**MINI PROJECT**

**DATA CRYPTING**

**SOFTWARE REQUIREMENTS SPECIFICATION**

DATE: 06-01-2016

Batch id:13A02

**STUDENT NAME HALL TICKET NO.**

G.SINDHU BHARGAVI 13251A1219

G.SRUTHI 13251A1220

G.VARSHITHA 13251A1221

I.BHAVYA 13251A1222

**G.NARAYANAMMA INSTITUTE OF TECHNOLOGY & SCIENCE**

**SHAIKPET,HYDERABAD.**

****

**TABLE OF CONTENTS**

1. INTRODUCTION
   1. PURPOSE
   2. BACKGROUND OF A PROBLEM
   3. EXISTING SYSTEM
   4. PROPOSED SYSTEM
2. SCOPE
   1. PROJECT SCOPE
   2. OUT OF SCOPE
3. HIGH LEVEL CONCEPTUAL SOLUTION ARCHITECTURE
4. ASSUMPTIONS & DEPENDENCIES
5. ACRONYMS & BUSINESS TERMS
6. FUNCTIONAL REQUIREMNTS
7. NON-FUNCTIONAL REQUIREMENTS
8. INTERFACES
9. **INTRODUCTION**

The hidden or embedded image, audio or a video files act as carriers to send the private messages to the destination without any security breach. Steganography techniques can be implemented on variousfile formats such as audio (.mp3 , .wmv , etc.), video ( .mpeg , .dat , etc.) and images (.jpeg, .bmp, etc.). However, the images are themost preferred file format for this technique. Steganalysis aims at discoveringand decrypting the suspected data transferred with the use of the available algorithms.

**1.1** **PURPOSE**

The Software Requirement Specification is documented in such a way that it breaks the deliverables into smaller components. The information is organized in such a way that the developers will not only understand the boundaries within which they need to work, but also what functionality needs to be developed and in what order.

**1.2 BACKGROUND OF A PROBLEM**

Data or information is very crucial to any organization or any individual person. None of us likes our conversation being overheard as it contains the potential of being misused. Same is the case with the data of any organization or of any person. The exchange of data among two potential parties must be in done in a secured method so as to avoid any tampering. Two types of threats exists during any information exchange. The unintended user who may try to overhear this conversation can either tamper with this information to change its original meaning or it can try to listen to the message with intention to decode it and use it to his/her advantage. Both these attacks violated the confidentiality and integrity of the message passed. Providing intended access and avoiding unintended access is a very challenging task. Information hiding has been since long time. In past, people used hidden pictures or invisible ink to convey secret information.

**1.3 EXISTING SYSTEM**

It Several techniques have been proposed by researchers for securing electronic communication.Before stegnography cryptoghy is used to send hidden information is the process of converting ordinary information into unintelligible text . Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. A cipher is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". The key is a secret (ideally known only to the communicants), usually a short string of characters, which is needed to decrypt the ciphertext.

**1.4 PROPOSED SYSTEM**

The goal is to hide messages inside other harmless messages in a way that does not allow enemy to even detect that there is a second message present. Steganography focuses more on high security and capacity. Even small changes to stego medium can change its meaning. Steganography masks the sensitive data in any cover media like images, audio, video over the internet.

Steganography involves four steps:

1. Selection of the cover media in which the data will be hidden.
2. The secret message or information that is to be masked in the cover media.
3. A function that will be used to hide data in the cover media and its inverse to retrieve the hidden data.
4. An optional key or the password to authenticate or to hide and unhide the data
5. **SCOPE**

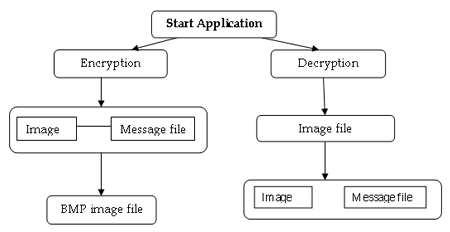
**2.1 PROJECT SCOPE**

The scope of the project is to limit unauthorized access and provide better security during message transmission. To meet the requirements, I use the simple and basic approach of steganography and digital watermarking. In this project, the proposed approach finds the suitable algorithm for embedding the data in an image using steganography which provides the better security patterns for sending messages through a network.

**2.2 OUT OF SCOPE**

In this aspect we are using user registration and login forms through .NET Framework 3.5.The system has inbuilt checker to check whether the image format(BMP images) is correct and image size is big enough to hide the data.

**3 HIGHLEVEL CONCEPTUAL SOLUTION ARCHITECTURE**



**4. ASSUMPTIONS AND DEPENDENCIES**

A project starts with assuming:

* The database information is valid and the operations are rightly performed and the database is updated for every transaction.
* Dedicated development resources are available.
* Requirements will be approved in timely manner.
* The communication between systems was good.

Constraints/Dependencies

* The Response time of the system should be with in seconds.
* The system has to depend on the status of communication between the bank database and the application performs the bank operation.

**5. ACRONYMS AND BUSINESS TERMS**

**5.1 ACRONYMS**

|  |  |
| --- | --- |
| **ACRONYMS** | **ABBREVATIONS** |
| JPEG/JPG | Joint Photographic Experts Group |
| PNG | Portable Network Graphics |
| WMV | Windows Media Audio and/or Video |
| LSB | Least Significant Bit |
| MPEG | Moving Picture Experts Group |
| LAN | Local Area Network |

**5.2 USER ROLES AND PERMISSIONS**

|  |  |  |
| --- | --- | --- |
| **Sl.no** | **Screen module** | **access** |
| 1 | Open the software: software will be loaded up as intended.There no anomalies. | yes |
| 2 | File>new:the required interface will be appeared.if any operation is half done thenconfirmation box will pop up. | yes |
| 3 | Action>decrypt:the decryption screen will appear and option to select image wil appear. | yes |
| 4 | Action>advancedview:1.if it is checked the advanced view of software will appear.  2.if it is unchecked the basic view of software will appear. | yes |
| 5 | Action>safe text as a file:an option to the decrypted file in an external file will appear.if there is no text pop up will show. | yes |
| 6 | Action>view image:image will be shown in a new window.if no file was encrypted when this button was pressed then no action will be taken. | yes |
| 7 | File>exit:if any operation was half done ask for confirmation otherwise close the application. | yes |

**6.FUNCTIONAL REQUIREMENTS**

|  |  |  |  |
| --- | --- | --- | --- |
| **FIELD NAME** | **FIELD DESCRIPTION** | **FIELD TYPE** | **BUSINESS**  **RULES** |
| User name: | Enter name of the user | Includes characters and numbers. | Size should be less than 15words. |
| Password: | Enter password | Includes the symbols on keyboard. | Minimum of 8  Characters. |
| data: | Data to be hidden | Includes text,images. | Should not be empty. |
| Covering data: | Data used to hide the orginal data. | Includes text,images. | Should not be empty. |
| Covering data size: | Size of the data that hides orginal data. | Includes text,images. | It should be greater than orginal data. |
| Covering image format: | Formt of covering image | Includes image. | It should be BMP format. |
| Encrypt: | Used to encrypt the given information. | Includes button. | It embed the data properly. |
| Decrypt: | Used to decrypt  the data into orginal format. | Includes button. | It should decrypt data properly without data lose. |

7. **NON-FUNCTIONAL REQUIREMENTS**

**Performance Requirements**:

The ram should be 128mb atleast. But 256mb ram is recommended. The disk space required to store the software is 10mb and to store the output files and other configuration files assosciated with the software. The recommended disk space required is 15mb.

**Safety Requirements**:

The size constraint have to be evaluated by the end user only. The software doesn’t check for the size constraint. This is done to enhance the performance of the software in terms of speed. In case the size of hidden object exceeds the max. Allowable size that can be hidden, the extra information is truncated. The part of hidden object of size equal to maximum possible size is stored in carrier file. The size of the hidden object that can be stored in a carrier file depends on carrier file size and type of steganographic task. The screen resolution should be set to 1027x768 or higher to get the complete view of the software. In case of the lower screen resolution, the software not only looks awkward but also not completely visible.

**Security Requirements**:

The user must have the registered account to run the software. The administrator account is needed to be created on the first run the software. The administrator account can be used to create other user accounts. If the user forgets the password, the password can be retrieved on the basis of Date of Birth. This date of birth is stored at the time of the creation of the account although it can be modified later.

**Usability**:

Usability is the factor for any data security system; the software should be flexible for transferring the data between one ends to another. It should provide a friendly interface between customer and user.

**Scalability**:

Scalability is one of the important issues when the software used in large institutions where the security plays a major role. Some systems can’t providethe high level security when the data to be embedded is large. In that case, Scalability plays major role.

**Reliability**:

The data security software or applications are used in many organisations like in military for securing the critical information, in financial organisations for securing the equities and trade information etc., the application should be consistent when using in different applications and provide better security in order to avoid modifications.

**Availability:**

Prevention of unauthorised persons from holding the important in formation. The program should provide the security from unauthorized modifications, should be available only for authorized persons. The program should be flexible and should be available within a mean time and should work in any operating system.

**8. INTERFACES**

**User Interfaces**:

* Splash Screen: It is the first screen which is shown to the user. It loads other modules of the project.
* Login Screen: It is for security purpose. It asks the user to give its name and password. Only authenticated user can use the software.
* Main Form: It provides various features to user about the mode of use of software. User can choose audio, text, image options and can do work on it. It also provides various other features like user management, encryption, zip, log file.
* Back: By clicking on this button the main form will appear.
* Exit: Click on the exit button the main form will shut down the application.
* Error Messages: Proper error messages will appear when any error is encountered.

**Software Interfaces:**

Microsoft visual studio 2010 is used in the project for developing the application and Microsoft visual C# is used for execution.

**Hardware Interfaces:**

Although the hardware is not mandatory for developing a steganographic application for transferring the data from one end to another, HUBs, LAN and Routers are needed for building the communication media from receiver to the sender.

**Communication Interfaces:**

TCP/ IP protocols and E-mails are used as communication media for transferring data from sender to receiver and vice versa.