

Usage of Biometric Security In Web Based Architecture

Ekta Rani

Dept. of Computer Engineering
Lovely Professional University, India
ktsan313@gmail.com

Sumit Bansal , Aman Tyagi

Dept. of Computer Science & Engineering
Gurukula Kangri Vishwavidyalaya, Haridwar

sb002@ymail.com

aman.tyagi74@gmail.com

Abstract — In commercial sites and net services uses internet to achieve the targets or to provide services to consumer. State of technology now days despite of being fully cultivated, have certain security flaws because of these users are in doubt to use internet services for critical data. Some matter of content that occurs are cyber threats, security, authentication and confidentiality etc.

To vanquish such security issues, 2 level protection will be provided if we use biometric & password [1]. This work, biometric and password both type of protection is merged in one design which can serve two level security. By considering the future use of such design on the broad network like on model itself RSA Encoding used.

Keywords— *Finger print recognition, Password, OTP, Fingerprint matching, Encryption.*

I. INTRODUCTION

With the speedy evolution of data technology, individuals have become even more of electronic connected. The ability to attain high level accuracy of automatic individual identification is becoming more critical. If there's money involved, scanners will unfortunately always follow. Modern hackers are refined, about a lot of the technology to area them off isn't. OTPs were alien as an added acceptable address of acceptance users, about it did not yield hackers continued to able them [2]. OTPs cannot longer be pondered secure because they've been attacked heavily in modern years.

Privacy issues in previous techniques: -

- Malwares: - Mobile phone malware, especially Trojans, which are helpful to intercept SMS messages that can contain One Time Password, are a rising threat.
- Brute Force: - Passwords and OTPs are the 4 or 6-digit alphanumeric codes which are produced dynamically with the usage of mathematical algorithms. There are software's which can generate combinations of 4 and 6 digits and strike them repeatedly on the OTP window to crack it.
- One has to trust the network providers to run a secure network. In the case of user roaming around in different networks, one has to trust multiple operators.
- Most of the cases when the data is created by any mobile phone connection then the SMS is not received. The user is not aware of this situation.
- Sometimes there are lots of traffic on mobile operators hence users are unable to get their OTP SMS on time.

For reducing the extent and to solve the problem we can use better and safer technique” BIOMETRICS”.

In the world of computer security, biometric techniques accomplish use of assessable physical characteristics of an alone to identify the individual automatically. Every human has one of affectionate attributes about him that can activated for the action of identification, including fingerprints, retinal patterns, and voice characteristics.

A. Biometric Authentication Techniques: -

This biometric technique is basically a pattern recognition technique which does the task of identification by deciding the authentication of certain physiological and behavioral appropriate bedeviled by the user. Designing an experimental approach to find out the way an individual entity is uniquely identified. An authentication process is possible with two modules:

- Enrollment module
- Identification or Verification module

B. Biometric Technologies Work: -

Enrolment-- This module plays important in enrollments of different biometric data. During the phase of enrollment, firstly some distinct biometric characteristics are read by biometric sensors. This biometric reader creates a digital representation of the individual’s characteristics in raw digital data. In adjustment to accommodate matching, this digital data is further used using feature extractor to create compact and expensive representations which is called a template. Conditional on the need of application and organization stored in central database.

Biometric Verification also called authentication which helps to verify a person’s identity, to know for sure the particular is who he says he is. Identification is process used to organize a person’s authenticity. Although different biometric technologies make use of different aspects in various procedures, yet all these biometric technique systems start from an enrollment stage are followed by verification or comparing stage that use the features from enrollment data [5].

II. PROPOSED WORK

HOW TO USE BIOMETRIC SECURITY IN WEB BASED ARCHITECTURE

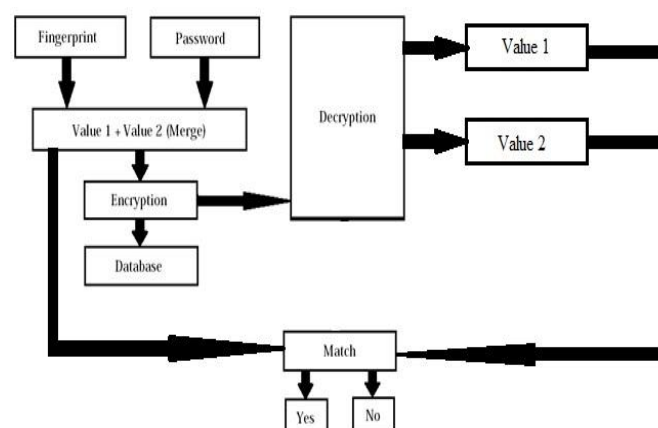


Figure 1: Purposed Model

- Fingerprint image: - this is the first inputs of security parameters. Fingerprint image is acquired by biometric fingerprint sensing device. The saved images of finger prints are stored in database and fetched into our project to merge with password.
- Password: - password is the 2nd parameter considered for security enhancing purpose. Password may contain numerical, alphabets and should be of six or more characters. In proposed work, we merge static password with finger print images.
- Encryption: - Encryption is the process to encrypt merged data which converts the plain data to ciphered data. Algorithm use to encrypt merged data is RSA algorithm.
- Database: - In Database, structured form of the data is stored. Encrypted data stored in the ASCII coding. This database holds the encrypted data which is added acclimated for decryption and matching.
- Decryption: - decryption is the process to covert the cipher data into the plain data. This plain data is help to matching purpose i.e. authenticating the user.
- Matching: - This step involves the matching of decrypted data to previously saved data from database.

III. BACKGROUND DATA

A. Merits of using Fingerprint Biometric

- Generality–Fingerprint exists with every discrete person. There are very rare people who may not have fingers that makes sparse case.
- Isolated–Every fellow has a unique fingerprint. Fingerprint patterns cannot be same of two persons.
- Ineradicable–Fingerprint remains forever with human beings. It is generated from the development of fetus that is of seven months and remains till the death.
- Biometrics cannot be neglected, duplicated, misplaced or pilfer.
- It is very secure because it cannot be used by others [3].

B. Demerits of Biometric

- Biometric systems must have the ability to carry the changes due to illness or injury.
- False rejections and acceptances must be led by the fingerprint scanner.

C. Fingerprint Processing Workflow

A fingerprint processing workflow is visible in the figure shown below. That will be explain all the steps and their usage.

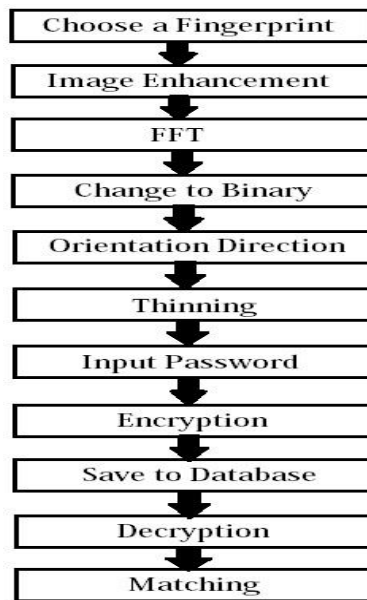


Figure 2: Figure print processing workflow

- *Image Enhancement*

Fingerprint Image enhancement provides better images to be used in further operations easily. The biometric sensors acquired are in the given below fingerprint image or any different means which is not consistent and assured with the entire quality, enhanced methods can increase the contrast between valleys and ridges which are accessible to join the false broken points of ridges because of inadequate ink amount. These operations used for enhancement are helpful in controlling the high accuracy in fingerprint recognition (figure1).



Figure 3 : Fingerprint Image Enhancement

So, for this part of research, image enhancement can be done by using following two methods: Histogram Equalization; and Fourier Transformation (FFT).

- *Histogram Equalization*

In Histogram equalization, we can increase the amount of pixel distribution in any image so that the compassionate information can be increased. The output of the result after histogram equalization is in Figure 4.



Figure 4 : -Left (Original Image) Right (His. Equalization)

- *Fingerprint Enhancement by Fourier Transform*

The image is transmitted into small blocks that are in processing (32*32 pixels or 16*16 pixels). To improve the dominant frequencies of the specific block, Fast Fourier Transformation of the block is measured by multiplying its magnitude for set of times. The resultant image after we apply a Fast Fourier Transformation will have the propensity to connect the false broken points on ridges and helpful in omitting some false connections which are between ridges.

- *Fingerprint Image Binarisation*

In this step, binarisation helps to explain the exact information that may be copied from a fingerprint kind of simple binary, valleys and ridges. But it is an absolutely necessary starting in ridges extraction process, and prints are on grayscale, thus ridges change in terms of intensity values. Binarization of the image depicts that from a 256 level of image to a 2 level of image provide the common data. Typically, “1” value is for object pixel and “0” value is given for background pixel.

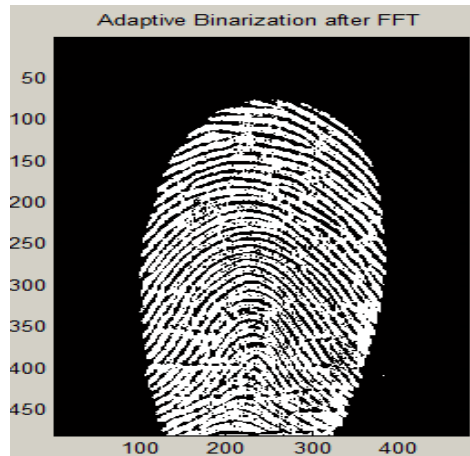


Figure 5 : Adaptive Binarization after FFT

- *Fingerprint Image Segmentation (Orientation Flow estimate)*

Normally, Interest regions are important that to recognize for each fingerprint image. At first, abandon the region of the image which does not have the effective ridges as it only carries surroundings data and sound [11].

- *Block Direction Estimation*

Make the estimations that is for the block direction, for every block in the fingerprint image that is with $W \times W$ in size (W is 32 pixels by default).

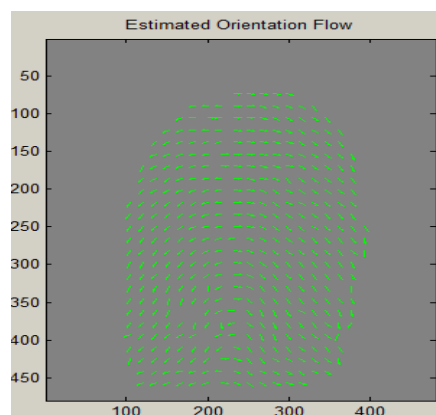


Figure 6 : Estimated Orientation Flow

- *Extraction of ROI from Morphological operation*

There are two operations of Morphological that are known 'OPEN' and 'CLOSE'. The operation 'OPEN' is used for expanding images and erasing peaks that are produced from background noise. The operation 'CLOSE' helps to shrink the images and also removing small cavities present in image.

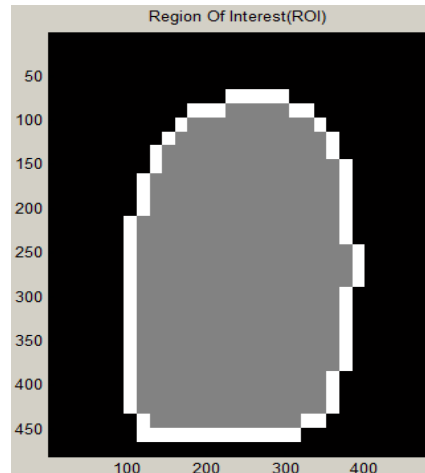
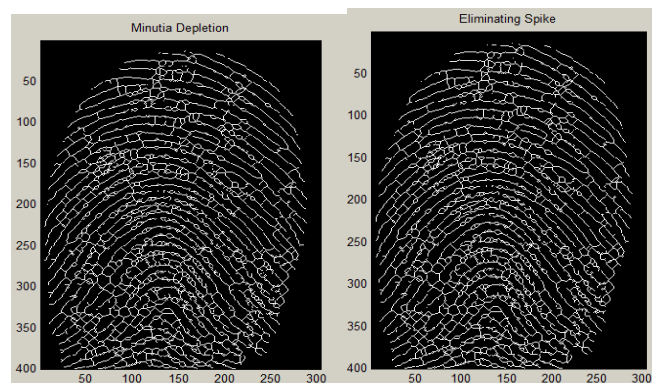


Figure 7 : Reason of Interest

(Figure 8) depicts the particular fingerprint image area with bound of fingerprint. The deduction of the area that is closed with the area that is opened is called bound. Then, removes those left-most, right-most, upper-most and bottom-most out of bound blocks that is to achieve the region of tightly bound including the bound and inside area [9].

- *Fingerprint Ridge Thinning*

The process of Ridge Thinning is used to omit the ridges pixels that are not in use till the ridges are of one-pixel width. To do this, we use an iterative, parallel thinning algorithm. The algorithm to mark down unnecessary pixels in each small image of window (3 by 3) and then in the end, eliminates all those marked pixels after doing several scans.

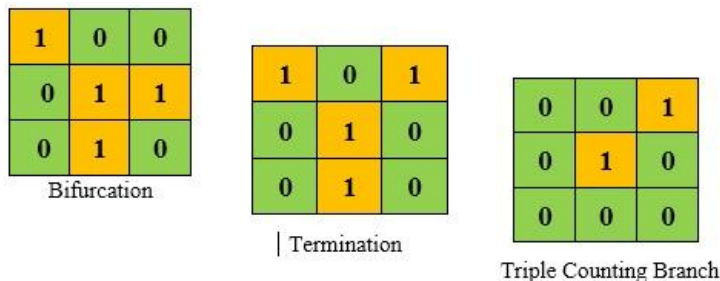


m Figure 8 : Thinning

Figure 9 : Eliminate Fault H and Spikes

- *Minutiae Marking*

As, after doing the ridge thinning on fingerprint image, marking the minutia points are easy to specify. The Crossing Number (CN) concept is usually taken into account for extracting the minutiae. Normally, for each window of matrix 3*3, the center pixel is of value 1 and also, has exactly three neighbors with value that is 1; therefore, the central pixel will be ridge branch.



For e.g., the value of the topmost pixel and rightmost pixel has the value and has other neighbor pixel outside the window of 3*3, so, the pair of the pixels will be active as branches, but in absolute there is only single branch is located in the small area. So, a analysis routine appended to apperceive that no one of branch neighbors are branches [6, 7].

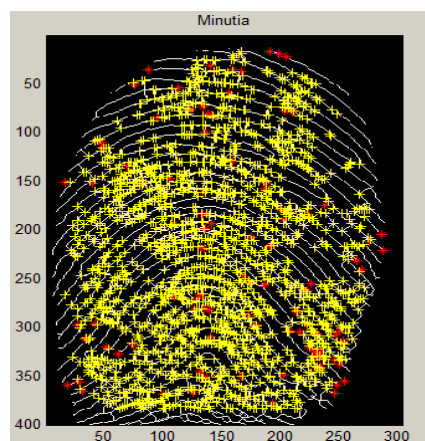


Figure 10 : Image After Minutiae Marking

IV. ALIGNMENT BASED MATCH ALGORITHM

The minutia matching algorithm examines whether the sets of two minutiae belongs to the same finger or not [4]. We compare the group of minutiae of fingerprint images with the database of images. This match algorithm based on alignment has consecutive stages: -

- **Alignment stage:** We have thirty fingerprint images, that are to be matched, then we can select any minutia from the database of images; then evaluation of the similarities of the ridges that are connected with the referred minutia marks. In case of value of threshold is less than the similarities found, then convert the set of minutiae into a new system of coordinates where initial point on the reference point and also with the referenced point direction x axis is ancillary.
- **Match Stage:** After obtaining the group of modified minutia points, the algorithm which will be used is the elastic matching algorithm and is helpful to evaluate the pairs of similar minutia points by presuming minutiae points that are having the same positions that is near to each other and directions are indistinguishable [8,10].

The final match ratios for fingerprints are: -

No. of total pairs that are matched / No. of minutia that are in fingerprint template.

(Interpretation: - The score calculation is $100 * \text{Ratio}$ and range is from 0 to 100. If the score exceeds more than specified threshold value (generally 80%), then result is of that the two fingerprints are from the same finger.

V. EXPERIMENTAL RESULT

Many number of the images have been experimented on the proposed algorithm and results shown in table1. In total nine hundred experiments were conducted on thirty images and matching percentage of each image was noted. These results are documented as Rejection ratio, both false acceptance and rejection table is given in below table. Evaluated outcome from finger print images experiments are:

Table 1: Result of Experiments

Biometric	Fingerprint
RR	66.7
FAR	0.28
FRR	0.33

VI. CONCLUSION AND FUTURE SCOPE

Purpose of this implementation is to maintain high level authentication and security. With the inclusion of biometric security there will be less reliability with OTP and more protection against security threats. This research work has taken biometric fingerprints and the password as the basic parameters. Biometric fingerprint values and password values are merged in a template and then the encryption is applied. RSA algorithm is used for encryption which uses public and private keys which provides confidentiality and authenticity. This system can be implemented in internet-based technology to prevent frauds and cyber thefts.

REFERENCES

- [1] International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 3, March 2016, "Secured Internet Banking Using Fingerprint Authentication" Priyanka Mahajan¹, Prof. B. Mahalakshmi⁵, Pune, Savitribai Phule Pune University, Pune, India.
- [2] "A Practical Guide to Biometric Security Technology" Simon Liu and Mark Silverman, 1520-9202/01/\$10.00 © 2001 IEEE.
- [3] Verginia Espinosa, "Minutiae detection algorithm for fingerprint recognition", IEEE AESS Systems Magazine, 2002.
- [4] Abinandhan Chandrasekaran and Dr. Bhavani Thuraisingham, "Fingerprint Matching Algorithm Based on Tree Comparison using Ratios of Relational Distances", Second International Conference on Availability, Reliability and Security.

- [5] Catalin LUPU, Vasile-Gheorghita GAITAN and Valeriu LUPU, "Security enhancement of internet banking applications by using multimodal biometrics", IEEE 13th International Symposium on Machine Intelligence and Informatics, January 2015.
- [6] Hossein Jadidoleslamy, "Designing A Novel Approach For Fingerprint Biometric Detection : Based On Minutiae Extraction", International Journal on Bioinformatics & Biosciences (IJBB) Vol.2, No.4, December 2012.
- [7] Aliaa A.A. Youssif, Morshed U. Chowdhury , Sid Ray and Howida Youssry Nafaa, "Fingerprint Recognition System Using Hybrid Matching Techniques", 6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2012).
- [8] Shashi Kumar D R, Kiran Kumar K, K B Raja, R. K Chhotaray, Sabyasachi Pattnaik, "Hybrid Fingerprint Matching using Block Filter and Strength Factors", 2010 Second International Conference on Computer Engineering and Applications.
- [9] Om Preeti Chaurasia, "An Approach to Fingerprint Image PreProcessing", I.J. Image, Graphics and Signal Processing, 2012, 6, 29-35, Published Online July 2012 in MECS DOI:10.5815/ijigsp.2012.06.05.
- [10] Bellamkonda sivaiah, Kotha Hari Chandana, "An Efficient Approach for Fingerprint Recognition by Matching Minutiae Pairings", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 2, February 2015, ISSN:2277 128X.
- [11] Ankita Mehta, "Design & Implementation of Features based Fingerprint Image Matching System", International Journal of Multidisciplinary and Current Research, Accepted 15 Dec 2014, Available online 20 Dec 2014, Vol.2 (Nov/Dec 2014issue).