IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 01-06

Windows Files And Folders Security Using Cryptography And Steganography

[1]AnushaJagannathachari, [2]Archana Nair, [3]Prof Dr.Bharati Wukkadada, [4]Prof. Dr. D.G Jha

[1](MCA student, KJ Somaiya Institute of Management Studies & Research, Mumbai University, India)
[2](MCA student, KJ Somaiya Institute of Management Studies & Research, Mumbai University, India)
[3](Assistant Professor, KJ Somaiya Institute of Management Studies & Research, Mumbai University, India)
[4](Professor, KJ Somaiya Institute of Management Studies & Research, Mumbai University, India)

Abstract: *This papers main aim would be to put forth the implementation of cryptography and steganography to secure files and folders in windows platform. It is a windows desktop application. Here the users can lock their various folders in a different format such as recycle bin, help and support, etc. Once it is locked, for example as recycle bin, the original contents of the locked folder will be hidden and replaced with recycle bin's contents. The locking and unlocking will be done with the help of passwords, which will be encrypted and stored in the database. Similarly, this application would also help us to lock an individual text file. By implementing steganography, the text file, pdf, PowerPoint slide etc can be converted to image and stored safely. The algorithm used for converting the text file to image and encrypting-decrypting the password is AES Algorithm.*

Keywords: *Asp.net with C#, Cryptography, Files, Folders, MySQL database, AES Algorithm, Steganography, Windows Desktop Application, Windows Operating System.*

I. Introduction

Adoption of technology is really excelling. With technology comes the threat to its security. These days' humans have become much more dependent on electronic gadgets. Gone are the days when one used to write important notes in diaries. These days all the important documents are stored in computers electronics. Thus it is very essential to secure them. Social media has by far influenced every individual's life. These social media accounts require passwords to log in. It becomes very difficult to remember these many passwords. Thus this windows desktop based application would help one to store their passwords in an encrypted format, it also helps to lock the folders securely from external hindrance. One can also transmit import text files in the form of text images so that important data is not tampered by attackers. This application follows the Technology Acceptance Model (TAM) theory.

II. Literature Review

Birget, J.C. D. Hong. Memon September 2006[7], discussed that the user can click only one point or the number of points he can remember based on his memorizing capability on each of the images rather than on clicking on several points on one single image. This paper also discusses the traditional alphanumeric password's drawback and talks about the innovation needed in security systems. S.Wiedenbeck, J.C.Birget, A.Brodskiy, N. Memon, ACM SOUPS", 2005[8], discussed recall-based techniques; a user selects images during the registration and is asked to reproduce something that he or she created during the registration phase. Ferhaoui Chafia, Chitroub Salim, Benhammadi Farid proposed a method based on the storage of the true minutia but under encoded shape, by using hashing function such that SHA1(Secure Hash Algorithm). Ferhaoui Chafia, Chitroub Salim, Benhammadi Farid also specifies the security principles and suggest a hybridization approach for more secure systems. Usage of the graphical password is the concept on which the paper focuses on. Giving birth thus to a new approach that uses the advantages of the 'Fuzzy commitment' to fill the weaknesses of 'Fuzzy Vault' [5].

III. Design Overview

Design and the concept implementation of the application has not been adopted from any reference. This application has a rich graphical user interface. The user will first have to log in to the application using their username and master password. After that, the user will be presented with various tabs, such as "Manage Password", "Folder Lock", "File Lock" and "Settings". The user will have to select one tab and give the appropriate details to lock the file or folders. Algorithm used for encryption decryption as well as steganography is AES(Advanced encryption standard).The application is designed keeping in mind the Technology Acceptance Model (TAM). As per this model theory, the major factors that influence the user's decision about how they will

use it are A) Perceived usefulness B) Perceived ease-of-use(PEOU). The first property was defined by Fred Davis. This property indicates the degree to which a person believes that the application would enhance his performance in the job. According to Fred Davis, PEOU states that using the application would free from effort.

IV. System Requirements

4.1. Windows Operating System

The proposed application would be functioning only on Windows Operating System.

4.2. Microsoft Visual Studio 2010 Or Higher

This is an IDE that is used to develop this windows based desktop application, with a .NET Framework 4 Client Profile.

4.3. Xampp Server

It is an open source platform which provides web server solution stack package which is totally free. It is very simple and easy for developers to create a local web server for development purposes.

4.4. MY SQL

To query the data My SQL is used which is an open source relational database management system.

4.5. Windows Form

Used to create Graphical User Interface for the application.

4.6. Cryptography And Steganography

Algorithms associated with these techniques would help develop this application.

V. Diagramatic Representation Of Application

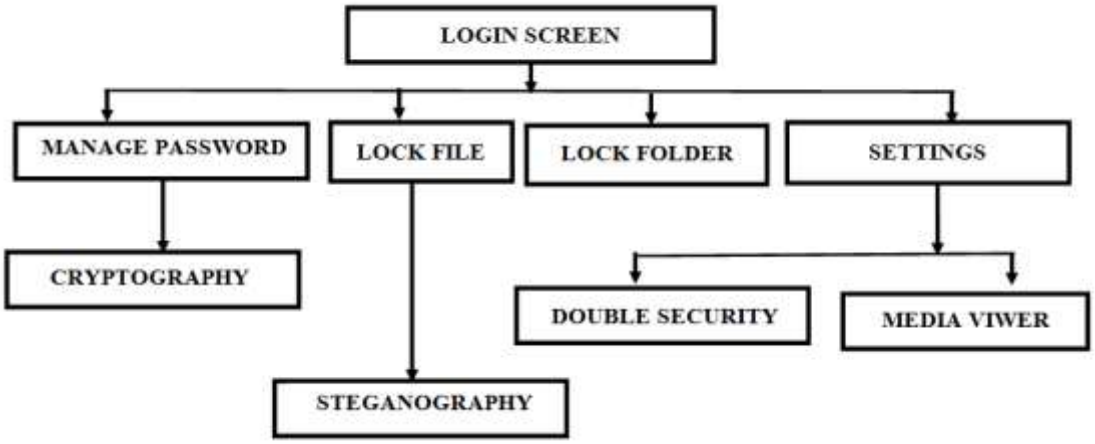
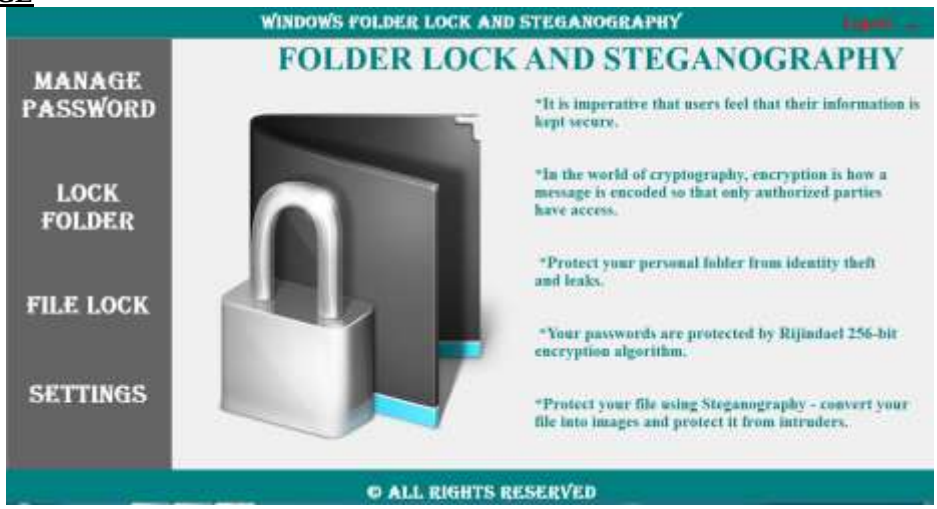


Fig. 1 Flow chart demonstrating the work flow and technique used behind each Form.

LOGIN PAGE

HOME PAGE



MANAGE PASSWORD

FOLDER LOCKING

FOLDER UNLOCKING

FILE LOCKING

SETTINGS

Fig. 2 Screenshots of the proposed application

VI. Algorithm

AES plaintext has to be 128 bits.
Key size can be of size 128, 192, 56 bits.
Pseudo code for 128 bit AES Encryption:

A. Do the one time initialization processes:
   a. Expand the 16 byte key
   b. Do the initialization of 16 byte plain text block called state
B. For each of the rounds proceed with the following operations:
   a. Apply S box to state
   b. Rotate row K of the plain text by K bytes
   c. Perform mix column operations
   d. XOR state with the key

VII. System Working

Here the user will initially have to sign up with username and master password. After that, the user will have to log in with the same username and master password. Once this is done the user will be presented with a home page wherein four tabs will be made available to the user. If the user clicks on Lock Folder, then the user will have to choose one radio button, then the user will have to specify the folder location along with a password. The folder will be locked using the specified password and the password will be encrypted and stored in the database. While unlocking the password the user will have to only specify the folder that he/she wants to unlock and the same password. If the password is valid, then the folder will be unlocked. Suppose the user wants to lock a specific text file, the user will have to select the Lock File tab. Here the user will have to select an image, a text file to lock and a password. The text file will be locked used steganography technique – AES(Advanced Encryption standard) algorithm and the text file will be converted to an image with .jpg, .png, .bmp, etc. extensions. To unlock the text file, the user will have to select the encrypted image and specify the same password. In order make it convenient for the user to remember all these passwords, the user can use the manage password section, wherein the user will have to mention the password and the title, the passwords will be encrypted and stored in the database. The user can easily access their passwords from this section. The user can also change their master password using the settings tab. If the user wants to just view the multimedia inside a folder which is locked, the user will have to unlock it, view it and then lock that folder again, we understand the overhead involved in such task. For removal of such repeated task, we have introduced a media viewer in the application which will allow access to view and play multimedia files through the application even if the file is locked. Also for highly confidential information, we avail the facility of encrypting the document and implement steganography together.

VIII. Conclusion

This application is very user-friendly. It reduces human effort to memorize all the passwords. The User will just have to remember one master password. The application helps secure all the folders and text files. It prevents access to an unauthorized user. Dual layer security mechanism that is locking a folder and then encrypting the password makes the application even more robust. The use of cryptography and steganography strengthens the security system by almost removing the chances of getting breached. Thus, a new security tool is created that lets you lock and unlock your folders as well as lock and unlock file with your personal password. This application is also completely cost efficient. One just has to download this application and start using it.

IX. Future Scope

Future scope of this application is to provide audit trails, wherein one can monitor how many times an unauthorized user tried to access a file or folder. Along with this, providing authorization to a specific user to access the files or folders locked by a different user would be a major enhancement part. This application is limited to the only windows platform, increasing its portability to various other platforms would be a major goal of future improvement.

References

[1]. Juan-hua, Zhu; Ang, Wu; Kai, Guo, " PC Lock Software Design Based On Removable Storage Device and Dynamic Password" , 2nd International Conference on Computer Engineering and Technology Journal VOL. 3, year 2010.
[2]. Rajkumar Janakiraman, Sandeep Kumar, Sheng Zhang, Terence Sim, "Using Continuous Face Verification to Improve Desktop Security", Seventh IEEE Workshop on Applications of Computer Vision, (WACV/MOTION'05).
[3]. Brendan Dolan-Gavitt, (May,2008), "Forensic analysis of the Windows registry in memory", MITRE Corporation, 202 Burlington Road, Bedford, MA, USA.

[4]. Umut Uludag, Sharath Pankanti, Anil K. Jain,"Fuzzy Vault for Fingerprints" ,2010.
[5]. Ferhaoui Chafia, Chitroub Salim, Benhammadi Farid , "A Biometric Crypto-system for Authentication",2010.
[6]. Youn Joo Lee, Kang Ryoung Park, Sung Joo Lee, Kwanghyuk Bae, and Jaihie Kim , "A New Method for Generating an Invariant Iris Private Key Based on the Fuzzy Vault System", 5th oct 2008.
[7]. Wiedenbeck, S., J.C. Birget, A. Brodskiy, and N. Memon. Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. ACM SOUPS, 2005.
[8]. S. Wiedenbeck, J.C. Birget, A. Brodskiy, N. Memon,"Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. ACM SOUPS", 2005.