IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

NCAIT 2017

JSS Academy of Technical Education

Vol. 4, Special Issue 8, May 2017

Biometric Encryption

Rashmi J. C[1]., Shohreh Kia[2]

Department of Information Science and Engineering, BMS College of Engineering, Bangalore[1, 2]

Abstract: Our project is a Java implementation of Chaos based algorithm for fingerprint encryption. Biometric traits are unique to each person and wherever he goes, it goes with him. It is a very effective identification system. A biometric trait, such as fingerprint, palm-print, iris-scan, face-scan, etc., is taken as marks to identify a person, as does our human brain. We have taken up fingerprint as our biometric trait, to experiment with, in our project. Fingerprint authentication is an efficient system, as opposed to password-based authentication, where the password can be lost or forgotten. Nevertheless, the security of the user's data and his biometric trait are a concern as they are unique to each person and can lead to identity theft if it's details get into the wrong hands. Hence, came forth the technique of encrypting sensitive data, so that, a random person who comes across this data will not be able to tamper with it, because, this data will not make any sense to him. When the authorized user needs it, it will be decrypted. A matching process will be implemented to match the provided user's fingerprint with that of the encrypted stored data, to cross check if the two are the same and grant access accordingly. There are several approaches in the recent years that have provided biometric revocability feature, but lack robustness and security. Chaos-based systems, on the other hand, have a good number of properties that are defined in the ideal features of secure cryptography, i.e., extreme sensibility to initial conditions withConfusion and, ergodicity with diffusion. We implement chaos based algorithm, using Java programing language, as a working software, where the system interacts with the user and allows him to register or sign-in to his account. The program is also connected to a securedatabase where the encrypted user data is stored. The scanning of image is done with the help of a fingerprint scanner. We use SMTP (JavaMail) to send an e-mail to the user if there has been any malicious activity detected on his/her account.This system is secure, effective at low cost and can be implemented on real, secure access control systems.

1. INTRODUCTION

As we all know, everything we do in our day-to-day life is being digitized for greater efficiency. We are now saving all our data online and making online transactions of various kinds (money, confidential information, etc.). The need for security for our data is also growing as we are storing most of our sensitive documentations online. Hence, to access such information, the conventional methods of using passwords seem inconvenient, since they can be forgotten or lost.

Biometric ways now enter the picture, where we use physical human traits such as fingerprint, iris, etc. as passcodes to get access to any sensitive components that need protection. These traits can neither be lost nor forgotten and are unique to each person.

The next aspect is, to make sure these biometric passcodes are safeguarded from theft, tampering and other ways of hacking. Hence, emerged Biometric Encryption.

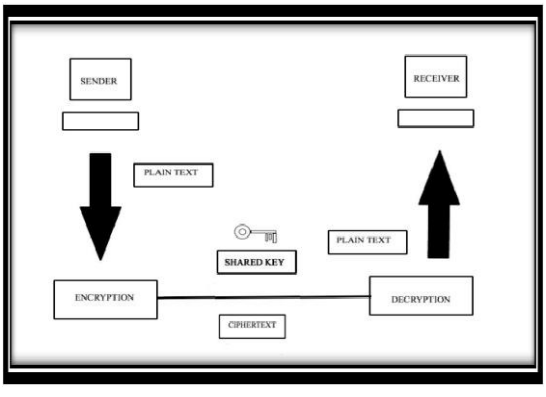
We looked into various methods of encrypting our biometric data, when we came across the latest paper published on IEEE platform, which used multiple chaotic maps and vectors to form an algorithm, with multiple iterations of varying values to form a robust system to safeguard the data.

He process of the working of the system, a new user gives his fingerprint via a scanner and other details, which are stored safely onto a database. The fingerprint (we use fingerprint as our biometric trait) is to be safeguarded by encrypting it, so that no one will be able to read or tamper it, if they gain access to this information.

When this registered user wants to login to his profile, he will give his fingerprint each time, along with his other details. The given fingerprint is matched with the fingerprint image stored in the database, after decryption. If the two values match, the user can login, otherwise, he will be denied access to his profile.

Using this basic methodology, our encryption algorithm is made complex by adding various layers to it, preventing it from being easily hacked by imposters, identity thieves and keeping our invaluable trait and data safe.

• BIOMETRIC: Measurable qualities of the individual in view of their physiological components/behavioral examples that can be utilized to perceive or check their personality.



IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

NCAIT 2017

JSS Academy of Technical Education

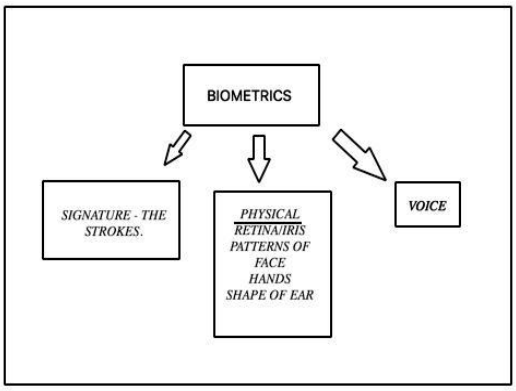
Vol. 4, Special Issue 8, May 2017

STANDARDS OF BIOMETRICS:

• Uniqueness: Distinction between people.
• Permanence: Resistance to maturing.
• Collectability: Ease to acquire a biometric for estimation.
• Performance: Accuracy, speed, vigor of the biometric framework.
• Acceptability: Degree of endorsement of an innovation.
• ENCRYPTION: It is the best approach to accomplish information security. To peruse a scrambled record, you should have entry to a mystery key or secret word that empowers you to DECRYPT it. Decoded information is called PLAIN TEXT; encoded information is alluded to as CIPHER TEXT.

UNIQUE MARK RECOGNITION:

- Fingerprints are special to every person and no two fingerprints are similar. Unique mark acknowledgment is most broadly acknowledged.
- Converts the picture of a unique mark into a numerical format of the print's particulars focuses.
- Fingerprints contains example of edges and valleys and also minutia focuses.
- Scanners: Optical scanners, Thermal scanners, Capacitances (strong state scanner), Minutia based, Correlation based.



• Fig II. Types of Biometrics

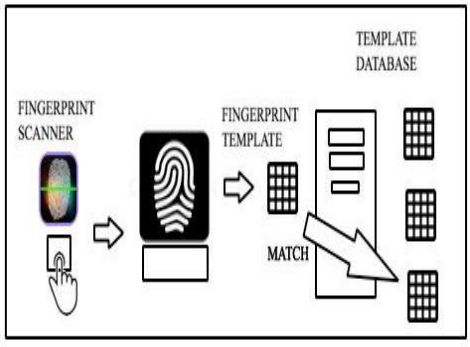


Fig III: Clearer picture of fingerprint authentication system

In the recent times, DNA cryptography has also been proposed. But, it is not very reliable, because of the influence of biological factors.

DANGERS TO BIOMETRIC SYSTEM:

• Attacks on the biometric sensor/Acquisition gadget
Case: use of incorporeal elements like a cut-off finger in the unique mark case or manufactured impersonations.
• Communication channel assaults (man-in-the-center assaults)
The principal sort is simply listening in, i.e., if the channel between the sensor and the component extraction unit or the one between the reference database and the coordinating unit is assaulted, the assailant can pick up data about the biometric information. In the second sort, deliberate utilize or change is done to the caught information for consequent presentation again into the framework.
Here are a couple of strategies that have established a solid framework to the present advances in biometric encryption frameworks:

• USING EMBEDED Frameworks:
Fons.M, Fons F., and Canto E. (2007). Installed security: New patterns in individual acknowledgment frameworks. (Departament d'EnginyeriaElectrònica, ElèctricaiAutomàticaUniversitatRovira I Virgili Tarragona, Spain) Most biometric frameworks are actualized utilizing installed frameworks (in view of programming and equipment).
• Uses processor with restricted computational power, constrained memory and I/O fringe.
• The minimal effort, low physical size, low power utilization, elite and adaptability are the significant focal points.
• Simple and successful utility and operation with complex programming.
• Demand being developed of constant control frameworks, with fast process and consistent operation immediately, engaged consideration and direct interface with sensor.

Client inserted equipment as microcontroller.
Case: FGPA field programmable door cluster.
Numerous biometric layout assurance actualized in different routes, in view of this be that as it may, client's format gets uncovered.

• FUZZY VAULT OR SECURE
Outline Procedure (Utilizing KEY Authoritative AND KEY Era): BIOMETRIC ENCRYPTION Teoh, A. B. J., and Kim J. (2007) (Secure biometric layout assurance in fluffy duty conspire. IEICE Gadgets Express, 4(23), 724–730.). Cavoukian An., and Stoianov A. (2007)(Biometric encryption: A positive-whole innovation that accomplishes solid validation, security and protection. Data and Security Official of Ontario, 48.).
Biometric cryptosystem plans secure cryptographic key with biometric or produce a cryptographic key frombiometric, utilizing fluffy vault method. The first biometric format is never put away in the database, just the cryptographic key, with some open information put away as partner date.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
NCAIT 2017
JSS Academy of Technical Education
Vol. 4, Special Issue 8, May 2017

• FEATURE Change and BIOMETRIC CRYPTOSYSTEMS:
Biometric Layout Security – Anil K. Jain, KarthikNandakumar and Abhishek Nagar
(To show up in EURASIP Diary on Advances in Flag Handling, Uncommon Issue on Biometrics, January 2008)
For biometric layout assurance their principle objective as revocability.

• SALTING and NON-INVERTABLE Changes:
Kaur. M, Sofat S., and Saraswat, (2010). Layout and database security in biometrics frameworks: A testing undertaking (Universal Diary of PC Applications, 4(5), 1–5.) As vigorous hashing and cancellable biometric.

• CHAOS BASED APPROACH:
Xiaomin Wang, Taihua Xu and Wenfang Zhang-Disorder Based Biometrics Layout Assurance and Secure Confirmation. Confusion Based Biometrics Format Assurance and Secure Confirmation (School of Data Science and Innovation, Southwest Jiaotong College China) (2011) Extraordinary affectability to beginning conditions and control parameter, blending information, ergodicity, pseudo irregular conduct, determinism, and so on. These properties are very related with the cryptographic properties to make phenomenal encryption calculation with incredible perplexity and dispersion process and many-sided quality in source framework.
Riotous MAPS: For picture encryption at Matlab recreation level, where most plans utilize dissemination and disarray design.

2. DESIGN

• **Programming Language**
Selection: Java
• **User Interface:** We have a userinterface where the user can input fingerprint image/fingerprint image scanned for enrollment or authentication.
• **Plaint Template:** The RGBvalues of each pixel are obtained and stored in an array.
• **Key Generation:**.A non-linearchaotic logisitc map formula is applied to each of the RGB values of the pixels, thereby forming a key for each pixel. With a fixed initial value, thenewly formed value is used as initial value, for next key genereration.
Encryption Process: Each pixel value is XOR-ed with each of the corresponding key and iterated 1000 times.
• **Database:** We save cryptogram in the database.
Decryption/Matching: Thecryptogram is extracted, key is generated again and negative XOR-ed to obtain plain text values. The decrypted cryptogram image values and newly scanned image values are matched, obtaining POI values. More POI values match, lesser the distance, implying a match.

ARCHITECTURE
We have an user interface where a user can register, if he doesn't have an account already. If he does, he can Log-in. To enroll as a new user, user details are asked for , along with his fingerprint (scanned by the scanner). If all the details are filled in, the fingerprint image is encrypted and the entry is saved onto the database.
When the user wants to log-in to his account, he has to provide the valid/right username and password(used during enrollment) , with the fingerprint. The encrypted file is called from the database, decrypted and matched with the fingerprint image that is newly scanned. If there is a match, user is directed to the new window. Otherwise, an error message is shown, implying failed authentication.
If the user has more than three failed attempts, an email is sent to the provided email-id, intimating the user of malicious activity and also, blocks the user from logging into his account for a minute.

2.1 Implementation
Our Work is divided into three major modules.

1. Registration
In first module user's personal details, such as: name, mail id, contact number - are received by using the registration form. In addition to that thumb impression of user is received by using finger print scanner.

2.2 Encryption and Decryption
In this module before storing the details into database, using the chaotic encryption algorithm will encrypt thumb impression of user. When the user is to be authenticated, the cipher text of the user ID is extracted from the database and decrypted for matching.

2.3. Validation
In this validation process given thumb impression on login page and decrypted original thumb impression will be matched by using feature extraction process. Key points of both images will be extracted first and those points' values are matched to ensure the originality. If same key points are identified then user will be validated, else, user will be invalidated by authentication system. More than 3 failed attempts will lead to the intimation to user via mail using SMTP communication.

2.4 Coding
We use java for our coding, MySql to store data, java swing for the user interface and SMTP for email service.
In our algorithm, the pixel data from the scanned image is first obtained and stored in an array. Key generation is done for the size of this array . We use a formula to generate this key, with initial value being fixed. Each value obtained by the formula is used as input value for the next key generation.

The pixel values are in decimals and we multiply it by a value to round them off. We apply modulous of 256 for this value, because pixel values are to be in the range of 0-256.
Next, we XOR the keys with each of the R, G amd B values of the pixels separately, to increase complexity.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

NCAIT 2017

JSS Academy of Technical Education

Vol. 4, Special Issue 8, May 2017

For authentication, we call the encrypted file to decrypt it. We match the decrypted image with the newly scanned fingerprint using Feature matching, by taking points of interest POIs from the two images, making two arrays. If the correspoding values of both arrays match, there is a match and the user is successfully authenticated.

SMTP

SMTP is an acronym for Straightforward Mail Exchange Convention. It gives a system to convey messages. JavaMail Engineering: The java application utilizes JavaMail Programming interface to create, send and get messages. The JavaMail Programming interface utilizes SPI (Specialist organization Interfaces) that gives the intermediate administrations to the java application to manage the distinctive conventions.

3. CONCLUSION

A cryptographic framework must be exceedingly touchy at little varieties (at bit level) in mystery key, in both encryption and unscrambling process, which is accomplished in our framework, with the disarray and dissemination forms, and the cycles to expand arbitrariness.

Right now, an encryption framework needs more than 2to the power10 mystery keys as per a couple of distributions, which are solid, i.e. each key must create riotous information to oppose a comprehensive assault, where every conceivable key is attempted until locate the plain layout. We utilize another key for each RGB esteem in every pixel, independently. On the off chance that the encryption procedure creates diverse encoded formats from comparative plain layouts (one piece distinctive between them), even by utilizing a similar mystery key, the encryption calculation is considered very touchy at plain format, exhibited in our work. In our plan, the biometric attribute could be lost if the encryption calculation is broken or the mystery key is known by an enemy. All things considered, we can accomplish a thorough security investigation to accomplish differences, security and execution. The essential drawback of our plan is the irreversibility of the biometric quality, since we require play out the coordinating procedure at plain area level. We can enhance the framework to a more noteworthy level, by adding to the framework the ability to utilize at least two biometrics, i.e., for instance, voice acknowledgment with unique mark format.

ACKNOWLEDGMENT

We express our deep sense of gratitude to our respected and learned guide, Asst. Prof. Sowmya K. S., for her invaluable help and guidance. We are thankful to her, for her constant encouragement and support during the difficulties we faced in the making of our project. Her kindness instilled a sense of courage and a greater drive to accomplish our project.

We are also grateful to our project coordinators who set us time frames to complete various phases of our project, which helped us approach our project implementation in a well organizedmanner. And, it goes without saying, their encouragement and positive reinforcement when it was much needed was a great boost.

We are also thankful to our HOD, Dr. Radhika K. R. and our principal DrMallikharjunaBabu K, for providing us with such a wonderful opportunity to explore and experience the real application of our knowledge, acquired in Information Science Engineering.

We are very grateful to our entire faculty and staff. We truly feel we are in the best department, with the entire faculty being absolutely down to earth and helpful at every possible time, when we, as students have approached them. They have been supportive from the beginning and never stopped at anything. They made us feel at home and have truly made our experience in college as if it was our second home.

Lastly, our classmates, who are brilliant, open-minded, always supportive and loving, and our amazing parents who have been there with us through everything, trusting in our future, in us, even when we could not.

REFERENCES

1. A new image encryption algorithm based on logistic chaotic map with varying parameter Lingfeng Liu and Suoxia Miao (https://www.ncbi.nlm.nih.gov/ pmc/articles/PMC4781823/)
2. Minutiae-based template synthesis and matching for fingerprint authentication Tamer Uz , George Bebis , Ali Erol a, SalilPrabhakar (https://www.cse.unr.edu/~bebi s/TamerCVIU09.pdf)
3. Finger Print Matching based on Miniature and PHOG Feature Extraction M. Malarvizhi , M. Madlin Asha , S. Sinduja (https://www.ijarcsse.com/docs /papers/Volume_5/10_October 2015/V5I10-0301.pdf)
4. A new image encryption algorithm based on logistic chaotic map with varying parameter Lingfeng Liu and Suoxia Miao (https://springerplus.springerop en.com/articles/10.1186/s40064 - 016- 1959-1)
5. Secure Biometric Authentication System using Chaotic Encryption Abirami S1, Harini T2, Annapoorani N3 (https://www.irjet.net/archives/ V3/i4/IRJET-V3I4140.pdf)
6. Using embedded systems. Fons.M, Fons F., & Canto E. (2007). Embedded security: New trends in personal recognition systems. (Departamentd'Enginyeria Electrònica, ElèctricaiAutomàticaUniversitatRoviraiVirgili Tarragona , Spain)
7. Teoh, A. B. J., & Kim J. (2007) (Secure biometric template protection in fuzzy commitment scheme. IEICE Electronics Express, 4(23), 724–730.). Cavoukian A., & Stoianov A. (2007)(Biometric encryption: A positive sum technology that achieves strong authentication, security and privacy. Information and Privacy Commissioner of Ontario, 48.).
8. Biometric Template Security – Anil K. Jain, KarthikNandakumar and Abhishek Nagar (To appear in EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics, January 2008)
9. Kaur. M, Sofat S., & Saraswat, (2010). Template and database security in biometrics systems: A challenging task (International Journal of Computer Applications, 4(5), 1–5.)
10. Xiaomin Wang, Taihua Xu and Wenfang Zhang- Chaos-Based Biometrics Template Protection and Secure Authentication. Chaos-Based Biometrics Template Protection and Secure Authentication (School of Information Science and Technology, Southwest Jiaotong University China) (2011)