A Systematic Literature Survey:Folder Lock Security Using Fingerprint Authentication

Neha Kharkhande[1], Shrutika Sonawane[2], Sakshi Rane [3], Pradnya Wathore[4,] Deepali Dhadwad[5]
[1,2,3,4]*Students, Department of Computer Engineering, Indira College of Engineering and Management, Pune, India*
[5] *Professor Department of Computer Engineering, Indira College of Engineering and Management, Pune, India*

***Abstract* - Our project is a Java implementation of AES algorithm for fingerprint encryption.**
Biometric traits are unique to each person and wherever he goes,it goes with him. Lock folder is one of method that used to ensure nobody intentionally gets access to your private and confidential information.
Fingerprint authentication is an efficient system, as opposed to password-based authentication, where the password can be lostor forgotten or hack.
It has been proved and has been tested that using fingerprint asan authentication method is more secure and reliable.

***Key Words*: AES, Biometric**

I.INTRODUCTION

A locked folder is a method used to ensure that no one intentionally has access to your private and confidential information. Currently used password-based systems have many associated inconveniences and problems such as requiring the user to remember passwords, passwords can be guessed or broken through brute force and also have non-rejection problemsis. In addition, the password authentication method is breakableas a keyword is allowed to access some. Therefore, it can be leaked and cracked using any method such as dictionary attack, or social engineering. Due to the drawback, this method lacks the universality of some features and the system's validation performance is the upper limit and the unacceptable error rate for a single modal authentication system. Multimodal biometric can be a combination of two types of any physical or behavioural biometric as it is applied in a system that has been developed. Therefore, a system is proposed to overcome the above problems by adding multimodal biometric authentication that will provide another layer of security. Those problems arebeing overcome and it has been proven that by adding another layer of security because authentication is more secure. It has been proved and tested that using a combination of two biometric methods, fingerprint and signature, as authentication method is more secure and reliable**.**

Biometric authentication (or simply biometrics) is to identify a person based on logical or behavioral characteristics such as fingerprint, face, iris, voice, signature, etc. So far, a variety of biometric recognition algorithms which combines computer vision, pattern recognition and image processing techniques have been proposed. On the other hand, we have proposed a unified biometric recognition algorithm using the signal processing based approach**.**

II. LITERATURE SURVEY

Multimodal biometric can be at least combination of two typesof any physical or behavioral biometric as it applies in the system that has been developed. Therefore, a system is proposed to overcome the aforementioned problems by adding multimodal biometric authentication will provide another layer of security. Those problems encountered have being overcome and it is proven that by adding another layer of security as the authentication is more secure. It has been proved and has been tested that using combination of two biometric methods, fingerprint and signature as an authentication method is more secure and reliable.[1]

One of the most challenging problems in fingerprint recognition continues to be establishing the identity of a suspect associated with partial and smudgy fingerprints left at a crime scene (i.e.,latent prints or fingermarks). Despite the success of fixed-length

embeddings for rolled and slap fingerprint recognition, the features learned for latent fingerprint matching have mostly been limited to local minutiae-based embeddings and have not directly leveraged global representations for matching. In this paper, we combine global embeddings with local embeddings for state-of-the-art latent to rolled matching accuracy with high throughput. This leads to a multi-stage matching paradigm in which subsets of the retrieved candidate lists for each probe image are passed to subsequent stages for further processing, resulting in a considerable reduction in latency (requiring just 0.068 ms per latent to rolled comparison on an AMD EPYC 7543 32-Core Processor, roughly 15K comparisons per second). Finally, we show the generalizability of the fused representations for improving authentication accuracy across several rolled, plain, and contactless fingerprint datasets.[2]

Security has always been a major concern for the households and the office environment, and for this concern various approaches are in place to address the problem. In the proposedsystem, fingerprints of the authorized users are enrolled and verified to provide access to a facility that is used by multiple users. A user can also be removed and a new user can be enrolled in the system. We have implemented a centralized control system from where we can control who can enter in which rooms and who cannot. This is an Arduino UNO device based flexible working device that provides physical security using the fingerprint sensor technology.[3]

Automatic fingerprint classification provides an important indexing scheme to facilitate efficient matching in large-scale fingerprint databases for any Automatic Fingerprint Identification System (AFIS). A novel method of fingerprint classification, which is based on embedded Hidden Markov Models (HMM) and the fingerprint's orientation field, is described in this paper. The accurate and robust fingerprint classification can be achieved with extracting features from a fingerprint, forming the samples of observation vectors, and training the embedded HMM. Results are presented on two fingerprint databases, Finger db. and Finger/spl I.bar/DUT, respectively.[4]

Most biometric systems deployed in real-world applications are unimodal, such as they use a single source of information for authentication (e.g., single fingerprint, face, voice...). Some of the limitations imposed by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity. In this paper, it is shown that fingerprint and face recognition can form a good combination for a multimodal biometric system and they are used in our work; where the system design in its hardware and software parts is done. The hardware part involves the capture devices, fingerprint signal processing unit, & PC. The software part includes the system software, databases, and face recognition module. The implementation of the system prototype as "Access Control System" with the suitable features was done.[5]

An urgent need to develop accurate biometric recognition system is expressed by governmental agencies at the local, state, and federal levels, as well as by private commercial companies. Fingerprinting is the most practical and widely used biometric technique. The pattern of ridges and valleys of each fingerprintis unique. The minutiae-based algorithm is widely used for fingerprint authentication. One of the significant parts of this algorithm is the classification of fingerprints which allows minimizing significantly the number of fingerprints referenced for each identification procedure. However, the minutiae algorithm has some serious drawbacks. If the core of a fingerprint is not visible, then identification cannot proceed. Yet in some cases, partial fingerprints need to be identified. We recently developed a novel contactless line scanner for recognition of fingerprint pattern that converts a three-dimensional object like a finger into a two-dimensional image with minimal distortion. This novel imaging technique based on a line by line scanned image required the development of a newrecognition algorithm. In this study, we propose two new algorithms. The first algorithm, called the spaced frequency transformation algorithm (SFTA), is based on taking the fast Fourier transform of the images. The second algorithm, called the line scan algorithm (LSA), was developed to compare partial fingerprints and reduce the time taken to compare full fingerprints. A combination of SFTA and LSA provides a veryefficient recognition technique.[6]

III. SYSTEM ARCHITECTURE

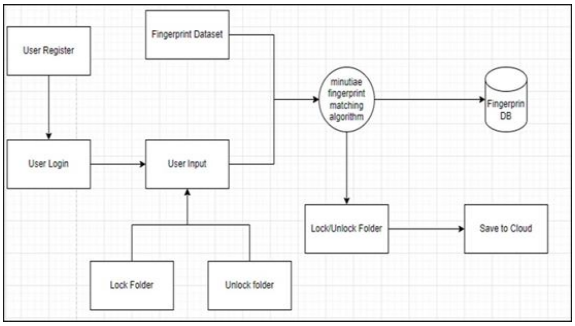

Fig -1: Architecture Diagram

1. User Register:

When a user registers, they typically enroll their fingerprint data into the system. This process involves capturing and storing unique characteristics of their fingerprint, such as ridge endings and bifurcations. These minutiae points serve asreference data for later authentication.

2. User Login:

To access the system, a registered user must initiate a login process. During login, the user presents their fingerprint to thesystem, which then attempts to match the presented fingerprint with the stored reference data. If the match is successful, the user gains access.

3. User Input in Lock Folder and Unlock Folder:

Once a user is successfully logged in, they can interact with the system to lock and unlock folders. Locking a folder typically involves selecting a specific folder and requesting that it be protected with fingerprint authentication. Unlocking a folder is the process of granting access to a previously secured folder, often by presenting the user's fingerprint.

4. Fingerprint Stored in Data set Using Minutiae FingerprintMatching Algorithm:

The minutiae fingerprint matching algorithm is used to extract and store key fingerprint features (minutiae points) in a data setor database. This data set serves as a reference for authentication. The algorithm compares minutiae points between the stored data and the fingerprint presented during authentication to determine if there's a match.

5. Lock and Unlock Folder and Saved to Cloud:

Locking and unlocking folders often involves encrypting and ddecrypting the folder's content using the user's fingerprint as the encryption key. Additionally, some systems may offer the option to save encrypted folders to a cloud storage service for backup and remote access. This can enhance data security andaccessibility.

IV. CONCLUSIONS

The fingerprint device-based system for securing the transactions of the user and providing the security for the User and even more for the Account verification using a finger printscanner has been followed.

This system is designed to overcome the limitations of traditional Password Authentication system by replacing password with Fingerprint Authentication System, making thesystem more secure and reliable. This Unimodal Biometric- Fingerprint Folder Lock system is useful not only at organizational level for protecting sensitive data but also at theindividual level for protecting personal data. The system is designed with enhanced GUI making it more user friendly. The fingerprint device-based system for securing the transactions of the user and providing the security for the User and even morefor the Account verification using a finger print scanner has been followed.

In the future we will try to increase Performance of the system in large amount of dataset and also implement speaking voice alarm can be used to indicate unauthorized person accessing the Account.

ACKNOWLEDGMENT

We would like to express our sincere gratitude to Prof. Deepali Dhadwad, whose role as project guide was invaluable for the project. We are extremely thankful for thekeen interest she took in advising us, for the reference materials provided, and for the moral support extended to us.We express our deep sense of gratitude and humble thanks,for his valuable guidance throughout the project work. Furthermore, we are indebted to Prof. Sunil Rathod Project Co-ordinator, Dr. Soumitra Das HOD Computer, Dr. Sunil Ingole Principal whose constant encouragement and motivation inspired us to do our best.

REFERENCES

[1] D. Florencio & c. Hurley, " Folder Lock by using Multimodal Biometric: Fingerprint and Signature Authentication"in WWW '07: Proceedings of the 16th International Conference on the World Wide Web. Banff, Alberta, Canada: ACM, 2021,pp. 657–666.

[2] Norhaiza Bt Ya Abdullah, Herny Ramadhani Bt Mohd Husny Hamid “Automated Latent Fingerprint

Recognition" A Global Perspectives, Vol. 17, no. 1, pp. 45–54, 2020.
[3] S. M. Rahal, H. A. Aboalsalamah, K. N. Muteb "Multimodal biometric authentication system" Proceedings of the annual meeting of the Human Factors andErgonomics Society, Vol. 53, pp. 459–463 (5), September 2020.
[4] H. Guo, Z. Ying Ou, Y. He "Automatic fingerprint classification based on embedded hidden markov models." 29th Proceedings Conference on Information Communication.Piscataway, NJ, USA: IEEE Press, 2019, pp. 983–991.
[5] J. S. Mil'shtein, A. Pillai, A. "Fingerprint recognition algorithms for partial and full fingerprints"Security and Privacy, IEEE, Vol. 2, No. 5, pp. 25–31, 2019.
[6] S. Madabusi, V. Srinivas, S. Bhaskaran and M. Balasubramanian, "On-line and off-line signature verification using relative slope algorithm," Proceedings of the 2005 IEEEInternational Workshop on Measurement Systems for Homeland Security, Contraband Detection and Personal Safety Workshop, 2005. (IMS 2005), Orlando, FL, USA, 2005, pp. 11-15, Doi: 10.1109/MSHS.2005.1502546.