Improved Double Identitiy Fingerprint Recognition In Authentication System

S.Janarthanan[1],H.Mohamed Sirajudeen[2],K.R.Chandradevan[3]
Department of CSE,
Arasu Engineering College, Kumbakonam.

Abstract*— *Fingerprint is a very interesting and unique feature of the human body, because the Fingerprints can uniquely identify the person and it does not changes from birth to death. Even twines' fingerprints do not match. Due to persistent and uniqueness property of fingerprint it has been implementing in many areas such as UID Card, Passport, Criminal Data, etc. Fingerprints are unique pattern of ridges (raised) and furrows (recessed). That appears on the pads of fingers and thumbs. A person fingerprint Impression or mark made on any surface, able to be used for the unique natural pattern of common matching methods or structure such as delta and core on the tips of the finger. The pattern left on surface or uncovered fingerprints. Where all Minutiae cannot be covered such pattern is called as partial fingerprints. Partial fingerprints can also define as the subset of full fingerprints. The partial fingerprint having a small area as compares to full fingerprint from which to takes measurements of Minutiae. Due to this limiting factor of partial fingerprints it declines the degree of certainty of identity as well as the uniqueness of fingerprints. In this project, we can implement fingerprint recognition using neural networks. We can input the two fingerprints to increase the authentication efficiency and also provide improved accuracy rate. This project puts the implementation of Artificial Neural Networks to provide an efficient matching algorithm for fingerprint authentication. Using the Back-Propagation technique, the algorithm works to match double fingerprint parameters and relate them to a unique number provided for each authorized user. Upon matching, the algorithm returns the best match for the given fingerprint parameters.

I. INTRODUCTION

Biometrics refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are then distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice.

Some researchers have coined the term behavior-metrics to describe the latter class of biometrics.

More traditional means of traditional control include token- based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or pin. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information.

II. FUNCTIONALITY

Many different aspects of human physiology, chemistry or behavior can be used for biometric authentication. The selection of a particular biometric for use in a specific application involves a weighting of several factors. And identified seven such factors to be used when assessing the suitability of any trait for use in biometric authentication.

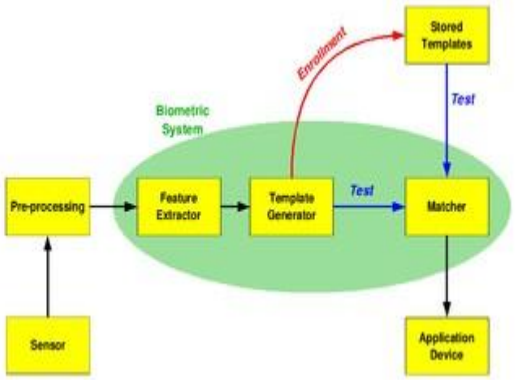
Universality means that every person using a system should possess the trait.

Uniqueness means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another.

Permanence relates to the manner in which a trait varies over time. More specifically, a trait with 'good' permanence will be reasonably invariant over time with respect to the specific matching algorithm.

Measurability (collectability) relates to the ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets.

Performance relates to the accuracy, speed, and robustness of technology used (see performance section for more details).
Acceptability relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed.
Proper biometric use is very application dependent. Certain biometrics will be better than others based on the required levels of convenience and security. No single biometric will meet all the requirements of every possible application.



The block diagram illustrates the two basic modes of a biometric system.[3] First, in verification (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps are involved in the verification of a person.[10] In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison. 'Positive recognition' is a common use of the verification mode, "where the aim is to prevent multiple people from using the same identity".
Second, in identification mode the system performs a one-to- many comparison against a biometric database in an attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold.
Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be". The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective. The first time an individual uses a biometric system is called enrollment.

During the enrollment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired.
The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way. A vector of numbers or an image with particular properties is used to create a template. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the file size and to protect the identity of the enrollee.
During the enrollment phase, the template is simply stored somewhere (on a card or within a database or both). During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm

mming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area). Selection of biometrics in any practical application depending upon the characteristic measurements and user requirements. In selecting a particular biometric, factors to consider include, performance, social acceptability, ease of circumvention and/or spoofing, robustness, population coverage, size of equipment needed and identity theft deterrence. Selection of a biometric based on user requirements considers sensor and device availability, computational time and reliability, cost, sensor size and power consumption

III. MULTIMODAL BIOMETRIC

Multimodal biometric systems use multiple sensors or biometrics to overcome the limitations of unimodal biometric systems. For instance iris recognition systems can be compromised by aging irises and finger scanning systems by worn-out or cut fingerprints. While unimodal biometric

systems are limited by the integrity of their identifier, it is unlikely that several unimodal systems will suffer from identical limitations. Multimodal biometric systems can obtain sets of information from the same marker (i.e., multiple images of an iris, or scans of the same finger) or information from different biometrics (requiring fingerprint scans and, using voice recognition, a spoken pass-code).

Multimodal biometric systems can fuse these unimodal systems sequentially, simultaneously, a combination thereof, or in series, which refer to sequential, parallel, hierarchical and serial integration modes, respectively. Fusion of the biometrics information can occur at different stages of a recognition system. In case of feature level fusion, the data itself or the features extracted from multiple biometrics are fused. Matching-score level fusion consolidates the scores generated by multiple classifiers pertaining to different modalities. Finally, in case of decision level fusion the final results of multiple classifiers are combined via techniques such as majority voting. Feature level fusion is believed to be more effective than the other levels of fusion because the feature set contains richer information about the input biometric data than the matching score or the output decision of a classifier. Therefore, fusion at the feature level is expected to provide better recognition results.

Spoof attacks consist in submitting fake biometric traits to biometric systems, and are a major threat that can curtail their security. Multi-modal biometric systems are commonly believed to be intrinsically more robust to spoof attacks, but recent studies have shown that they can be evaded by spoofing even a single biometric trait.

IV. EXISTING SYSTEM

In present system for electronic banking (e-banking) ,the user opens his account using his login which contains a username and the password provided by the bank for first time logging in. After opening the account he/she can compose of his own password. When logging in every time he/she has to enter the username and password for accessing the account. After opening the account for doing transaction the user has to enter an one time password (OTP) which will be send by the bank to the user mobile number. Once the OTP is entered the transaction is done successfully. Complex encryption software is used to protect account information. However, there are no perfect systems. Accounts are prone to hacking attacks, phishing, malware and illegal activities. Learning – Banks with complicated sites can be cumbersome to navigate and may require one to read through tutorials to navigate them. Transaction problems – face to face meeting is better in handling complex transactions and problems. Customary banks may call for meetings and seek expert advice to solve issues. User-ID and password can be captured using Trojan Horse programs. And also in existing system use single fingerprint recognition system to secure transactions. Fingerprint templates are stored in database and easily hacked by third parties. Then extend the approach to use mixed fingerprint templates are recognized, but difficult to separate the templates of fingers.

V. DISADVANTAGES

Provide complexity to create
templates Hacked by
malicious users
High error rate and less similarity
score values Templates are stored as
image values

VI. PROPOSED SYSTEM

Banking is not only focused on transferring money, but also to conduct many banking transactions with minimum time. Banking means any user can get connected to his bank's system with personal computer. But many hacking process is done in banking. To avoid these problems, novel algorithm has been developed for secure internet banking with finger print recognition. Therefore, there should be strong authentication provided for the Transaction process. Our system provides this authentication by using the biometrics of the User. The biometrics is in the form of Fingerprint of the user. In our system along with the Username and Password of the User he needs to provide his double fingerprints biometric for the transaction. For this the bank initially stores all the user details along with his double fingerprints. Our system will check for the biometrics of the user and match it with the original biometrics stored in the bank's Database. In this database, we can store the fingerprint features such as island, ridge end, core and delta values. These are maintained for double fingerprints instead of templates. If a valid match is found then only the user is Authenticated and treated as valid. Otherwise even if there is a small mismatch in the fingerprint the user is not allowed to access the Bank Account. The matching can be done using neural network algorithm to authenticate people who want to accede to an automated fingerprint system for Banking. The idea is to apply back propagation algorithm on a multilayer perceptron during the training stage. One of the advantages of this technique is the use of a hidden layer which allows the network to make comparison by calculating probabilities on template which are invariant to translation and rotation. Our system mainly focuses on the objective to provide security for online transaction and to see that the valid User should always get access to his account without any inconvenience.

ADVANTAGES

Difficult to hack the

adversary users Less

computational cost

Time
consuming
process

Preserve sufficient information about fingers

VII. MODULES

i. FINGERPRINT ACQUISITION

ii. FINGER FEATURES EXTRACTION

iii. ENROLLMENT IN DATABASE

iv. AUTHENTICATION

v. FEATURES MATCHING

VIII. FINGERPRINT ACQUISITION

In this module, image of Fingerprint is first acquired with the help of sensors. Captured images may be blurred or may contain noises, which Detroit the quality of an image and affect the performance of Fingerprint recognition system. The fingerprint image acquired may vary by location of finger placed, direction and stretching degree. After acquiring the image through sensors, preprocessing or image enhancement is done on the image. Sometimes image may contain noise while enrollment process, noise can be remove with help of filters utilized in processing/enhancement part of the processing. Sometimes there is a need of images normalization. A live- scan image is acquired by sensing tip of finger directly, using a sensor. Live-scan is done with the help of sensors. There are three types of sensors used. They are optical sensors, ultrasonic sensors and capacitance sensors. Our system uses Optical sensor (Fingerprint scanner).

IX. FINGER FEATURES EXTRACTION

An image, such as that of a fingerprint, may be considered as a two-dimensional continuous signal. By this, it can have an infinite number of brightness intensities in an infinitesimal area. In order for an image to be handled by a computer, it must first be digitized. For this study, the image had to be sampled in a different manner. In feature extraction phase, features of image are extracted such as Ridges, valleys, minutiae and singular points (loops, core, whorls and delta). These features are helpful for unique identification or verification of an individual. The features obtained from captured images are stored in database for further process of matching. The major minutia features of fingerprint ridges are ridge ending, bifurcation, and short ridge (or dot). The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges.

X. ENROLLMENT IN DATABASE

In this module, fingerprint features are stored in database. We can store double fingerprint entity for improved authentication. Then we stored these features numerical values instead of templates. These featured are saved along with registered details such as name, id, phone number, email and so on.

XI. AUTHENTICATION

This phase is known as login phase. User can enter into the system using user name and password. After that sensing fingerprints of same person with sub sequence press. Minutiae matching are required to check whether the input image is same as that stored in the bank database. Minutiae matching can be done using different techniques as Point matching i.e. the matching is done by comparing pixel by pixel. One pixel from the input image is taken and compared with one pixel from the reference image, Segment Creation the minutiae points extracted from the stage II are connected with each other using segments. The distance between each segment is calculated for both query and reference images.

XII. FEATURES MATCHING

Feature matching phase identifies similarities between current fingerprints features and previously stored features. Input images provided to the system are matched with previously stored features present in database. Matching is entirely dependent on whether the system Performs identification or verification. If it performs identification i.e. one-to-many matching approach is used, where fingerprint of an individual matches with all available templates in database otherwise one-to-one match is done for verification, where input image of a person is matched with double fingerprint features. It can be done by back propagation neural network algorithm which is the standard way of training neural networks. It works basically like this: The input pattern on which the network is to be trained is presented at the input layer of the net and the net is run normally to see what output it actually does produce. The actual output is compared to the desired output for that input pattern. The differences between actual and desired form an error pattern. Extract the features for both fingers at testing side. These features are matched with data base using classification approach. If there is match found means, user can be register into system, otherwise rejected.

XIII. CONCLUSION

We have implemented a system for providing strong authentication for online banking transactions

using fingerprint biometrics. Fingerprint recognition has various phases as image enrollment, preprocessing or enhancement, feature extraction and matching. The singular points are quite frequently features for classification. In a similar fashion, the rule based and neural network classifiers have been frequently used. It describes in brief about the enhancement, extraction and matching of fingerprint images. It contains the details of types of biometrics, its advantages over password/key authentication. It briefs about the image pre-processing techniques. The method has been used for feature extraction of minutiae. This method is able to detect accurately all valid bifurcations and ridge endings from the thinned image. For matching purpose back propagation neural network algorithm, has been trained as a fingerprints classifier to identify fingerprints with time effective preprocessing, which greatly increases the performance of the network. The recognition rate of fingerprints depends on the quality of fingerprints and effectiveness of preprocessing system. In this, input minutiae are aligned with the template by estimating the parameters between an input and features. The input which satisfies the matching score is declared as a matched fingerprint with the features.

XIV. FUTURE ENHANCEMENT

Nowadays everyone is using Internet on mobiles. So we can develop an android App for scanning the fingerprint biometric. We can use our inbuilt mobile camera for capturing fingerprint image and build up algorithms for improving the image enhancement.

REFERENCES

[1] A. Othman and A. Ross, "On Mixing Fingerprints," IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 260-267, January 2013.

[2] R. Cappelli, M. Ferrara, and D. Maio, "A Fast and Accurate Palmprint Recognition System based on Minutiae," IEEE Transactions on Systems, Man and Cybernetics - Part B, vol. 42, no. 3, pp. 956-962, June 2012.

[3] R. Cappelli and M. Ferrara, "A fingerprint retrieval system based on level-1 and level-2 features," Expert Systems with Applications, vol. 39, no. 12, pp. 10465–
10478, September 2012.

[4] J. Galbally, R. Cappelli, A. Lumini, D. Maltoni, and J. Fierrez, "Fake fingertip generation from a minutiae template," in International Conference on Pattern Recognition, Tampa, FL, 2008, pp. 1-4.

[5] R. Cappelli, M. Ferrara, and D. Maltoni, "Minutia Cylinder-Code: a new representation and matching technique for fingerprint recognition," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 32, no. 12, pp. 2128 - 2141, December 2010.