International Journal of Future Generation Communication and Networking
Vol. 13, No.2s, (2020), pp. 1572–1577

A Survey on Folder Lock System based on Fingerprint Authentication

D. H. Patil, Dhananjay Nehere, Neha Takale, Rutika Kadam, Pankaj Sharma(2019)

Abstract

There are many local, state, and federal levels, including private companies, MNCs, security agencies, educational institutions where people share their equipment. It is possible that some unauthorized person may harm your important and confidential data, such as stealing information, copying, modifying, deleting or other illegal activities. Folder Lock is one way to ensure that your data remains secure and only accessible to an authorized person. So, it's protected against Biometric-protected Folder Lock - Fingerprint Authentication here. Think of the existing password Authentication system in place, there are many issues and issues associated. For example, a user needs to remember a password, it is human tendency not to forget passwords, many passwords can be guessed or cracked using multiple methods, such as Brute Force, can be broken using social engineering attacks, etc. Therefore, the program replaces password authentication with Biometric Fingerprint Authentication. The non-encrypted biometric authentication proposed here try to overcome the above mentioned issues, locking your data to be stored in an encrypted format, thus making it more secure and more reliable.

Keywords- *Biometric, Fingerprint, Authentication, Folder, Password*

I. INTRODUCTION

Accessing your confidential and confidential information is very important, as it is possible that someone who is unauthorized could harm it. Security problems arise when someone tries to steal or damage them to cause trouble and loss. Authentication is the process or act of proving or proving something that is true, factual or affirmative, a process or action to verify a user's identity and thus be permitted to reach only the authorized person. Replacing password authentication with Biometric Authentication has proven to be extremely beneficial and worthwhile.

Biometric authentication is a process that relies on the unique physical characteristics of a person to verify their identity. Biometric authentication systems compare the biometric data capture data stored, verified the actual data to the database. If both samples are biometric game data, the validity is guaranteed. Biometric technology is divided into two types namely Physical and Behavioral. Physical Biometries include physical features namely, Fingerprint scan, retina and facial recognition, and Behaeveal Biometrics include Signature, Word and Keystroke recognition.

Methodologically speaking, there are two types namely, Unimodal or Multimodal Biometrics. Unimodal Biometrics is the use of one biological element while Multimodal Biometrics is the use of a combination of more than one feature, thus adding another layer of security.

This program uses Unimodal Biometric Authentication

- Fingerprint recognition for locking and opening your folder. The contents of the locked folder will be stored in an embedded format, thus ensuring data confidentiality, data integrity and availability. With the right encryption solution, you can rest assured that your data is safe and that there is no direct way in which hackers can get their hands on that data. Although there are other ways in which data can be accessed, taking a simple step of encryption helps make the task more difficult for carpenters who may be keen to direct your data.

II. LITERATURE REVIEW

Folder Lock using Multimodal Biometric: Fingerprint and Signature Authentication (2015) [1] has proposed an application that requires two main devices namely a fingerprint scanner platform and a signature drawing pad. An application program is required for running on a PC desktop using the Windows Operating system..

ISSN: 2233-7857 IJFGCN

With regard to the initial authentication process, the user needs to place his finger on the fingerprint scanner, and if the fingerprint matches the database, only then the following authentication can be processed. After confirming the second method, the user can access the folder. The program had three major problems, first it was based on the platform (optimized for Windows only), secondly they didn't create standard listed folders either locked or open to make the user easy to see which files were locked and open, and thirdly there was no Graphical User Interactive interaction to make the system work Very helpful to the technician is the easy to use Multimodal Biometric Folder Lock program.

In the Multimodel Biometric Authentication System [2], it is shown that fingerprinting and face recognition can make a good combination of a biometric biometric system. This use of the biometric system is more accurate than the current method (such as password and pin need to remember). Facial recognition measures different aspects of the human face such as the width of the nose, the distance between the eyes, the shape and size of the mouth and so on. These calibrated objects are used to compare whenever a user is standing in front of a camera. The face recognition component contains the camera and face algorithm.

First, fingerprints and faces are stored in the database using sensors and camera. The finger recognition unit compares the fingerprint features stored in the database and the facial recognition algorithm is used to extract facial features and compare them to the database.

The Fingerprint Recognition Algorithms for Comprehensive Fingerprints Components [3] propose new algorithms-

1. Spaced Frequency Transfform Algorithm (SFTA).
2. Line Scan Algorithm (LSA).

SFTA was based on 2D Fast Fourier Transformation (FFT). The SFTA converts a local domain into a frequency domain. The results of this change show an image in the low and high frequency components. The computer calculates the FFT of two images per pixel and calculates the number of similar objects in both. If this calculation is higher than the limit value, then a match is obtained. Otherwise, it's a mistake.

The LSA was developed to reduce the comparison time when using the SFTA. LSA can be defined as a sequence of steps:
1. Image is stored and unwanted information was harvested.
2. Calculate the image border and resize the image to a larger size.
3. Correlations of the correlating function are used to judge the final outcome of the comparison.

In fingerprint classification [4], the novel method is based on the Hidden Markov Model (HMM) field and the imprint oriental field. With the extraction of fingerprints, making sample test protocols and HMM training for accurate embedding can be achieved.

The Automatic fingerprint scanner (AFIS) consists mainly of -
1. To achieve the fingers
2. Fingerprint separation
3. To align the fingers

For every default fingerprint there are two problems
1. How to remove and use the active fingerprint feature.
2. How to give us a more logical classification system.

Automatic fingerprint classification using HMM is a mathematical method depending on the fingerprint identification field .The precise and powerful fingerprint classification is trained and tested on two fingerprints.
Automatic fingerprint classification based on embedded HMM contains 5 steps [HMM operation]

1. HMM fingerprint embedding.

ISSN: 2233-7857 IJFGCN

2. Input field image of the input finger.
3. fingerprint scanning.
4. Uninstalling the feature and creating view vectors.
5. Performing a vector tracking sequence.
6. To compare the plans of the classification system.
7. Integrated HMM training.

III. RELATED WORK

A. Fingerprint Authentication & Authentication Operations

Today, Fingerprint authentication is widespread authentication returned instead of password. It provides easy access to the user by creating and remembering a password. Also, fingerprint scanning is much safer because our unique ecological features cannot be cracked or duplicated, thus providing an easy user access option. Fingerprint is a sign of the arches and fingerprints of the finger, it is a way of judging line structures called ports, where the skin has a higher profile than the surrounding area, called valleys. There are different ways of matching fingers like -

1. A comparison based on an image.
2. Coordination based on convention.
3. Comparison based in Minutiae.

Minutiae-based Matching -Techniques-based comparisons based on minutia represent the fingerprint for its local symbols, such as Core and Delta. The two fingerprints are the same if only their muscles point at each other. There are two important aspects of fingerprints considered in simulation -

1. Core 2. Delta

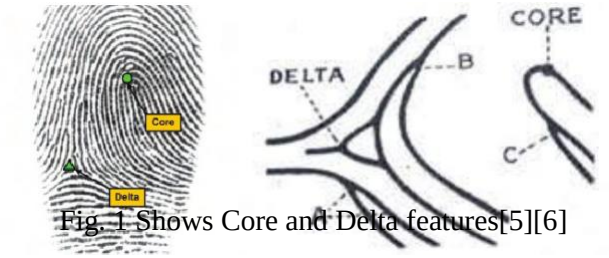


Fig. 1 Shows Core and Delta features[5][6]

Fingerprint matching process –The system will compare two fingerprints, the incoming fingerprint with the existing one in the database, focusing on the minutiae. When user will complete the initial scan of their fingerprint the system identifies the pinpoints the minutiae and transforms the information into an encrypted key or mathematical code or human unreadable format. The system actually stores this format for the purpose of comparison. When the user wants to unlock, he'll place his finger on the scanner. The system will scan the fingerprint and transform it into a code and compare the code with the original, in order to compare a match.

The matching algorithm–System uses **KNN (K -Nearest Neighbors) algorithm** for fingerprint verification. It is the simplest classification algorithm in which the class label of the nearest neighbors is used to decide the class label of the testing instances.

ISSN: 2233-7857 IJFGCN

A query- instance is classified by a majority vote of its k-neighbors. It uses Euclidean distance measurement to find out the nearest neighbors of the query instance. Here, we will classify the incoming data points and determine labeling it as matched or unmatched.

KNN Algorithm has following steps –

1. Determine parameter k = number of nearest neighbors
2. Calculate the distance between the query instance of interest and all the instance of dataset.
3. Sort the distances in ascending order and determine nearest neighbors based on the kth minimum distance.
4. Identify the class label of the nearest neighbors.
5. Use simple majority rule of the class label and predict the class label of a query-instance of interest.

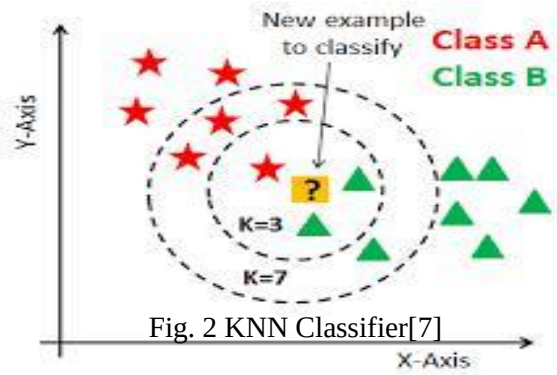


Fig. 2 KNN Classifier[7]

B. Encryption Algorithm

The data in locked folder will be stored in encrypted format to ensure it remains secured. For the purpose of encryption we use AES (Advanced Encryption Standard) Algorithm. AES is a symmetric key based cipher standard used for encryption and decryption. It is at least six times faster than triple DES. AES is widely used and supported software and hardware. Till now, no practical attacks against AES has been discovered, hence is more secured.

Major attributes of AES –

It is a symmetric key based algorithm .It works as a block cipher based on 128-bit blocks.Itcan work with key sizes 128,192 and 256 bits.the number of rounds of operation dependsupon the keys size

o 128 – bit key undergoes 10 rounds
o 192 – bit key undergoes 12 rounds
o 256 – bit key undergoes 14 rounds

AES is considered highly secure due to its long key sizes and is used in the industry today

AES Encryption and Decryption Process –

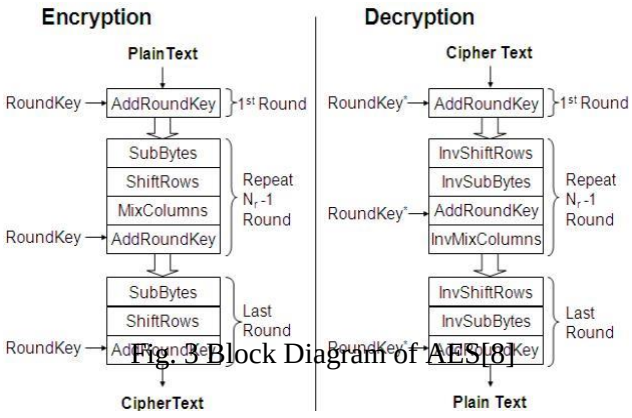


Fig. 3 Block Diagram of AES[8]

ISSN: 2233-7857 IJFGCN

Understanding of blocks –

1. AddRoundKey – In this transformation step, a round key is generated and XORed with the intermediate (temporary) ciphertext. This block is used in both encryption as well as decryption process.

2. SubBytes – In this transformation step, the intermediate ciphertext undergoes various substitution operations. It is used for encryption process.

3. ShiftRows – In this transformation step, the intermediate ciphertext undergoes various row-wise transpositions operations. It is used for encryption process.

4. MixColumns – In this transformation step, the intermediate ciphertext undergoes various column-wise transpositions operations. It is used for encryption process.

5. InvSubBytes – This is inverse of SubBytes operation. It is used in decryption process.

6. InvShiftRows – This is inverse of ShiftRows operations. It is used in decryption process.

7. InvMixColumns – This is inverse of MixColumns operation. It is used for decryption process.

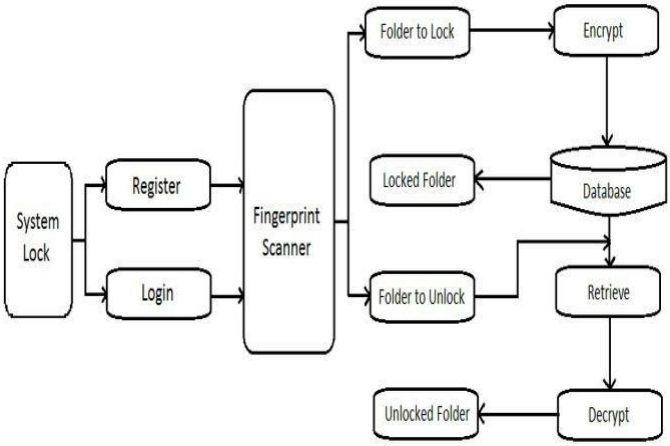
IV PROPOSED SYSTEM

A Unimodal Biometrics Folder Lock system based on Fingerprint Authentication is an application that needs a Fingerprint scanner. Figure below shows a basic block diagram for the system. It will basically consist of three modules. The details of modules is as follows –

1) *Fingerprint Registration*:
When user will install the software, in case he wants to lock the folder, he will need to register first.If he is already registered, he will need to login and then proceed forward.During login he will need to apply his finger which will be compared with existing fingerprints stored in the database. If matched, access will be granted otherwise denied.

2) *Folder Lock*:
After login is successful, he will get options of either lock or unlock a folder.In case of folder lock, he will need to browse for a folder in order to select a folder he desires to lock.The data of locked folder will be saved in an encrypted format, making it more secure.

3) *Folder Unlock*:
In case of unlocking a folder, when he will click on unlock option, he will get list of folders he has locked.He will need to choose a folder he desires to unlock.Then the folder will be unlocked.



ISSN: 2233-7857 IJFGCN

Fig. 4 Generalized Block Diagram for the System

V. ADVANTAGES

1. No need to remember passwords and pincodes.
2. Individual security identification.
3. By overcoming the limitation of existing system, the system is made to be platform independent.

VI CONCLUSION

This program is designed to overcome the limitations of the traditional password authentication system by entering a password through the Fingerprint Authentication System, which makes the system safer and more reliable. This Unimodal Biometric-Fingerprint Lock Folder Lock program works not only at the institution level for protecting sensitive data but also at every level of protecting personal data. The program is made with an improved GUI making it even more useful.

VII REFERENCES

1] Norhaiza Bt Ya Abdullah (2015). Folder Lock using Multimodal Biometric: Fingerprint and Signature Certification.

[2] Dr. Salah M. Rahal, Dr. Hatim A. Aboalsamah, Dr. Khaled N. Muteb (2006). Multimodal Biometric Authentication System - MBAS

[3] S. Mil'shtein, A. Pillai, A. Shendye, C. Liessner, and M. Baier (2008). Fingerprint recognition Alphabet with partial fingers and full fingers.

[4] Hao guo, Zong-Ying Ou, Yang He (2003). Automatic fingerprint classification based on embedded markov input models.

[5] Fulufhelo V Nwwondo (2011). Fingerprints showing a clear marking of a basic delta triangle.

[6] John Edgar Hoover (1963). The science of fingerprinting and its use.

[7] Avinash Navlani (2018). KNN classification using Scikit-read.

[8] Prabhakar T (2011) .AES-Encryption-Decryption-Flowchar.

ISSN: 2233-7857 IJFGCN