Software Requirement Specification

for

Advanced Data Encryption and Steganography

Prepared by:

Sabina Bhadrish, Roll No. 805
Sayantan Chakraborty, Roll No. 819
Dolly Lee, Roll No. 820

Table of Contents

1. Introduction

1.1 Product Purpose

The primary objective of the product is to provide means to hide critical and confidential data within other files, thus rendering them undetectable by unauthorized individuals. The hidden information can be a text, audio, image or video file. The carrier file also can be of any uncompressed file format. The information to be hidden is first encrypted using a new advanced encryption algorithm, the output of which is then stored within the carrier file, ensuring high level of security. This document describes the scope, functionalities, software requirements and viability of the project undertaken.

1.2 Document Conventions

The document has been prepared in accordance with IEEE standards. The primal components of this document are highlighted in Bold Face.

1.3 Intended Audience

End Users: They are the ones who will be operating the software product most. So, this SRS is extremely useful for the End Users as they get a clear idea about the requirements, scope, functionality and performance of the software.

Software Developers: This SRS is also helpful for developers who contrive to develop any such similar software product based on advanced data encryption and image steganography from scratch.

Software Testers: It is imperative that the professionals involved with testing this software product have a clear idea about the product, which is provided in this SRS document.

Students: The SRS can also be regarded as a practicable solution to queries regarding data encryption and image steganography.

1.4 Product Scope

The software product is able to perform encryption technique on text, audio, image, video files or just simple plaintext based messages. It also supports steganography, hiding the encrypted file in an uncompressed file. Both of these data hiding techniques is protected by secure passwords, thus being highly difficult for cryptanalysts to decode.

1.5 References

1. Symmetric key cryptography using random key generator, A.Nath, S.Ghosh, M.A.Mallik, Proceedings of International conference on SAM-2010 held at Las Vegas(USA) 12-15 July,2010, Vol-2,P-239-244
2. Modified Version of Playfair Cipher using Linear Feedback Shift Register, P. Murali and Gandhidoss Senthilkumar, UCSNS International journal of Computer Science and Network Security, Vol-8 No.12, Dec 2008.
3. Richard A. Mollin, An Introduction to Cryptography, CRC Press, 2000
4. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, Digital Watermarking and Steganography, Morgan Kaufmann Publishers, 2008
5. Peter Wayner, Disappearing Cryptography - Information Hiding, Steganography and Watermarking, Morgan Kaufmann Publishers, 2008

2. Overall Description

2.1 Product Perspective

Steganography is the science of hiding messages within some sort of carrier files in such a way that no one apart from the sender or the receiver suspects the existence of the message. This software product applies an advanced encryption algorithm to encode data, and then in turn hide the encrypted file within the carrier file. First the cipher algorithm is applied on the input file, the output of which is hidden in an uncompressed file using bit manipulation steganographic technique. The primary advantage of this software is that it's not just limited to hiding plaintext data within a carrier file; it can be used to hide other images, audio and even video files within such hosts, in its encrypted form, thus ensuring security to the utmost degree.

2.2 Product Features

- An advanced data encryption algorithm is implemented which is the primary feature of the software.
- Multiple encryptions are supported.
- Steganography is also supported.
- The hidden object can be a simple plaintext file, an image, or even an audio/video file.
- Carrier files can be of any uncompressed file type.
- The software provides authentication check during login. Without a proper username and password the user cannot access the software.
- The software also provides high levels of security via a secure password used during encryption and during steganography without which the decryption would not be possible.

2.3 User Classes and Characteristics

The software product can be used by developers to understand, and if possible, improve the encryption standard, and can be operated by naïve end users to securely transmit confidential data.

2.4 Operating Environment

Operating System: Windows XP, Vista, 7
Software Requirements: Microsoft .NET Framework 4
Recommended Configuration: Intel Pentium 4, 2 GHz or higher, 256mb RAM or higher, sufficient disk space to install the software product and the necessary files.
Optimal Screen Resolution: 1024x768

2.5 Design and Implementation Constraints

- Although the software is portable, it cannot run on platforms other than windows. It cannot be made to run over LAN or any form of network.
- The size of the file to be hidden should preferably be approximately 20% of the size of the carrier file for efficient and fast steganographic operations.

2.6 Assumption and Dependencies

- The minimum system requirements must be satisfied for efficient software performance.
- The Operating System should be any one of the Microsoft Windows NT family.
- Relevant software must be installed to view audio/video files.

3. External Interface Requirements

3.1 User Requirements

Login Screen: It's the first screen that is shown to the user. The user should provide a valid user id and password to access the software.

Main Form: It provides the user with all the features of the software product, including option for implementing steganography and data encryption. It also provides the current date and time. Options are provided to reset the fields entered and to shut down the application.

3.2 Hardware Requirements

Apart from the recommended hardware specifications as mentioned, no other specific hardware is necessary to operate the software.

3.3 Software Requirements

Microsoft .NET Framework should be present in the system, along with the necessary software to view the audio/video files.

4. Other Non-functional Requirements

4.1 Performance Requirements

- ✓ The RAM should be 256mb though 512mb is recommended.
- ✓ The processing unit should be fast enough to perform the encryption and steganographic functions efficiently.
- ✓ Sufficient storage space is necessary to install the software and other dependent files, along with the hidden object and carrier file.

4.2 Safety Requirements

- ➢ The size constraints for steganography are to be evaluated by the end user.
- ➢ The size of the object to be hidden depends on the carrier image.
- ➢ The software is fully visible with a screen resolution of 1024x768 or higher.
- ➢ The size of the file to be hidden should preferably be approximately 20% of the size of the carrier file for efficient and fast steganographic operations.

4.3 Security Requirements

The user must possess a valid user id and password to access the software. The user should also possess two unique passwords used for encryption and steganography to get back the original file. The password for encryption process determines the number of times encryption and decryption is performed, thus it should be same for both the processes, whereas the one used for steganography is embedded in the carrier file and is validated before retrieving the data.

5. Other Requirements

The software performs efficiently when the object to be hidden and the carrier file are in the same folder, preferably in the folder where the software is, else there is a slight decrease in performance. It should also be noted that the size of the carrier file is preferred to be much more than the source object so that it can be completely hidden in the carrier. There are no further requirements than those specified in the SRS under the different headers.