NOVEL PASSWORD KEY TRANSFER METHOD FOR STEGANOGRAPHY

A PROJECT REPORT

Submitted by

Jagatheswari J	**71205104015**
Padmavathy S	**71205104028**

in partial fulfillment for the award of the degree

of

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

KUMARAGURU COLLEGE OF TECHNOLOGY, COIMBATORE

ANNA UNIVERSITY: CHENNAI 600025

APRIL 2009

ANNA UNIVERSITY: CHENNAI 600025

BONAFIDE CERTIFICATE

Certified that this project report **"NOVEL PASSWORD KEY TRANSFER METHOD FOR STEGANOGRAPHY"** is the bonafide work of **JAGATHESWARI.J , PADMAVATHY.S** who carried out the project work under my supervision.

S. Thangasamy

SIGNATURE
Dr.S.Thangasamy,
HEAD OF THE DEPARTMENT

Dept of CSE,
Kumaraguru College of Technology,
Coimbatore-641006

Rajini 23/04/09

SIGNATURE
Mrs.S.Rajini,
SUPERVISOR
Senior Lecturer,
Dept of CSE ,
Kumaraguru college of Technology,
Coimbatore-641006

The candidates with University Register Nos. **71205104015** , **71205104028** were examined by us in the project viva-voce examination held on..27-4-09

INTERNAL EXAMINER

EXTERNAL EXAMINER

ACKNOWLEDGEMENT

We are extremely grateful to **Prof. Annamalai, M.E,** Vice Principal, Kumaraguru College of Technology for having given us this opportunity to embark on this project.

We are deeply obliged to **Dr. S. Thangasamy, Ph.D.,** Head of the Department of Computer Science and Engineering for his valuable guidance and useful suggestions during the course of this project.

We wish to express our heartiest thanks to **Mrs.P.Devaki**, Assistant Professor, who helped us to overcome the perplexity while choosing the project.

We thank our guide **Ms.S.Rajini**, Senior Lecturer, Department of Computer Science and Engineering, for her excellent guidance in each and every step of our project and been with us to complete the project.

We thank the **teaching and non-teaching staff** of our department for providing us the technical support during the duration of our project.

We also thank all our **parents and friends** who helped us to complete this project successfully.

ABSTRACT

One of the methods introduced for establishing hidden communication is steganography. Steganography refers to a practice of hiding secret messages in communication over a public channel so that an eavesdropper cannot even tell that a secret messages is being sent. In contrast to the active literature proposing new concrete steganographic protocols and analyzing the existing protocols, there has been very little work on formalizing steganographic notions of security, and there are no complete rigorous proofs of security in a satisfying model. One of the problems in these methods is the security of transferring password key used for steganography between sender and receiver of secure data. In this project a new method is proposed for solving this problem using CAPTCHA method. In this method the password key is drawn into the CAPTCHA image. And this image is hidden in the cover image. Then the data are hidden in the image by this password key. The human receiver has to extract CAPTCHA image and recognize the password from the image and get the data from the cover image using this password. By this method the user need not memorize any password for extracting the data and also the password and the data are sent securely.

TABLE OF CONTENT

LIST OF DIAGRAMS

LIST OF ABBREVATIONS

LSB	-	Least Significant Bit
BMP	-	Bitmap image
CAPTCHA	-	Completely automatic Public Turing Test to Tell Computer Human Apart
OCR	-	Optical Character Recognition
IDE	-	Integrated Development Environment
JPEG	-	Joint Photographic Experts Group

INTRODUCTION

CHAPTER 1

INTRODUCTION

1.1 Problem Definition

One of the methods introduced for establishing hidden communication is steganography. The problems in these methods are the security of transferring password key used for steganography between sender and receiver of secure data. Here a new method called CAPTCHA is used for transferring the password key. CAPTCHA (Completely Automatic Public Turing Test to Tell Computer Human Apart) are the systems which are used to identify human beings and machines automatically. The password key is hidden in the image and data are hidden in the image using this password key. So the human receiver can recognize the password from the image and extract the data from the image using this password key.

1.2 Overview

Steganography is widely used for hidden exchange of information. Most Steganography jobs have been done on images, video clips, text, music and sound. Among the methods of steganography, the most common one is image steganography. In some image steganography methods, the data are hidden in the image using a password key and the receiver should know the password key for extracting data from the stego-image (the image which is contained the hidden data). One of the major problems is how to send the password for the receiver, because there is possibility of disclosure of password. For solving this problem, a new method for sending the stego-key (the password key which is used for hiding data in the image) to the receiver by using CAPTCHA method. CAPTCHA (Completely Automatic Public Turing Test to

Tell Computer and Human Apart) are systems which are used to identify human beings and machines automatically. These systems are based on Artificial Intelligence (AI) . They are similar to Turing test, but they differ in that the judge is a computer. The goal of these systems is to ask questions which human users can easily answer, while current computer programs cannot. In our method, the password key is hidden in image which is deformed to some extent. Then the data are hidden in the image by this key and the image is sent to the receiver. The receiver should recognize and type the displayed password to extract the data from the image. Since the present OCR programs cannot recognize the word, only a human user can recognize and type the displayed password.

1.2.1 Steganography

Although all digital file formats can be used for steganography, but the formats that are more suitable are those with with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Images comply with these requirements. And also the most cover media used for steganography is image. Since there is a large redundancy in the images and the possibility of hiding information in the images without attracting attention to human visual system. In these methods, the pixels of image are changed in order to hide the information so as not to be identifiable by human users and the changes are not tangible. Two major kinds of image steganography are: temporal and spatial domain methods.

Temporal Method: In this method, the data in question is added to quantities of luminosity of pixels in the image. This technique embeds messages in the intensity of the pixel directly. One of the common temporal methods is the least significant bit (LSB). LSB insertion is a common, simple approach to embedding information in a cover image. The least significant bit (in other words, 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message.

Spatial Domain Method: Another method is the calculation of conversion of frequency of the image and adding information in the frequency domain. A well-known method is to use the Discrete Fourier Transform (DFT) or the Discrete Cosine Transform (DCT) . Considering the use of exchange of cosine transform in JPEG image format, this method is good for the JPEG format.

1.2.2 CAPTCHA

CAPTCHA methods can be generally divided into two groups: OCR-based and Non-OCR-Based. In OCR-based methods, the image of a word is shown to user with distortion and various pictorial effects and the user must type that word. Due to the presence of various pictorial effects, the computer will encounter problems in the recognition of these words and only human users will be able to recognize the word. Examples of these methods include Scatter Type and Gimpy. But these methods usually result in dissatisfaction of users. In contrast, the Non-OCR-based methods which are easier to work with than OCR-based ones. Examples of these methods include Collage CAPTCHA and PIX .For example, in Collage CAPTCHA method image of some objects is shown with distortion and the user is asked to click on a certain object.

LITERATURE REVIEW

CHAPTER 2

LITERATURE REVIEW

2.1 EXISTING SYSTEM

Informally, steganography refers to the practice of hiding secret messages in communications over a public channel so that an eavesdropper who listens to all communications cannot even tell that a secret message is being sent. In contrast to the active literature proposing new concrete Steganographic protocols and analyzing as in existing protocols, there has been very little work on formalizing Steganographic notions of security, and none giving complete, rigorous proofs of security in a satisfying model. In this method, the main purpose is to hide data in a cover media so that other persons will not notice the presence of such data. Most steganography jobs have been done on images, video clips, text, music and sound. In practice, there are basically three types of steganographic protocols used.

They are Pure Steganography, Secret Key Steganography and Public Key Steganography. Pure Steganography is defined as a steganographic system that does not require the exchange of a cipher such as a stego-key. This method of Steganography is the least secure means by which to communicate secretly because the sender and receiver can rely only upon the presumption that no other parties are aware of this secret message.

Secret Key Steganography is defined as a steganographic system that requires the exchange of a secret key (stego-key) prior to communication. Secret Key Steganography takes a cover message and embeds the secret message inside of it by using a secret key (stego-key). Only the parties who know the secret key can reverse the process and read the secret message. Unlike Pure Steganography where a perceived invisible communication channel is present, Secret Key

Steganography exchanges a stego-key, which makes it more susceptible to interception. The benefit to Secret Key Steganography is even if it is intercepted; only parties who know the secret key can extract the secret message.

Public Key Steganography takes the concepts from Public Key Cryptography as explained below. Public Key Steganography is defined as a steganographic system that uses a public key and a private key to secure the communication between the parties wanting to communicate secretly. The sender will use the public key during the encoding process and only the private key, which has a direct mathematical relationship with the public key, can decipher the secret message.

One of the problems in these methods is the security of transferring password key used for steganography between sender and receiver of secure data and how to send the password for the receiver, because there is possibility of disclosure of password. In the existing method, the user has to memorize the key and there is a need for a trusted channel to send the password to the receiver. Hence it will not be a secured one, since the hackers may hack the key. This may down the usage of stegnography.

In order to overcome these disadvantages, a new method is proposed for sending the password key securely to the receiver by using CAPTCHA method.

2.2 PROPOSED SYSTEM

In existing method there is no trusted channel for sending the password key to receiver. In this project a new method is proposed for sending the key to the receiver by using CAPTCHA method.

CAPTCHA methods can be generally divided into two groups: OCR-based and Non-OCR-Based. In OCR-based methods, the image of a word is shown to user with distortion and various pictorial effects and the user must type that word. Due to the presence of various pictorial effects, the computer will encounter problems in the recognition of these words and only human users will be able to recognize the word. Examples of these methods include Scatter Type and Gimpy. In Non-OCR-based methods which are easier to work with than OCR-based ones. Examples of these methods include Collage CAPTCHA and PIX .For example, in Collage CAPTCHA method image of some objects is shown with distortion and the user is asked to click on a certain object.

Since our focus is on the transferring of the password key, therefore we are using a simple LSB (Least Significant Bits) method for steganography, and invisible water marking algorithm for hiding CAPTCHA image. In LSB method each byte of information is hidden in two pixels. Before hiding the data in the image, first the password key is selected. Then the password key is converted to an image. Two methods are used for using a password as CAPTCHA image.

- Random CAPTCHA generation.
- User key to CAPTCHA image.

In random CAPTCHA generation method, the CAPTCHA image is generated randomly every time it is used. The sender can use this image as the password key. In this, the sender itself came to know the password at the moment of sending. And hence there is no way of guessing the password of the sender. Based on the sender convenience, the difficulty level can also set to the CAPTCHA generation.

In user key to CAPTCHA image method, the sender can convert his own password key into a CAPTCHA image. For this the password key is drawn in a crooked shape. For preparing this image, each character of the password key is written with a random font and a random degree of skew in the image.

Then this CAPTCHA image is hidden using the invisible water marking algorithm. Now the data are hidden in the cover image by using the password key and sent to the receiver. The receiver has to extract this CAPTCHA image and recognize the password from the image. By entering the extracted password the user can get hidden data from the cover image.

In this project, the cover media used for hiding data is image - image stenography. Since there is a large redundancy in the images and the possibility of hiding information in the images without attracting attention to human visual system. In these methods, the pixels of image are changed in order to hide the information so as not to be identifiable by human users and the changes are not tangible.

The cover image used must be in BMP format. Hence When embedding a message in a "raw" image, that has not been changed with compression, such as a BMP, there exits a trade-off between the invisibility of the message and the amount of information that can be embedded. BMP is capable of hiding quite a large message.

SYSTEM REQURIMENTS

CHAPTER 3

SYSTEM REQUIREMENTS

3.1 HARDWARE SPECIFICATIONS

Processor	:	Intel Pentium IV 3.0 GHz
RAM	:	512 MB RAM
Hard Disk	:	80 GB Hard Disk
CD Drive	:	52 * CD Drive
Key Board	:	114 Keys Keyboard
Monitor	:	15' CRT / TFT
Mouse	:	Optical Mouse

3.2 SOFTWARE SPECIFICATIONS

Operating System	:	Windows XP
Front End	:	Microsoft Visual Studio .NET 2008
Coding Language	:	Visual C# .NET

3.3 SYSTEM ENVIRONMENT

3.3.1 Introduction to .NET

Visual Studio .NET is a complete set of development tools for building ASP Web applications, XML Web services, desktop applications, and mobile applications. Visual Basic .NET, Visual C++ .NET, and Visual C# .NET. All use the same integrated development environment (IDE), which allows them to share tools and facilitates in the creation of mixed-language solutions. In addition, these languages leverage the functionality of the .NET Framework, which provides access to key technologies that simplify the development of ASP Web applications and XML Web services.

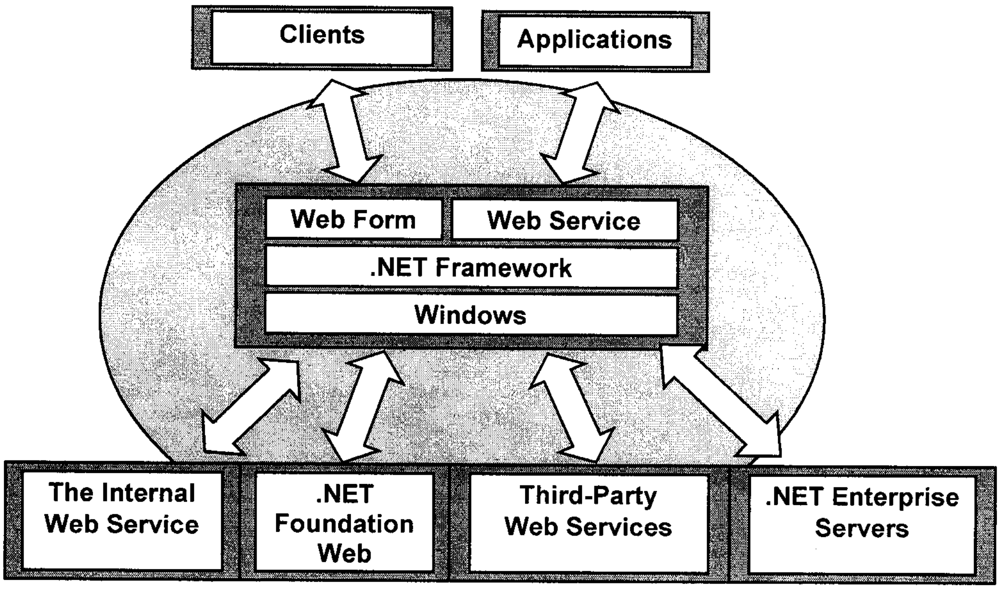


Figure 3.3.1a Components of visual studio .NET

Visual Studio .NET Highlights

This section contains information about some of the latest features available in this release of Visual Studio.

Language Enhancements

Microsoft Visual Basic, Microsoft C++, and Microsoft JScript have all been updated to meet the development needs. Additionally, a new language, Microsoft C#, has been introduced. These languages leverage the functionality of the .NET

Framework, which provides access to key technologies that simplify the development of ASP Web applications and XML Web services.

Visual Basic

Visual Basic has been updated to include many new and improved language features that make it a powerful object-oriented programming language. These features include inheritance, interfaces, and overloading, among others. Visual Basic also now supports structured exception handling, and custom attributes.

C#

Visual C#, pronounced C sharp, is a new object-oriented programming language that is an evolution of C and C++, providing a simple and type-safe language for developing applications.

C++

Managed Extensions for C++ and attributed programming are just some of the enhancements made to the C++ language. Managed Extensions simplify the task of migrating existing C++ applications to the new .NET Framework. Attributes, like C++ keywords, are used in the source files and interpreted by the compiler.

Jscript

JScript has been updated to be a class-based, object-oriented scripting language that maintains full backwards compatibility. JScript now provides class-based objects, typed variables, true compiled code, and cross-language support through Common Language Specification (CLS) compliance. The primary role of JScript is development of Web sites with ASP.NET and customization of applications with Script for the .NET Framework.

Web Forms

Web Forms are an ASP.NET technology that are use to create programmable Web pages. Web Forms render themselves as browser-compatible HTML and script, which allows any browser on any platform to view the pages. Using Web Forms, we can create Web pages by dragging and dropping controls onto the designer and then adding code, similar to the way that we create Visual Basic forms.

Windows Forms

Windows Forms is the new platform for Microsoft Windows application development, based on the .NET Framework. This framework provides a clear, object-oriented, extensible set of classes that enables to develop rich Windows applications.

XML Web Services

XML Web services are applications that can receive requests and data using XML over HTTP. XML Web services are not tied to a particular component technology or object-calling convention and can therefore be accessed by any language, component model, or operating system. In Visual Studio .NET, we can quickly create and include XML Web services using Visual Basic, Visual C#, JScript, Managed Extensions for C++, or ATL Server.

XML Support

Extensible Markup Language (XML) provides a method for describing structured data. XML is a subset of SGML that is optimized for delivery over the Web. The World Wide Web Consortium (W3C) defines XML standards so that structured data will be uniform and independent of applications. Visual Studio .NET fully supports XML, providing the XML Designer to make it easier to edit XML and create XML schemas.

3.3.2 The .NET Framework

The .NET Framework is a multi-language environment for building, deploying, and running XML Web services and applications. It consists of three main parts:

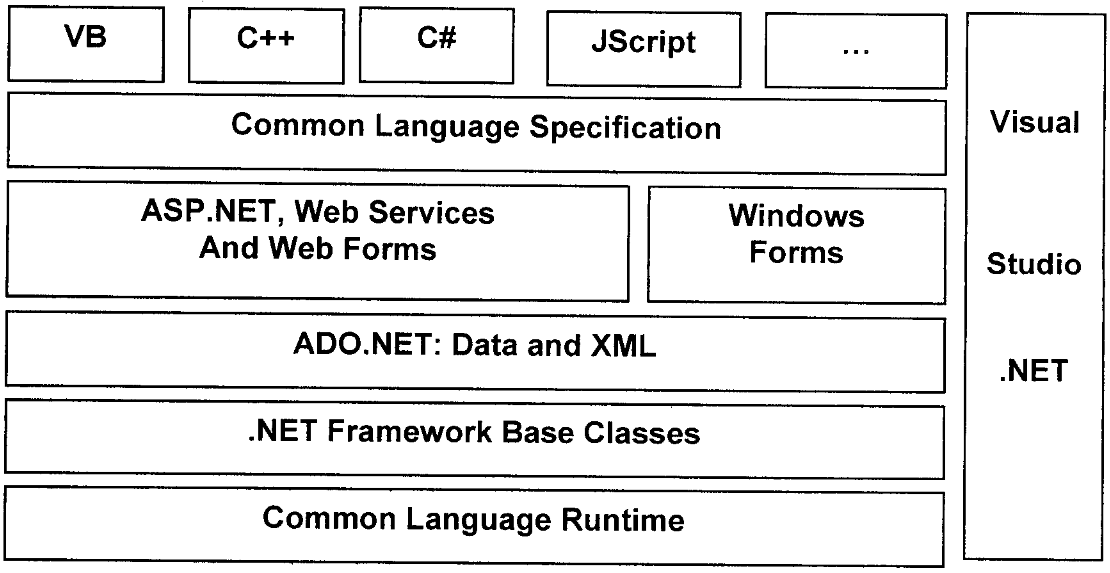


Figure 3.3.2a The .NET framework

Common Language Runtime

Despite its name, the runtime actually has a role in both a component's runtime and development time experiences. While the component is running, the runtime is responsible for managing memory allocation, starting up and stopping threads and processes, and enforcing security policy, as well as satisfying any dependencies that the component might have on other components.

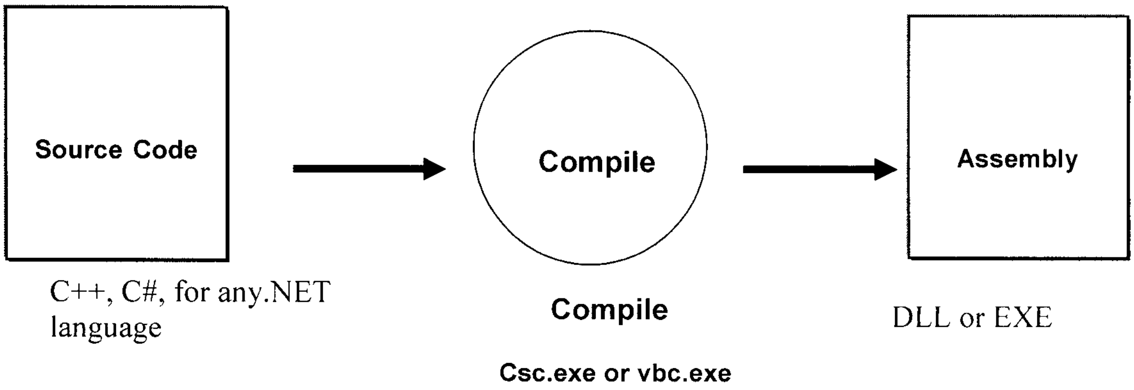


figure 3.3.2b Common Language Runtime Compilation

Unified programming classes

The framework provides developers with a unified, object-oriented, hierarchical, and extensible set of class libraries (APIs). Currently, C++ developers use the Microsoft Foundation Classes and Java developers use the Windows Foundation Classes. The framework unifies these disparate models and gives Visual Basic and JScript programmers access to class libraries as well.

ASP.NET

ASP.NET builds on the programming classes of the .NET Framework, providing a Web application model with a set of controls and infrastructure that make it simple to build ASP Web applications. ASP.NET includes a set of controls that encapsulate common HTML user interface elements, such as text boxes and drop-down menus. These controls run on the Web server, however, and push their user interface as HTML to the browser.

ADO.NET

To move data between a data store and the application, we must first have a connection to the data store. In ADO.NET it is able create and manage a connection using one of two connection objects:

SYSTEM ANALYSIS

CHAPTER 4
SYSTEM ANALYSIS

4.1 USE CASE DIAGRAM

SENDER USE CASE DIAGRAM

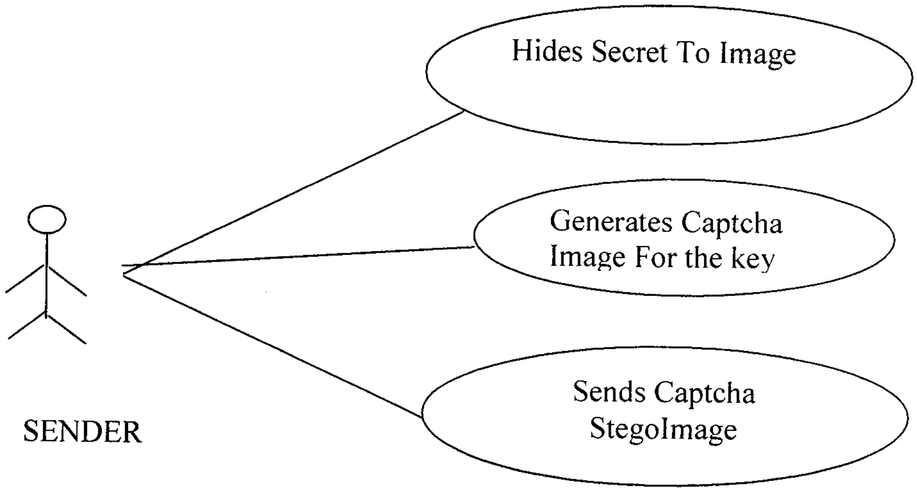


Figure 4.1a Sender use case diagram

The sender first generates the CAPTCHA image , and hides the secret text by CAPTCHA image in the original image.Sender sends the stegoimage to the receiver.

RECEIVER USE CASE DIAGRAM

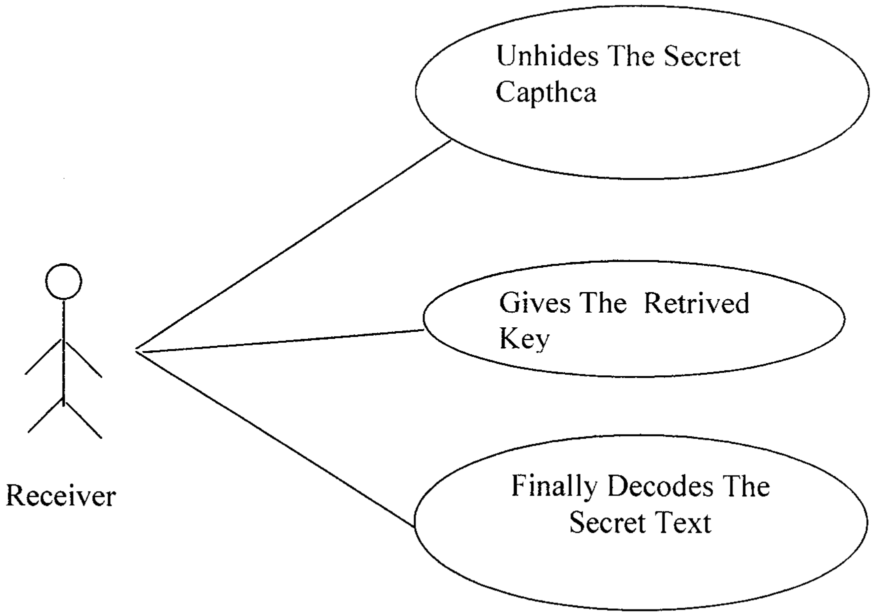


Figure 4.1b Receiver use case diagram

Receiver unhides the password key(CAPTCHA image) and then extract the secret text by using the CAPTCHA image.

4.2 System Design

Over All Encoding:

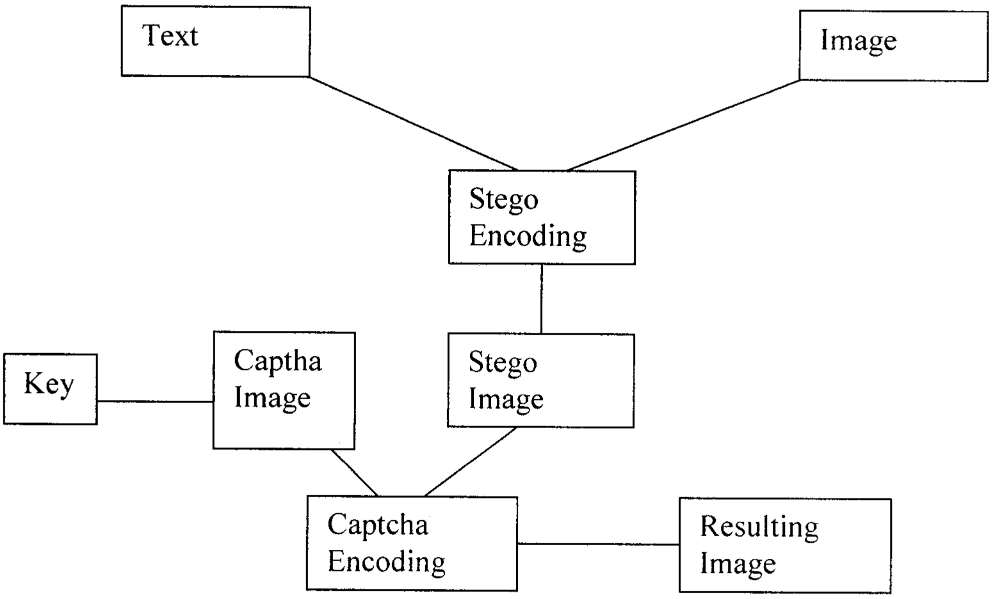


Figure 4.2a Over all encoding

First the text is embedded in the image and the resulting image is stego-image. Then the password key is converted into a CAPTCHA image. The CAPTCHA image is hidden in the stego-image.

Over All Decoding :

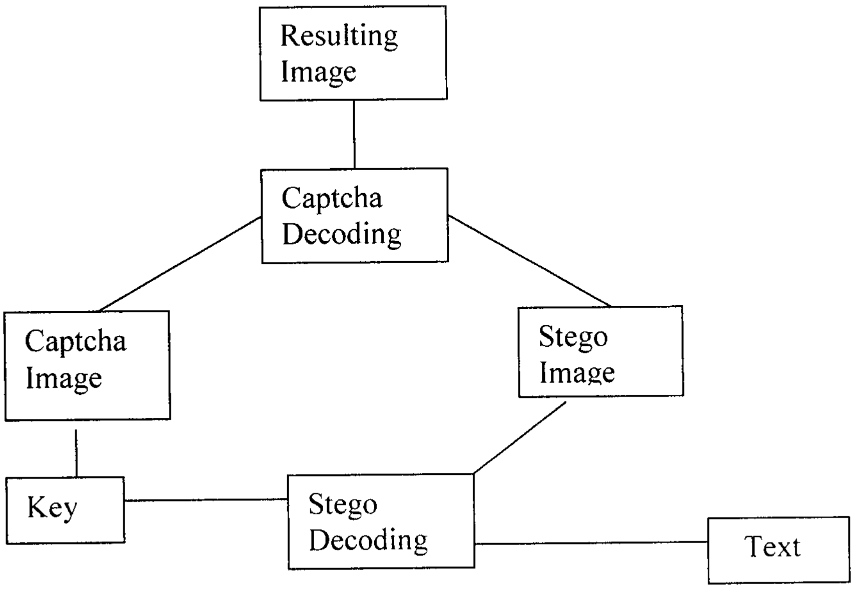


Figure 4.2b Over all decoding

In the receiver end, the CAPTCHA image and the stego-image will be separated by CAPTCHA decoding process. From the CAPTCHA image the receiver can extract the password key. On entering this key, the secret text can be retrieved.

4.3 Modules

Stego Encoding:

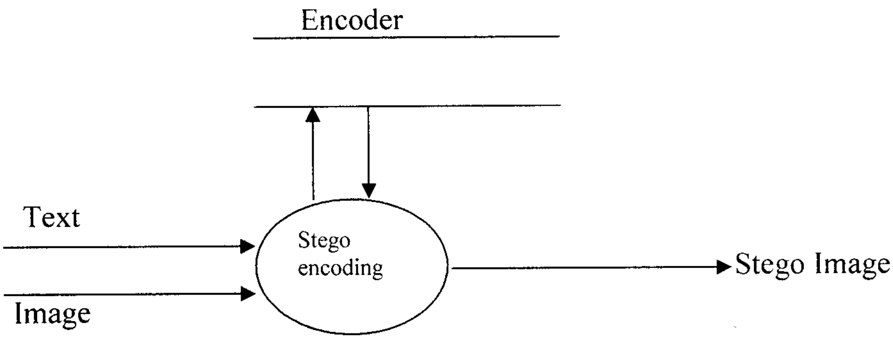


Figure 4.3a Stego encoding

Stego encoding is the process of hiding the secret text in the image.this embedded image is called as stegoimage.

CAPTCHA Encoding:

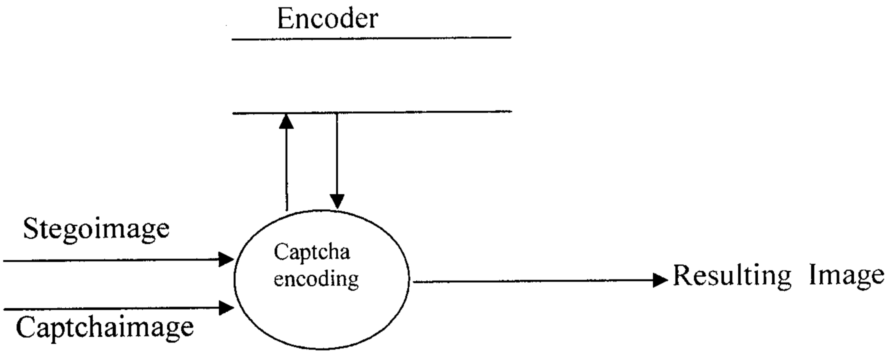


Figure 4.3b CAPTCHA encoding

The CAPTCHA encoding is the process of hiding the CAPTCHA image into the stegoimage.

CAPTCHA Decoding:

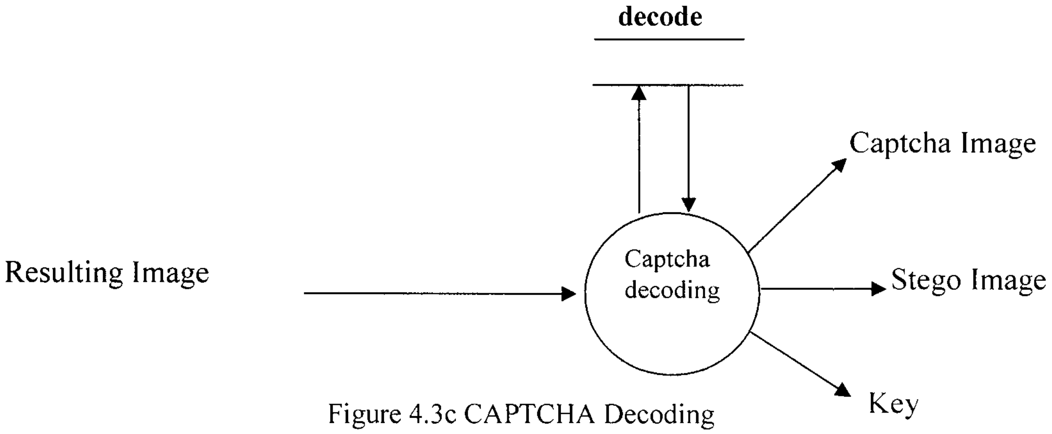


Figure 4.3c CAPTCHA Decoding

CAPTCHA decoding is the process of segregating the CAPTCHA image(key), stego image from the resulting image.

Stego Decoding:

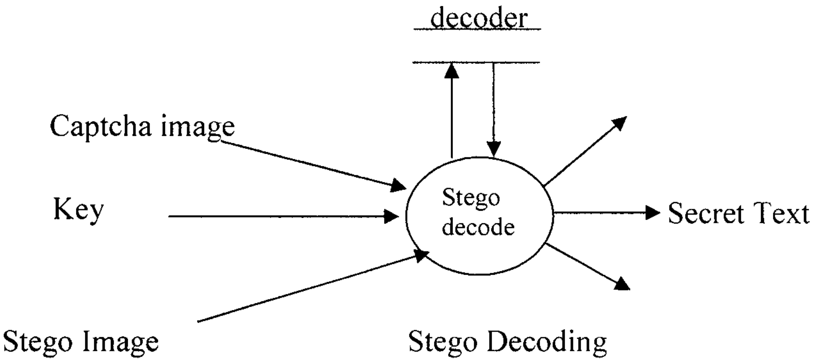
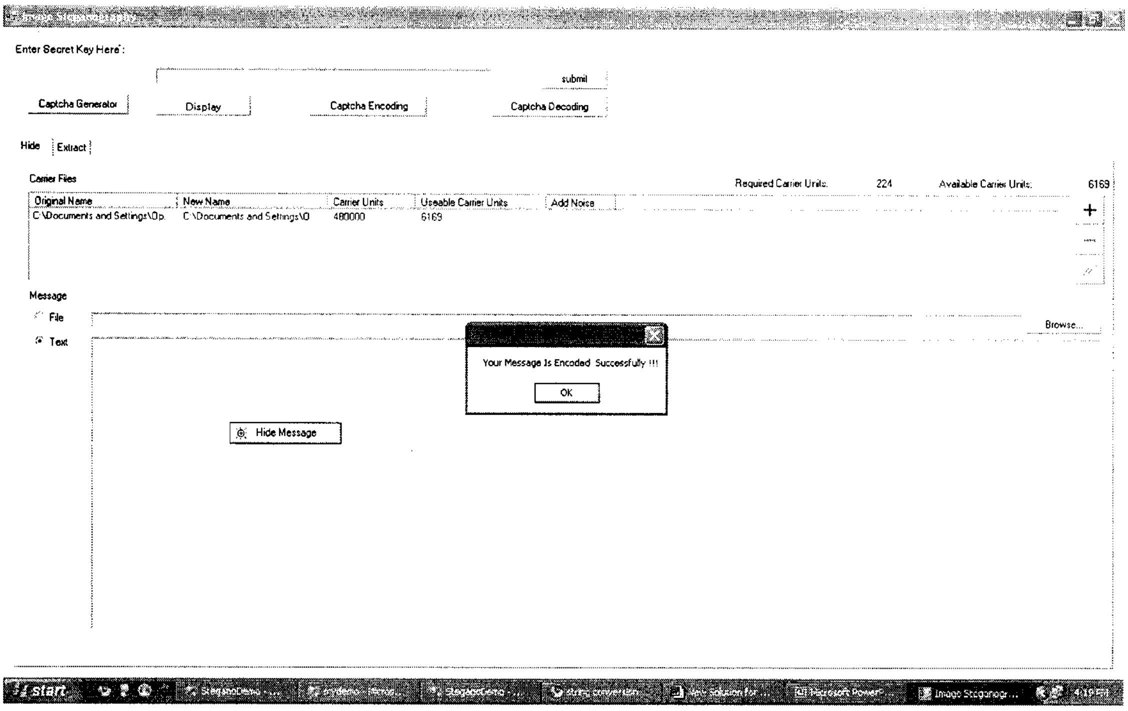


Figure 4.3d Stego Decoding

Stego decoding is the process of extracting the secret text from the stegoimage by giving the CAPTCHA image as input.

4.4 System Implementation

Stego Encoding :



Required Carrier Units: 224 Available Carrier Units: 6169

Original Name	New Name	Carrier Units	Useable Carrier Units	Add Noise
C:\Documents and Settings\Op.	C:\Documents and Settings\O	480000	6169	

Your Message Is Encoded Successfully !!!

Figure 4.4a stego encoding

Using the captcha generator, a captcha image is generated. And key Is given based on that image. Then a given is given as input. The secret text to be hidden is then given. Then as a result of Stego Encoding , the secret text is encoded with the input image which is given.

Captcha Encoding :

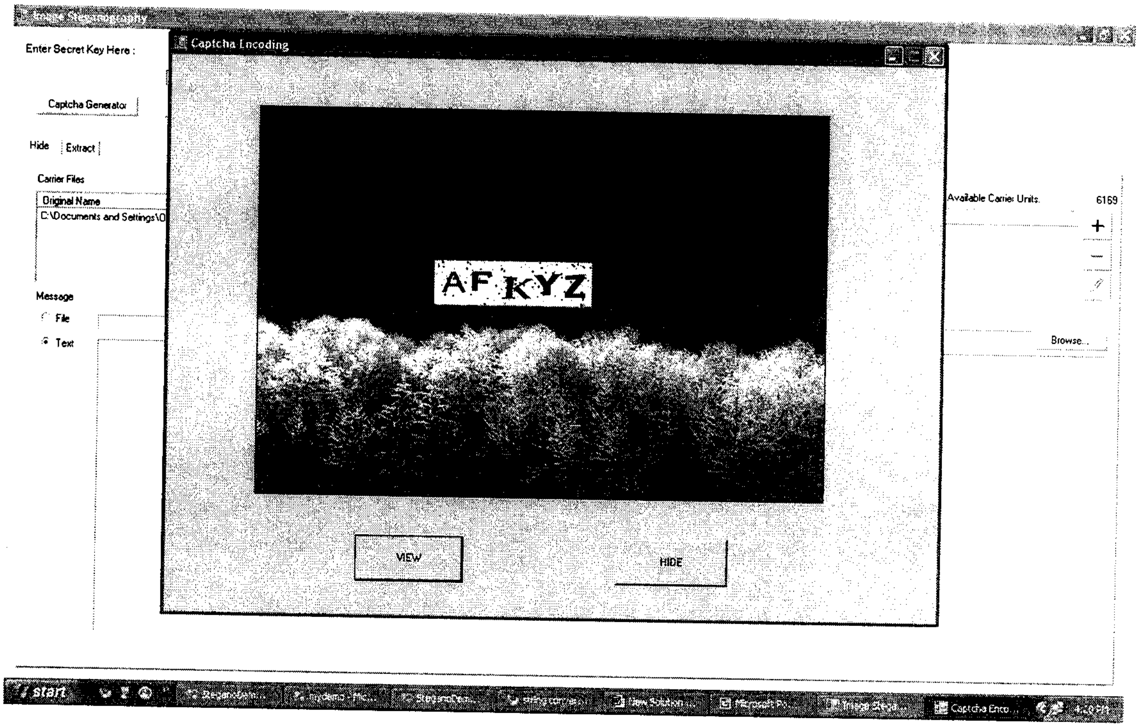


Figure 4.4b CAPTCHA encoding

After the process of Stego Encoding, Image comparisons are made.Then During the captcha Encoding phase, the captcha image is watermarked with the Stego image. Then after that, it is hidden securely so that no interruption can be made.

Captcha Decoding :

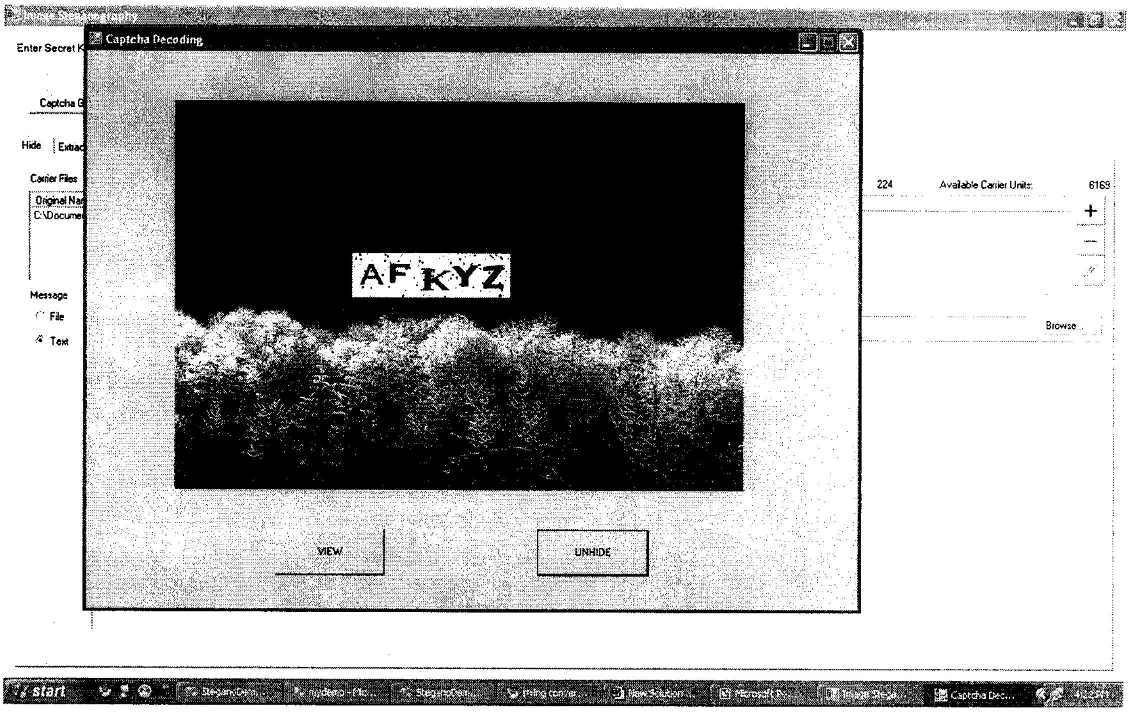
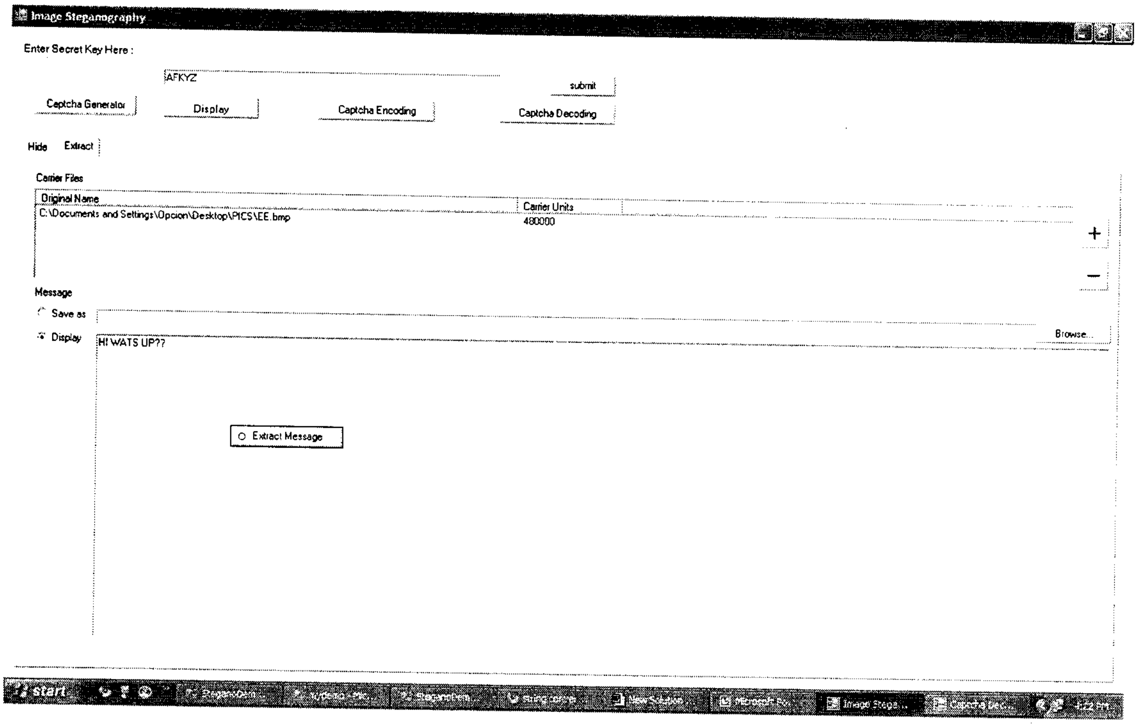


Figure 4.4c CAPTCHA decoding

In the CAPTCHA encoding phase , CAPTCHA image is watermarked with the image. In the CAPTCHA decoding phase , the hidden image is unhidden by the decoder. Now the decoder is ready with the secret Key. He is ready to retrieve the data.

Stego Decoding :



Enter Secret Key Here : AFKYZ

Carrier Files

Original Name	Carrier Units
C:\Documents and Settings\Opcion\Desktop\PICS\EE.bmp	480000

Message

○ Save as

● Display HI WATS UP??

Figure 4.4d Stego decoding

Finally in the stego decoding phase, the secret key is given as input and the stego image is also given as input. Now the secret text is retrieved safely.

4.5 RESULTS AND DISCUSSIONS

The secret text will be hidden in the original image by using the password key. This password key can be generated by Random CAPTCHA image generation method and User key to CAPTCHA image method. The secret message is either a file or text. Then the secret message will be embedded in the original image by CAPTCHA image. The resulting image is known as stego-image. In the random CAPTCHA image generation method the complexity level of the password key can be varied. In the receiver side first the CAPTCHA decoding process will be performed and the password key will be extracted. By giving this password key as an input the secret message can be extracted.

CONCLUSION

CHAPTER 5
CONCLUSION

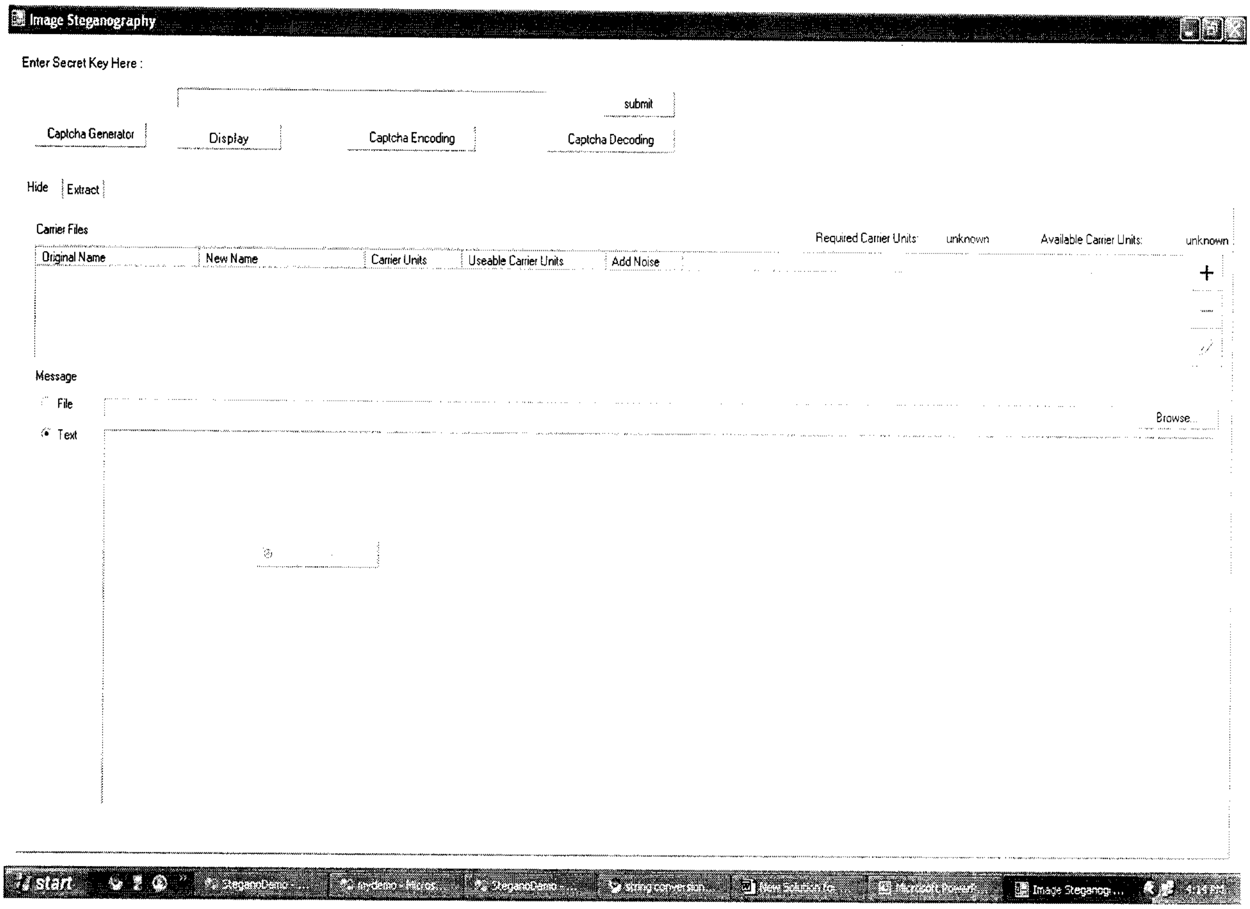
In this project a new method for secure transferring of password key in image steganography methods has been introduced. For this purpose the CAPTCHA method is used. In this method the password key which is used in steganography is hidden in the image, so there is no need for a trusted channel for sending the password key and the password is sent along with the image. Therefore there is no need to memorize the password. This method can also be used on other devices such as mobile phones and Pocket PCs. In addition to color images, this method can also be applied for grayscale and binary images. Only a human can extract the password from the image. Due to high cost of human employment and low speed in examining the images, the probability of finding the password key and the text hidden in the images is low.

APPENDIX

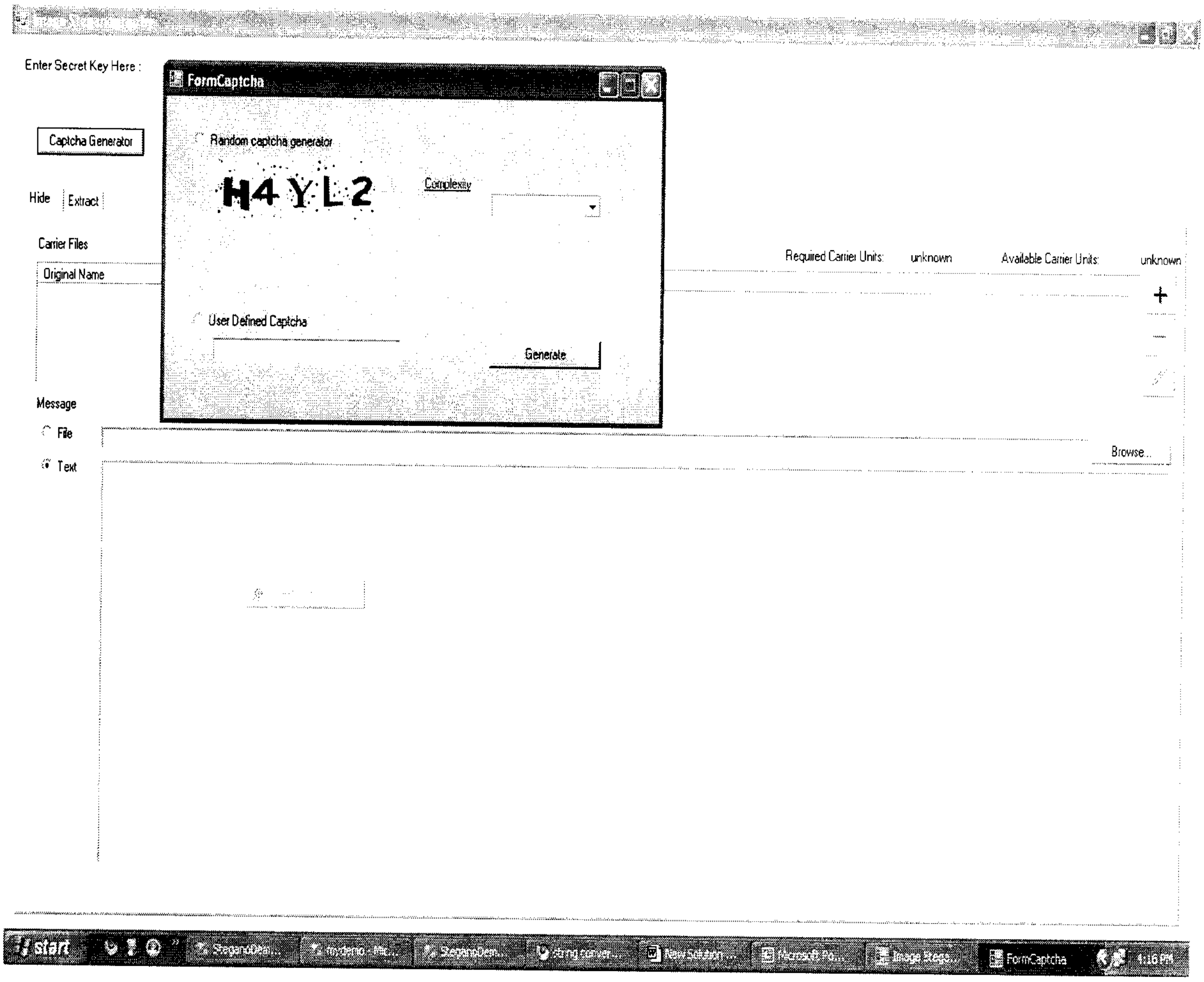
APPENDIX

SENDER SIDE

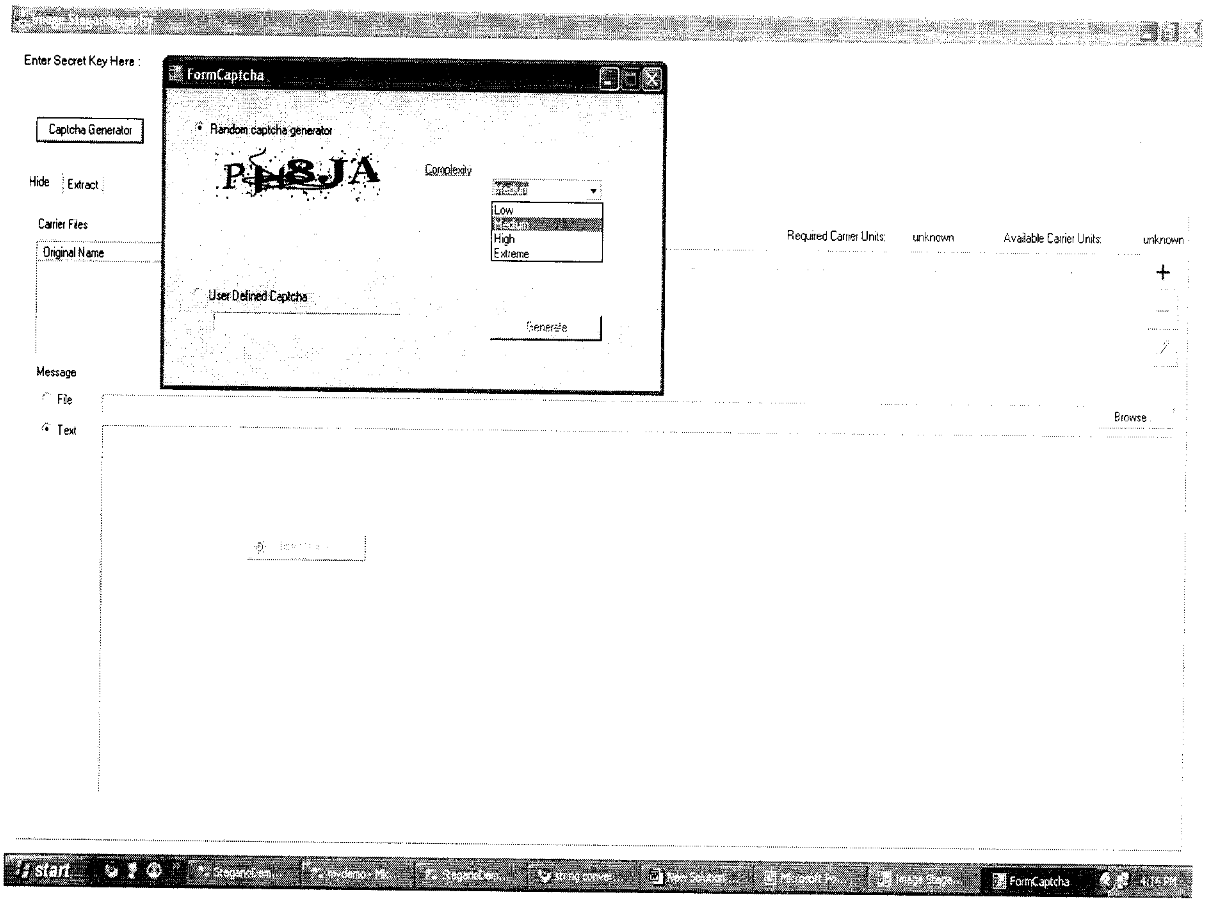
USER INTERFACE



CAPTCHA GENERATION



SETTING COMPLEXITY FOR CAPTCHA



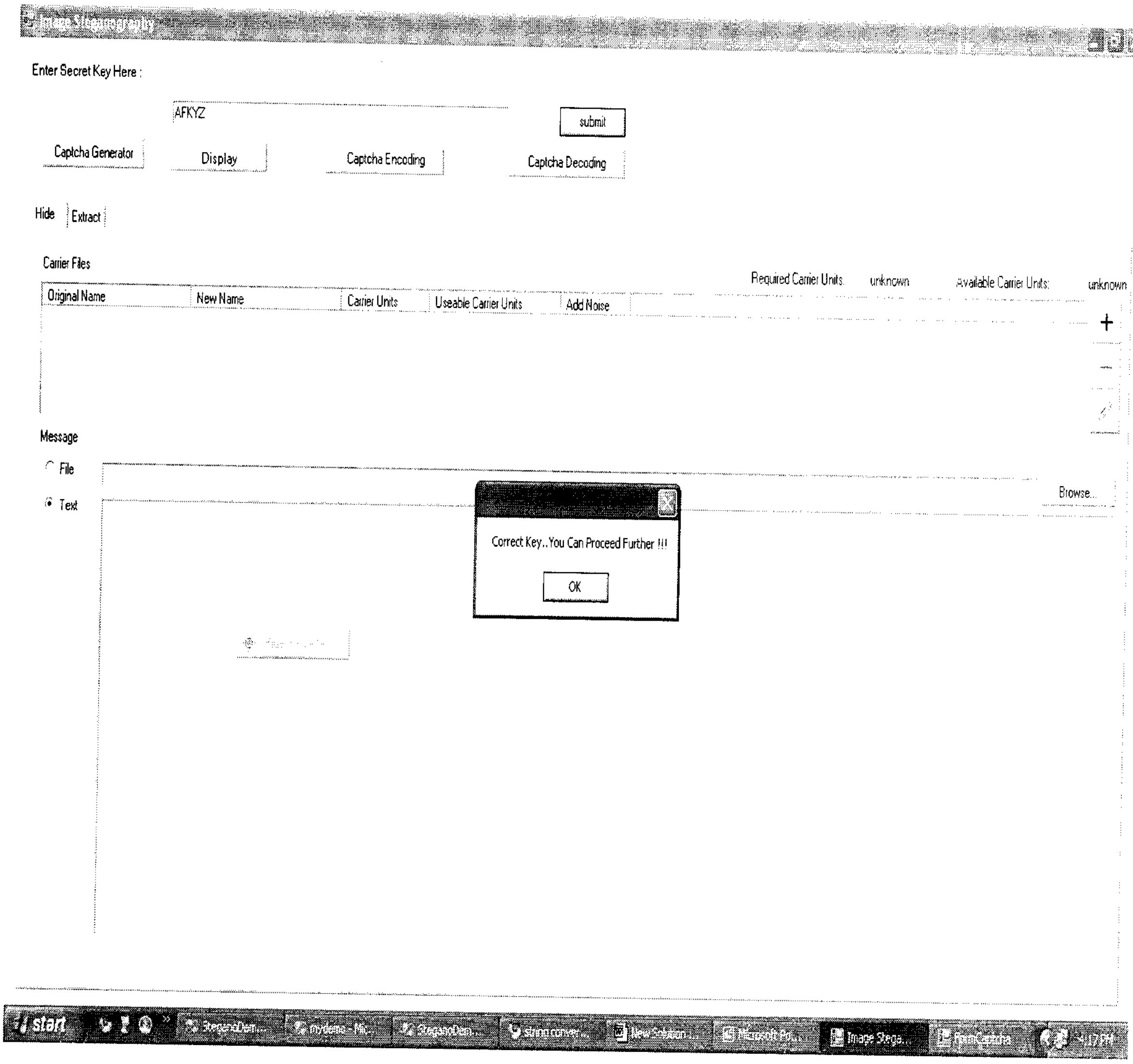
● Random captcha generator

Complexity: Medium

○ User Defined Captcha

Message: ○ File ● Text

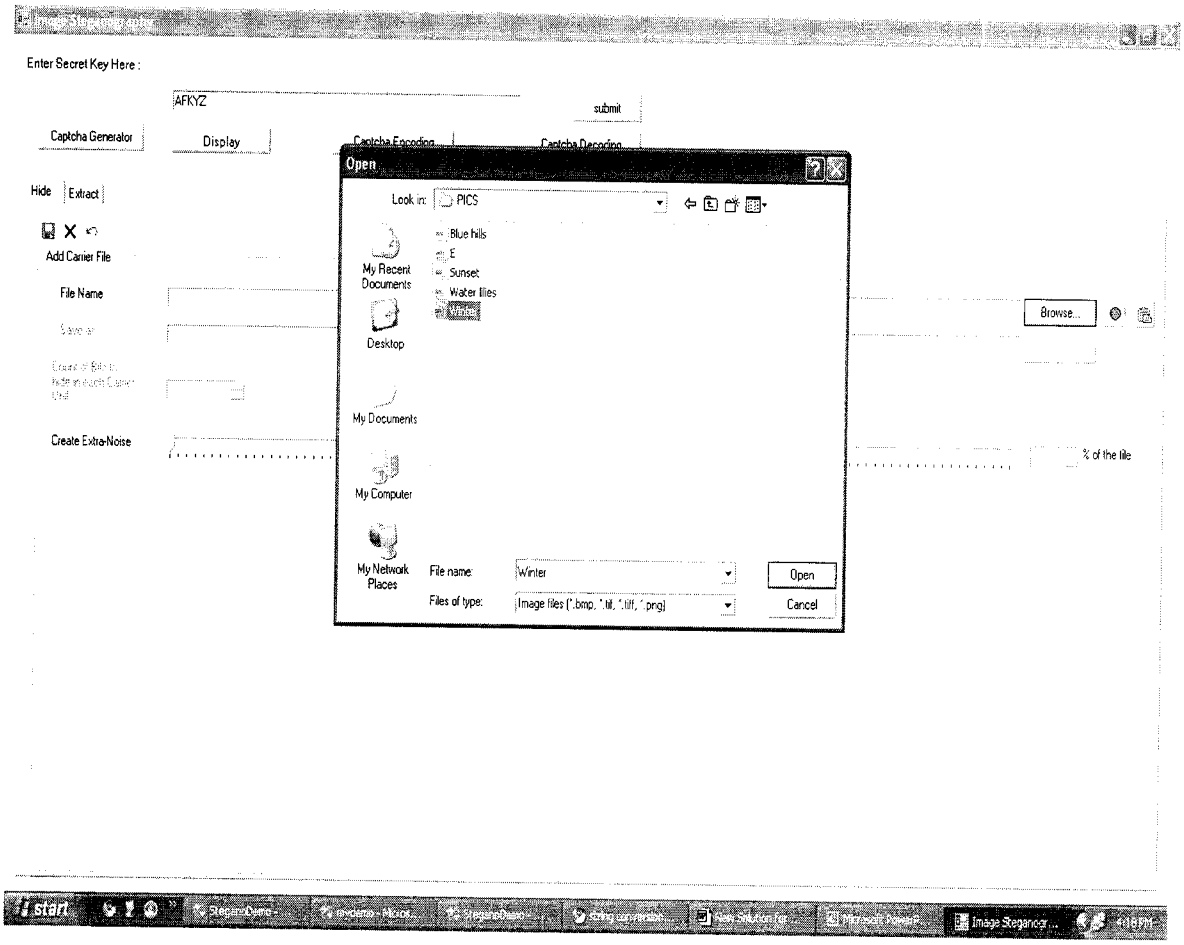
ENTERING THE PASSWORD KEY



Enter Secret Key Here : AFKYZ

Correct Key..You Can Proceed Further !!!

SELECTING THE CARRIER FILE

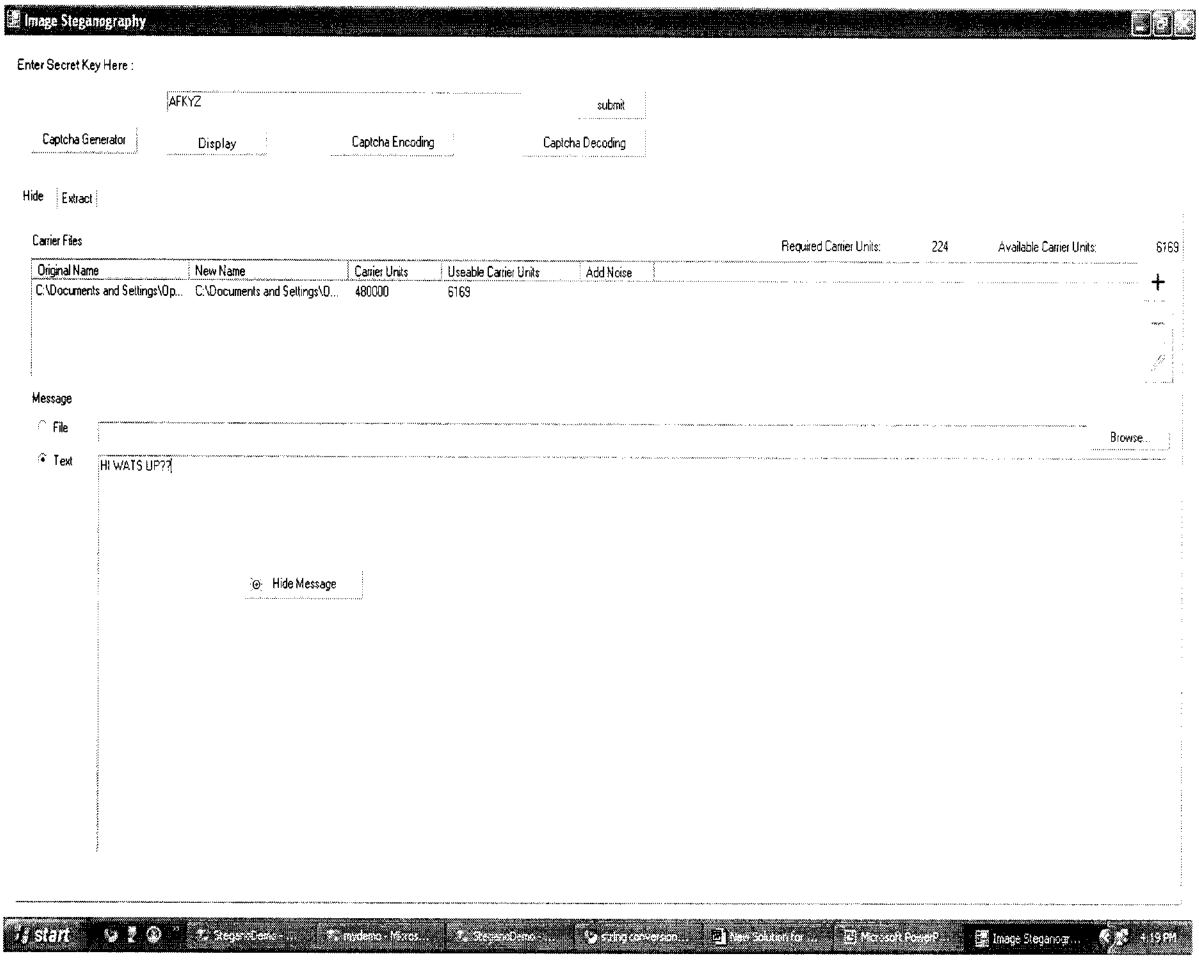


Enter Secret Key Here : AFKYZ

File name: Winter

Files of type: Image files (*.bmp, *.tif, *.tiff, *.png)

SELECTING THE DESTINATION FILE



Enter Secret Key Here : AFKYZ

Carrier Files

Required Carrier Units: 224

Available Carrier Units: 6169

Original Name	New Name	Carrier Units	Useable Carrier Units	Add Noise
C:\Documents and Settings\Op...	C:\Documents and Settings\O...	480000	6169	

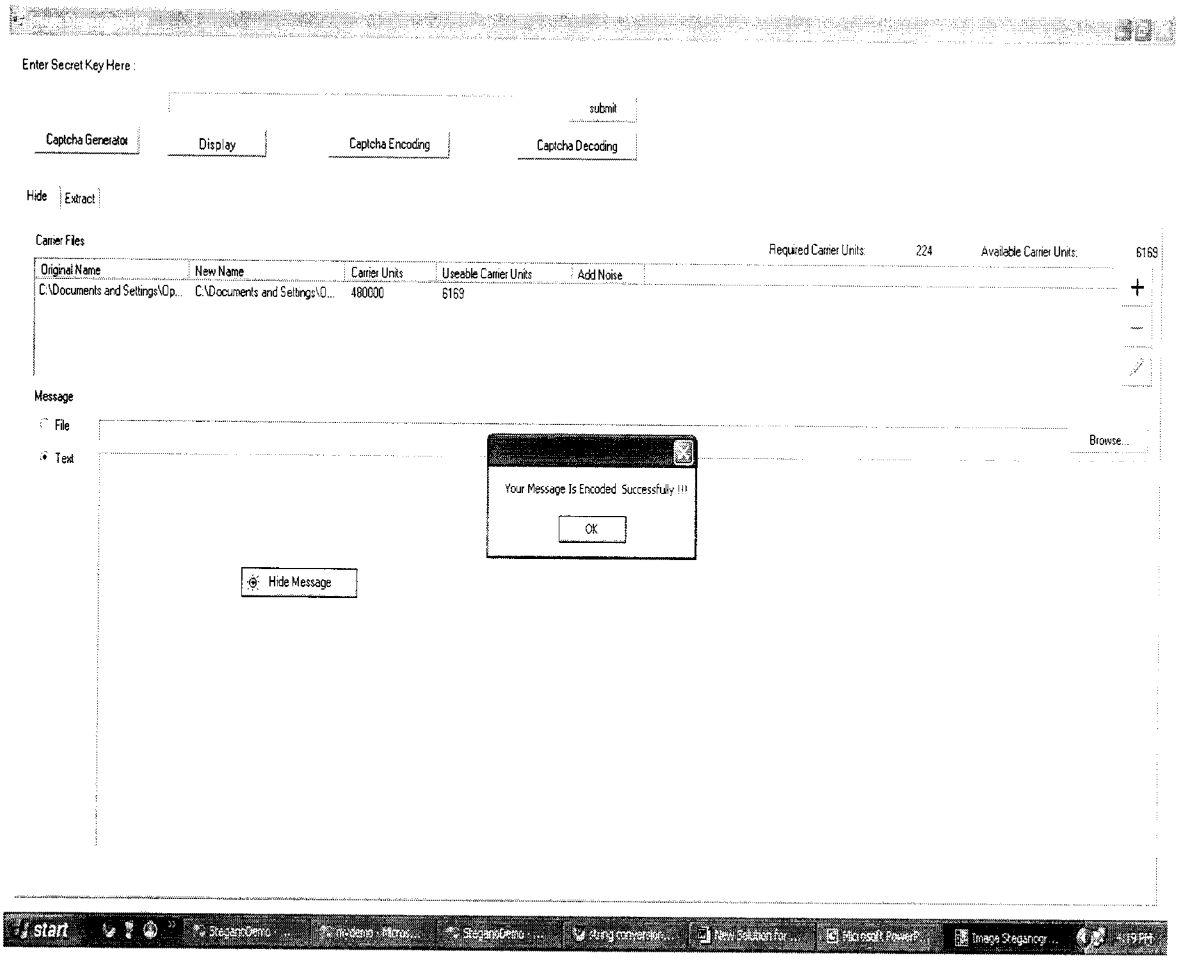
Message

○ File

● Text

HI WATS UP??

STEGO ENCODING:



Enter Secret Key Here :

Carrier Files

Required Carrier Units: 224 Available Carrier Units: 6169

Original Name	New Name	Carrier Units	Useable Carrier Units	Add Noise
C:\Documents and Settings\Op...	C:\Documents and Settings\O...	480000	6169	

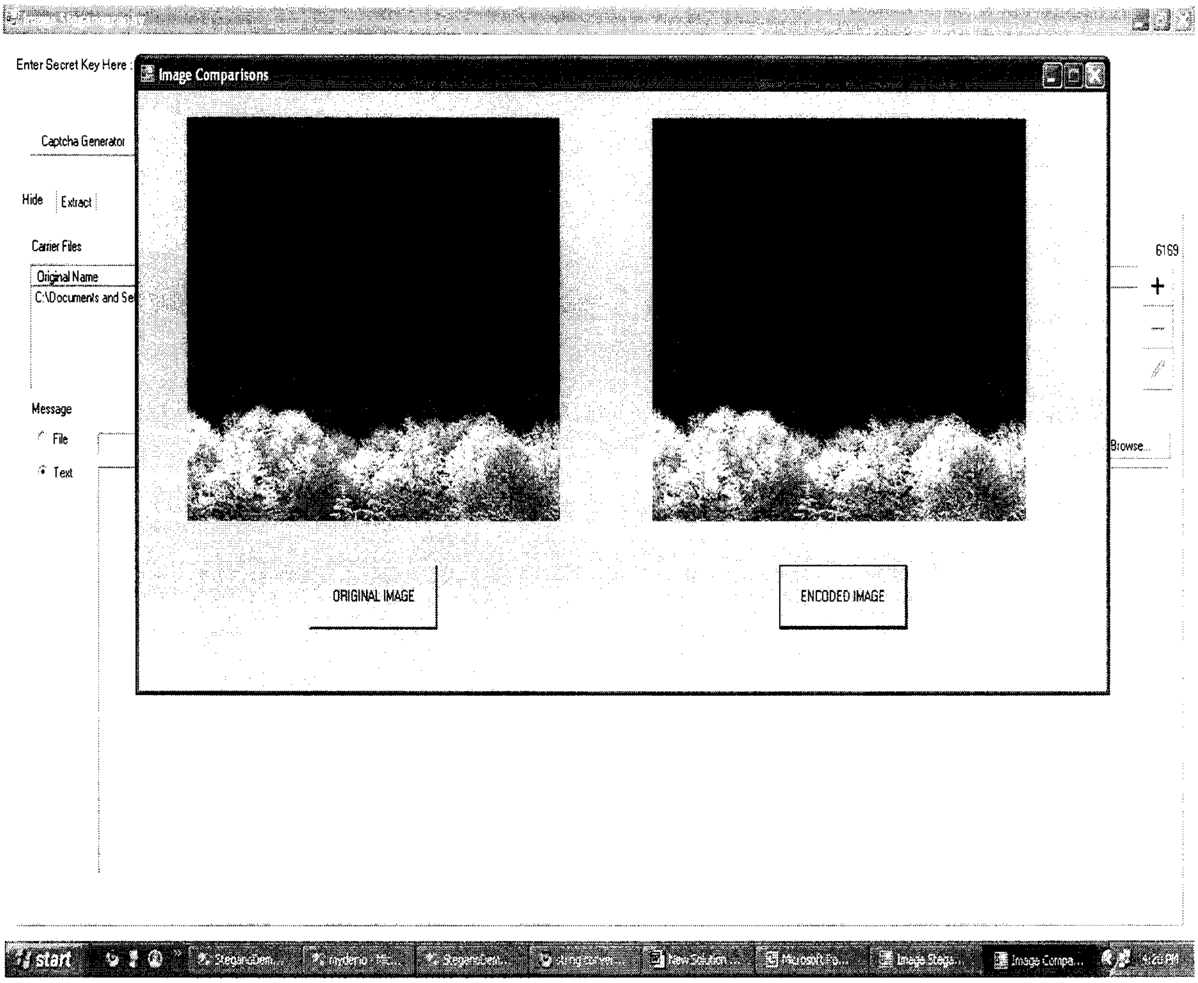
Message

○ File

● Text

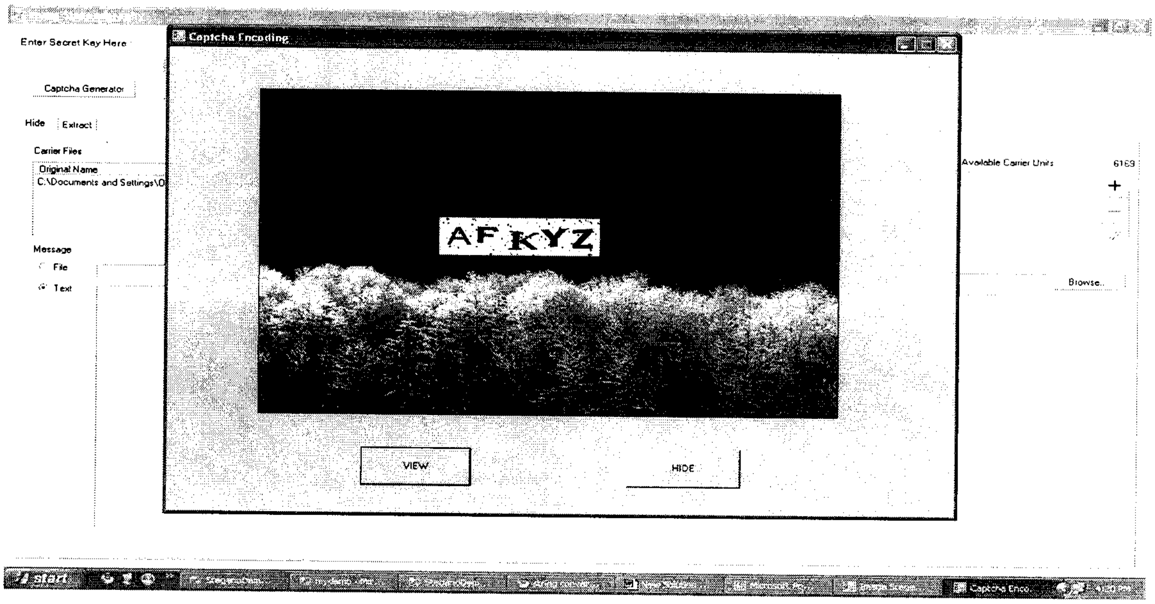
Your Message Is Encoded Successfully !!!

AFTER ENCODING:



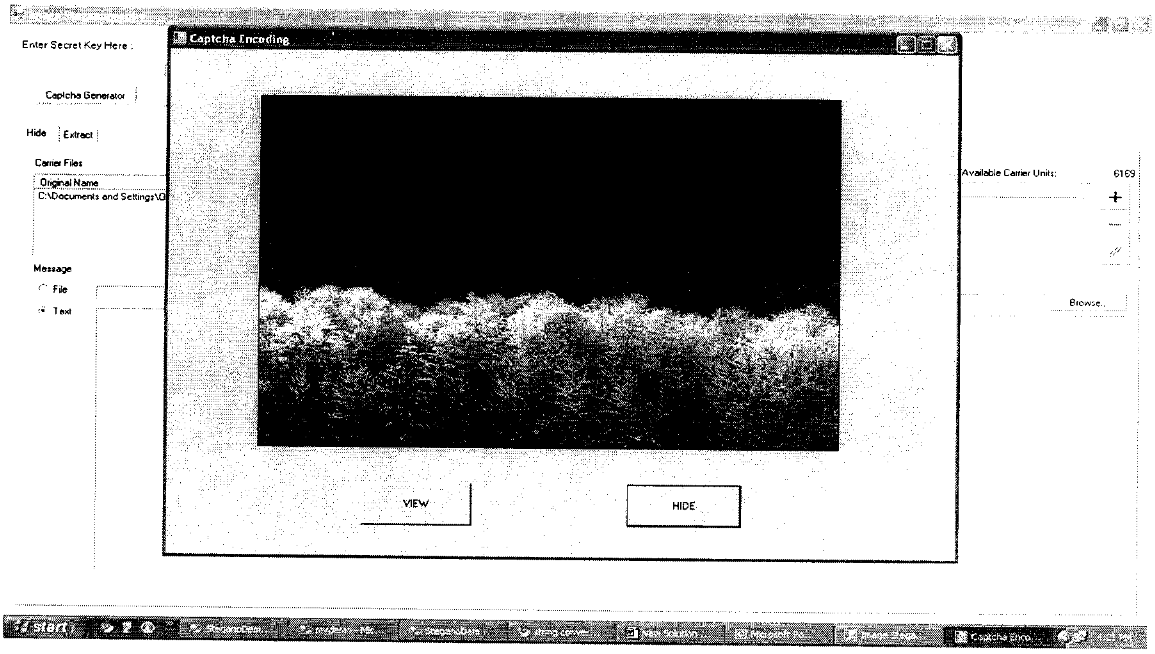
RECEIVER SIDE

CAPTCHA ENCODING:



C:\Documents and Settings\D

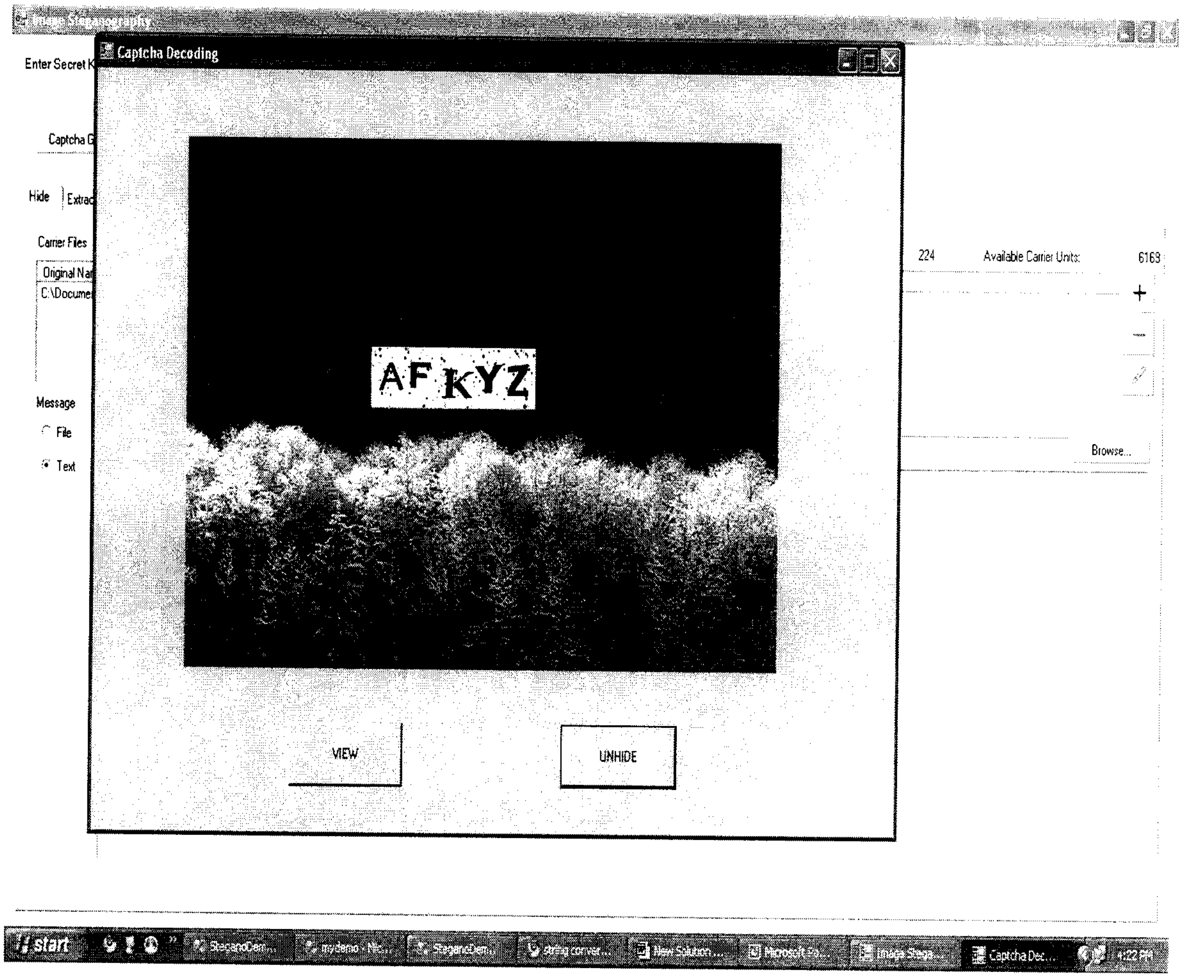
Available Carrier Units: 6169



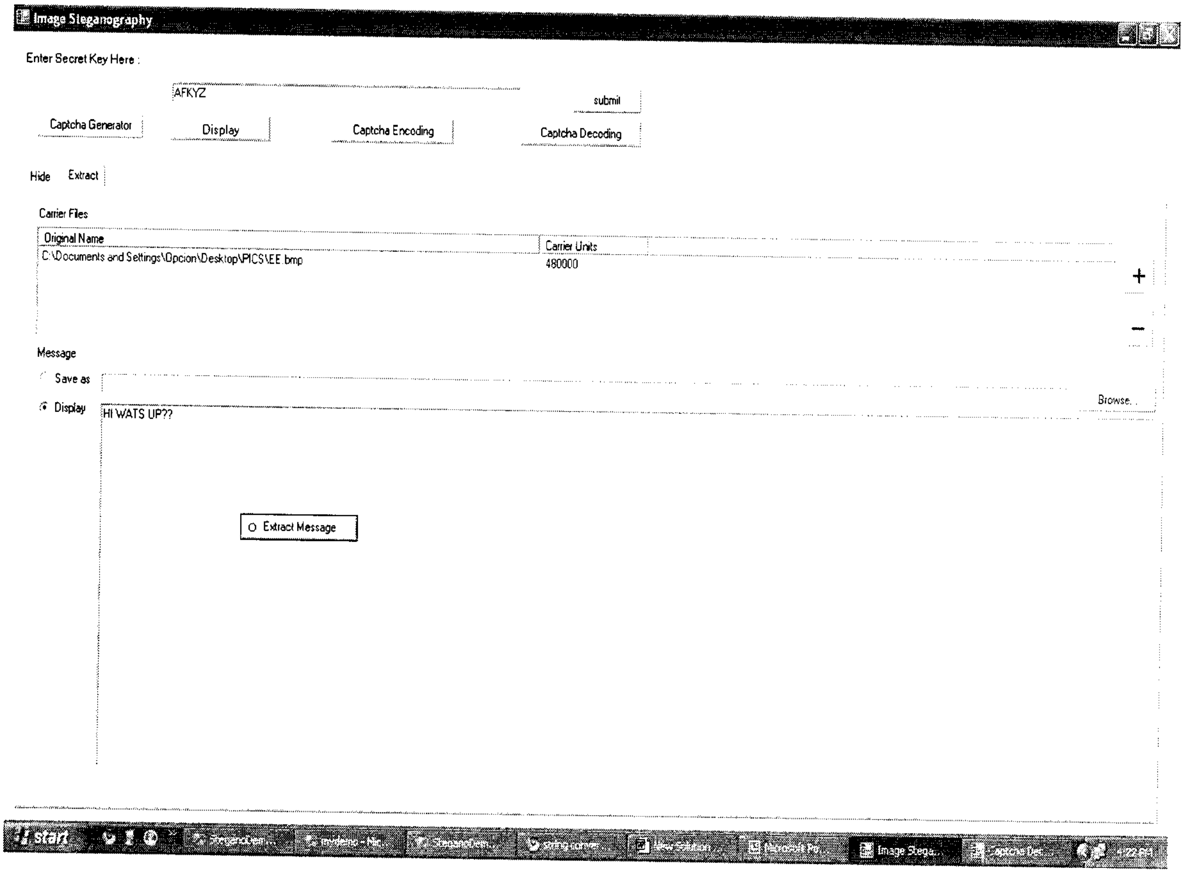
C:\Documents and Settings\D

Available Carrier Units: 6169

CAPTCHA DECODING:



STEGO DECODING:



Enter Secret Key Here : AFKYZ

Original Name	Carrier Units
C:\Documents and Settings\Opcion\Desktop\PICS\EE.bmp	480000

○ Save as

● Display: HI WATS UP??

REFERENCE

References

[1] Baird.H.S and Riopka.T, “ScatterType: a Reading CAPTCHA Resistant to Segmentation Attack,” Proceedings of the IS&T/SPIE Document Recognition & Retrieval XII Conference, CA, USA, 2005, pp. 197-207.

[2] Blum.M et al, "The CAPTCHA Project (Completely Automatic Public Turing Test to tell Computers and Humans Apart)," School of Computer Science, Carnegie-Mellon University, http://www.captcha.net

[3] Curran K and Bailey .K, "An Evaluation of Image Based Steganography Methods," International Journal of Digital Evidence, vol. 2, issue 2, pp. 1-40, Fall 2003.

[4] Hopper N.J, Toward a theory of Steganography, Ph.D. Dissertation, School of Computer Science Carnegie Mellon University, Pittsburgh, PA, USA, July 2004.

[5] Provos.N and Honeyman.P, "Hide and Seek: An Introduction to Steganography," Security & Privacy Magazine, pp. 32-44, May/June 2003.

[6] Shirali-Shahreza.M and Shirali-Shahreza.S, "Collage CAPTCHA," Proceedings of the 20th IEEE International Symposium Signal Processing and Application (ISSPA 2007), Sharjah, UAE, February 2007.

[7] Shirali-Shahreza.S, "Stegano Grades: Secure Announcement of the Students' Grades Using Steganography," Proceedings of the 20th IEEE International Symposium Signal Processing and Application (ISSPA 2007), Sharjah, United Arab Emirates (UAE), February 12-15, 2007.

[8] Stirmark software: http://www.cl.cam.ac.uk/fapp2/watermarking/stirmark, 1997.

[9] UnZign software: http://altern.org/watermark, 1997.

[10] Von Ahn .L, Blum .M, and Langford J, "Telling Humans and Computers Apart Automatically," Communications of the ACM, vol. 47, no. 2, pp. 57-60, February 2004.

[11] Wolfgang.R.B and Delp.E.J, "Fragile watermarking using the VW2D watermark," *Proceedings of the SPIE/IS&T Conference on Security and Watermarking of Multimedia Contents*, SPIE Vol. 3657, San Jose, CA,January 1999.