bin
```



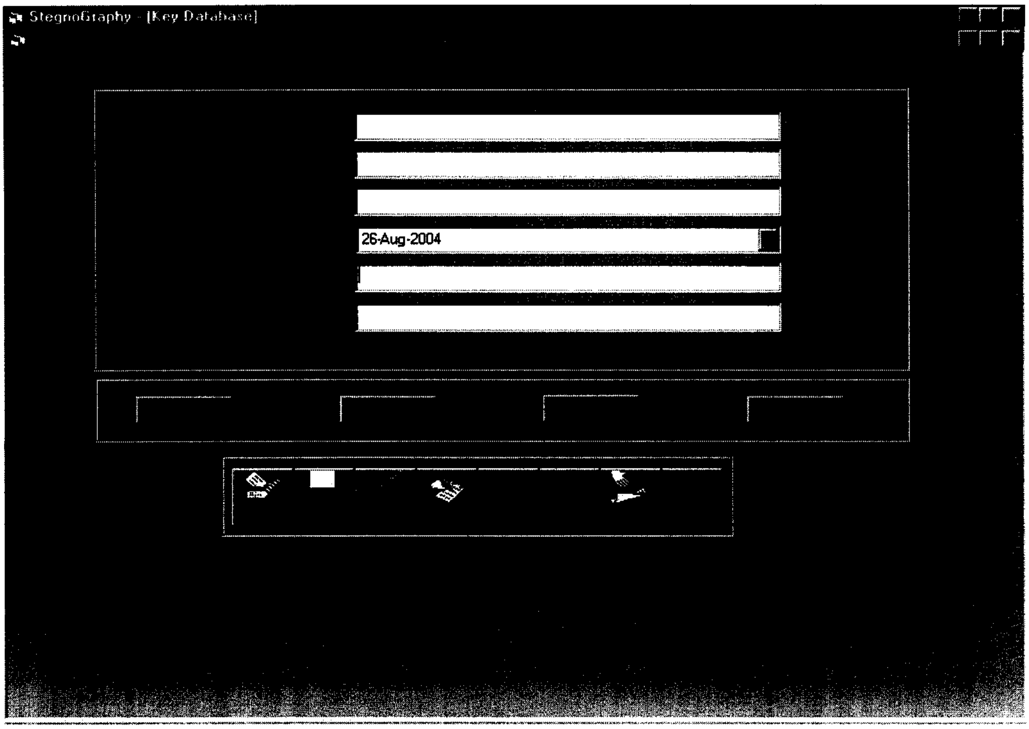
11111111	01000100	1	0	11111110	FE	&HFEFFFE
11111111	01001001	1	1	11111111	FF	&HFFFEFE
11111111	01000111	1	0	11111110	FE	&HFEFEFE
11111111	01001001	1	0	11111110	FE	&HFEFEFF
11111111	01010100	1	0	11111110	FE	&HFEFEFF
11111111	01000001	1	1	11111111	FF	&HFFFEFF
11111111	01001100	1	0	11111110	FE	&HFEFEFE
11111111	00100000	1	0	11111110	FE	&HFFFFFF
11111111	01010111	1	0	11111110	FE	&HFEFFFE
11111111	01000001	1	1	11111111	FF	&HFEFFFE
11111111	01010100	1	0	11111110	FE	&HFEFFFE
11111111	01000101	1	0	11111110	FE	&HFFFEFF
11111111	01010010	1	1	11111111	FF	&HFEFFFE
11111111	00100000	1	0	11111110	FE	&HFFFEFE
11111111	01001101	1	0	11111110	FE	&HFEFEFE
11111111	01000001	1	1	11111111	FF	&HFFFEFE
11111111	01010010	1	0	11111110	FE	&HFEFFFE
11111111	01001011	1	1	11111111	FF	&HFFFFFE
11111111	01001001	1	0	11111110	FE	&HFEFEFE
11111111	01001110	1	0	11111110	FE	&HFEFFFE
11111111	01000111	1	0	11111110	FE	&HFEFEFE
11111111		1	1	11111111	FF	&HFFFEFE
11111111		1	1	11111111	FF	&HFEFFFE

DIGITAL WATER MARKING



Stephen is back today. He is a very pleasant, 40-year-old male with history of hyperlipidemia. In the past, his triglycerides went up to the 1200 range. The patient does not smoke or drink. He is feeling well. Unfortunately, he has been having repeated problems with his left foot. He will have another surgery soon. The patient takes niacin, Lopid, and fish oil without any inconvenience. Denies muscle weakness or any other complaints.

345-ABC-789-XYZ



26-Aug-2004

```
Next i
End Sub

Private Sub cmdSave_Click()
SavePicture Picture2.Image, "C:\DWM.bmp"
MsgBox "saved"
End Sub

Private Sub Command3_Click()
Dim i As Long
For i = 0 To List1.ListCount - 1
List3.AddItem Right$(List1.List(i), 1)
Next i
End Sub

Private Sub Command4_Click()
For i = 0 To List2.ListCount
For j = 1 To 8
List4.AddItem Mid$(List2.List(i), j, 1)
Next j
Next i
For k = 0 To List1.ListCount - 1
If List4.List(k) <> "" Then
List5.AddItem Left$(List1.List(k), 7) & (List4.List(k))
Else
List5.AddItem List1.List(k)
End If
Next k
End Sub

Private Sub Command5_Click()
Dim i As Long
Dim j As Long
Dim h As String
For i = 1 To List5.ListCount
BINLUT List5.List(i - 1)
j = j + 1
   If j >= 3 Then
   h = hexval & h
   List7.AddItem "&H" & h
   j = 0
   h = ""
   Else
   h = hexval & h
   End If
```

```
List6.AddItem hexval
Next i

For k = 0 To Picture2.ScaleWidth
Picture2.PSet (k, 0), List7.List(k)
Next k
End Sub

Private Sub Command6_Click()
Dim i As Integer
Dim rv As Long
List1.Clear
For i = 0 To Picture3.ScaleHeight - 1
For j = 0 To Picture3.ScaleWidth - 1
rv = GetPixel(Picture3.hdc, j, i)
List1.AddItem Hex(rv)
Next j
Next i
End Sub

Private Sub Form_Load()
Show
Dim f As Integer
f = FreeFile
Open "C:\white1.bmp" For Binary As #f
Get #f, , h1
Get #f, , h2
xres = h2.biWidth
yres = h2.biHeight
ReDim pic(xres, yres, 2)
ReDim ba(xres * yres * 2) As String * 8
For i = 0 To yres
For j = 0 To xres
Get #f, , rgbentry
pic(j, i, 0) = Asc(Mid$(rgbentry, 3, 1)) 'red
pic(j, i, 1) = Asc(Mid$(rgbentry, 2, 1)) 'green
pic(j, i, 2) = Asc(Mid$(rgbentry, 1, 1)) 'blue
rv = Hex(pic(j, i, 0))
gv = Hex(pic(j, i, 1))
bv = Hex(pic(j, i, 2))
LUT (CStr(rv))
List1.AddItem bin
LUT (CStr(gv))
List1.AddItem bin
LUT (CStr(bv))
List1.AddItem bin
```

```
Next
  If Int((xres * 3) / 4) <> (xres * 3) / 4 Then
    For k = 1 To 4 - ((xres * 3) Mod 4)
    Get #f, , pix
    Next
  End If
Next
Close #f
MsgBox List1.ListCount
End Sub

Private Sub LUT(hexvalues As String)
Dim hb As String
Dim lb As String
Dim s As String
Dim t As String
hb = Left$(hexvalues, 1)
lb = Right$(hexvalues, 1)
s = ConvertToByte(hb)
t = ConvertToByte(lb)
bin = s & t
End Sub
Private Function ConvertToByte(hexval As String) As String
Select Case hexval
Case "0"
ConvertToByte = "0000"
Case "1"
ConvertToByte = "0001"
Case "2"
ConvertToByte = "0010"
Case "3"
ConvertToByte = "0011"
Case "4"
ConvertToByte = "0100"
Case "5"
ConvertToByte = "0101"
Case "6"
ConvertToByte = "0110"
Case "7"
ConvertToByte = "0111"
Case "8"
ConvertToByte = "1000"
Case "9"
ConvertToByte = "1001"
Case "A"
ConvertToByte = "1010"
```

```
Case "B"
ConvertToByte = "1011"
Case "C"
ConvertToByte = "1100"
Case "D"
ConvertToByte = "1101"
Case "E"
ConvertToByte = "1110"
Case "F"
ConvertToByte = "1111"
End Select
End Function

Private Function ConvertToHex(binval As String) As String
Select Case binval
Case "0000"
ConvertToHex = "0"
Case "0001"
ConvertToHex = "1"
Case "0010"
ConvertToHex = "2"
Case "0011"
ConvertToHex = "3"
Case "0100"
ConvertToHex = "4"
Case "0101"
ConvertToHex = "5"
Case "0110"
ConvertToHex = "6"
Case "0111"
ConvertToHex = "7"
Case "1000"
ConvertToHex = "8"
Case "1001"
ConvertToHex = "9"
Case "1010"
ConvertToHex = "A"
Case "1011"
ConvertToHex = "B"
Case "1100"
ConvertToHex = "C"
Case "1101"
ConvertToHex = "D"
Case "1110"
ConvertToHex = "E"
Case "1111"
```

```
ConvertToHex = "F"
End Select
End Function

Private Sub BINLUT(binvalues As String)
Dim hh As String
Dim hl As String
Dim s As String
Dim t As String
hh = Left$(binvalues, 4)
hl = Right$(binvalues, 4)
s = ConvertToHex(hh)
t = ConvertToHex(hl)
hexval = s & t
End Sub
```