Biometric Security with Password for Web Based Architecture

[1]Sumit Bansal, [2]Supreet Kaur
[1, 2]Deptt. of Computer Engineering, Punjabi University, Patiala, India-147002
Email: sb002@ymail.com

Abstract:

Commercial web sites and web services uses internet and its services to reach the user or consumer. Current state of art technology, even though quite sophisticated, has certain security flaws due to which users tend to doubt the use of internet services. Some of the issues that occur are security, confidentiality, Authentication and cyber threats *etc*. To overcome these problems, two level of protection is provided by using biometric and password [1]. In this research paper, biometric is used along with password merged in a template which provides two level security. Keeping in account the future usage of template on the internet, RSA encryption is applied on the template itself.

Keywords: Password, OTP, Finger print recognition, Encryption, Fingerprint matching,

Merging

I. INTRODUCTION

With the speedy evolution of data technology, individuals have become even more of electronically connected. As a result, the ability to achieve highly accurate automatic personal 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.
- In cases when a mobile phone creates a data connection it can't receive SMS messages and user might not be alive of this situation in most cases.
- 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 safety, biometrics give to techniques that 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*:* -

A biometric authentication is basically a pattern-recognition technique that does the task of identification by deciding the authentication of certain physiological and behavioral appropriate bedeviled by the user. Designing an experimental approach to determine how an individual is identified is a helpful issue. An authentication process can be differentiated into 2 modules:

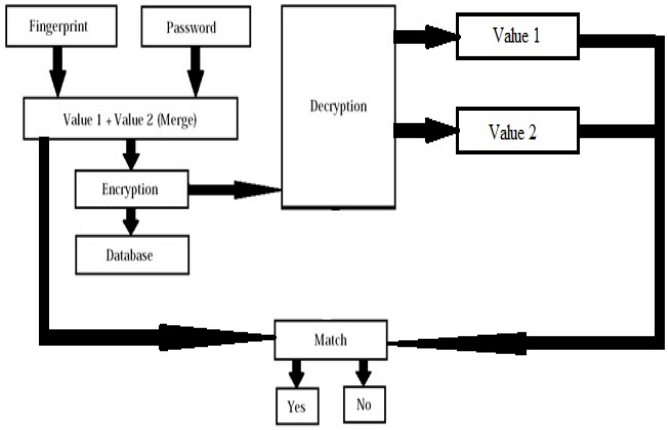
- Enrollment module
- Identification or Verification module

B. Biometric Technologies Work: -

Enrolment-- It is the module responsible for making 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 upon the requirement of application, the arrangement may be stored in central database.
Verification also called authentication is helped to verify a person's identity that is, 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 characteristics in quite different ways, yet all the biometric systems start with an enrollment stage followed by verification or matching stage that use the features from enrollment data [5].

II. Proposed Work

HOW TO USE BIOMETRIC SECURITY IN WEB BASED ARCHITECTURE



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: - structured form of the data is stored in the database. Encrypted data is saved in the ASCII form. 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

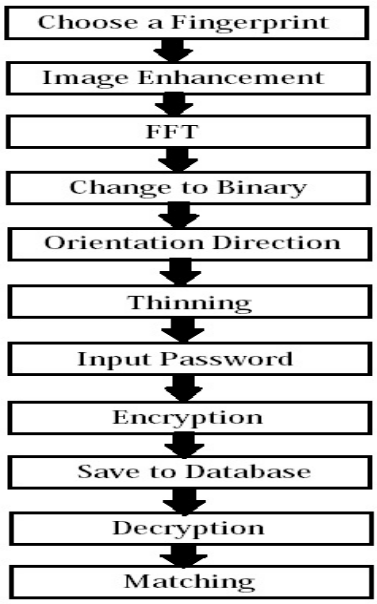
- Generality–Fingerprint exists with every discrete person. There are very rare people who may not have fingers that makes sparse case.
- Isolated–Every fellow has a unique fingerprint. fingerprint patterns cannot be same of two persons.
- Ineradicable–Fingerprint remains forever with human beings. It 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.



- **Fingerprint Image Enhancement**

Fingerprint Image enhancement is used to provide clearer and better image for using further operations easily. The following fingerprint images which are acquired from biometric scanners or any different means that are not consistently assured with absolute quality, enhancement methods are bare to increase the contrast between ridges and valleys that are as well accessible in joining the false broken points of ridges because of inadequate ink amount. These operations used for enhancement are useful in controlling the higher accuracy for fingerprint recognition (figure1).

Figure.1: - Fingerprint Image Enhancement

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

- **Histogram Equalization**

Histogram equalization is helpful in increasing the pixel amount distribution of an image so as to increase the compassionate information. The output of the result after histogram equalization is in Figure 4.

Histogram Equalization

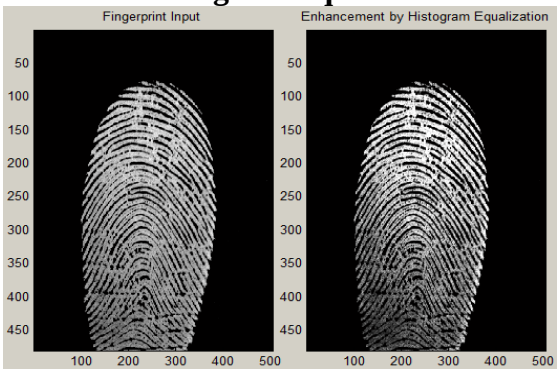


Figure 4: -Left (Original Image) Right (His. Equalization)

- **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, FFT of the block is measured by multiplying its magnitude for set of times. The modified image after applying FFT has the propensity to connect some falsely broken points on ridges and helps to omit some false connections that are between ridges.

- **Fingerprint Image Binarization**

The step, binarization helps in explaining the exact information that can be copied from a finger print is simple binary; ridges and valleys. But it is an absolutely necessary step in the process of extracting ridges, since the prints are in grayscale, so ridges, still differs in intensity values. Binarization of the image tells that from a 256-level image to a 2-level image gives the common information. Typically, "1"value is for object pixel and "0" value is given for background pixel.

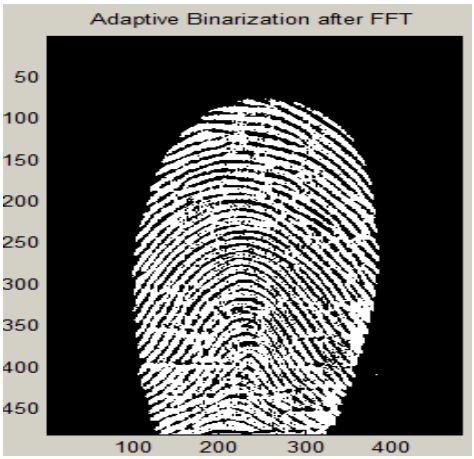


Figure 6: - Adaptive Binarization after FFT

- **Fingerprint Image Segmentation (Orientation Flow estimate)**

Normally, Region of Interest is important that is to be recognized for every fingerprint image. At first, abandon the region of the image which does not have the effective ridges as it only carries background information and noise [11].

- **Block Direction Estimation**

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

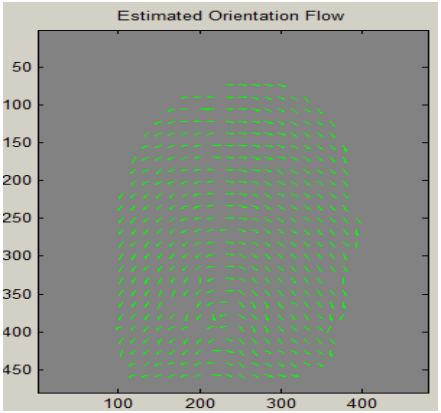


Figure 7: – Estimated Orientation Flow

- **ROI extraction by Morphological operation**

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

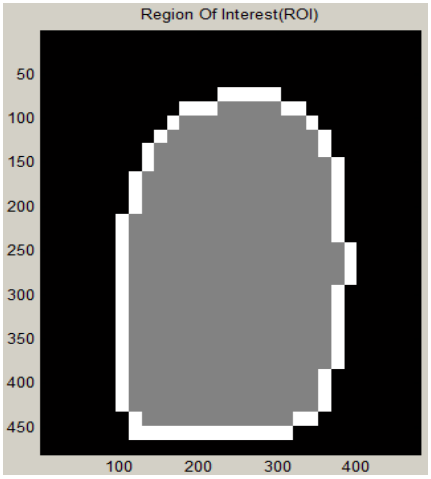


Figure 8: – Reason of Interest

(Figure 8) shows the interest fingerprint image area and its bound. The bound is the deduction of the area that is closed with the area that is opened. Then, removes those left-most, right-most, upper-most and bottom-most blocks out of the bound that is to achieve the tightly bounded region just containing the bound and inner area [9].

- **Fingerprint Ridge Thinning**

The process of Ridge Thinning is used to omit the pixels of ridges 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 is used to mark down the unnecessary pixels in each small image of window (3 by 3) and finally, eliminates all those marked pixels after doing several scans.

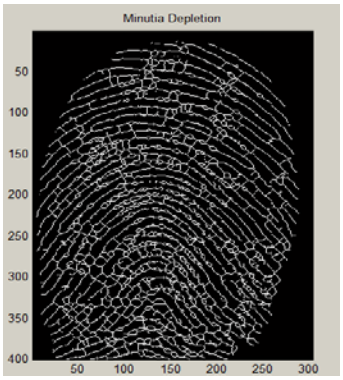


Fig. 9: Thinning

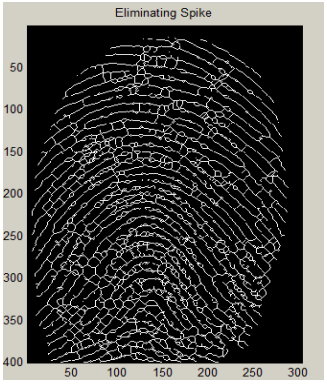
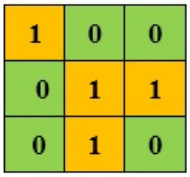


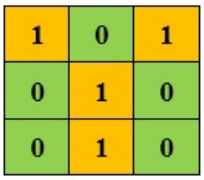
Fig. 10: Eliminate Fault H and Spikes

- **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 central pixel is of value 1 and also, has exactly three neighbors with value that is 1; therefore, the central pixel will be ridge branch.



Bifurcation



Termination

Triple Counting 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 is added to apperceive that none of the neighbors of a branch are branches [6, 7].

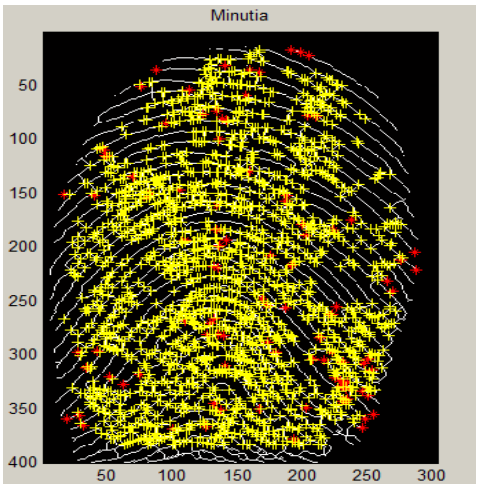


Figure 14: - Image After Minutiae Marking

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.
An alignment-based match algorithm is used. It has two 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 referenced minutia points. If the value of threshold is less than the similarities found, then convert the set of minutiae into a new system of coordinates where initial point is at the reference point and x-axis is ancillary with the direction of the referenced point.
- Match Stage: After obtaining the set of modified minutia points, the algorithm that will be used is the elastic match algorithm and is used to evaluate the pairs of similar minutia by presuming minutiae 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 the template fingerprint
(Interpretation: - The score is 100*ratio and ranges are from 0 to 100. If the score exceeds more than a pre-specified threshold (i.e. typically 80%), then the results is 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 table (1). 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, False rejection ratio and False acceptance ratio is given table. The results that are evaluated experimentally of the input fingerprint images are:

Table 1: - Result of Experiments

Biometric	Fingerprint
RR	66.7
FAR	0.28
FRR	0.33

VI. CONCLUSION AND FUTURE SCOPE

We have implemented a system for providing strong 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,Dec2014,Vol.2,Nov/Dec2014issue.