HIGH LEVEL SECURITY IN MULTI BIOMODEL SYSTEM USING FINE QUANTIZATION TECHNIQUE

S.Nishanthini[1] ,Dr.R.Nallusamy[2]
PG scholar[1] , Principal[2]
Nandha College of Technology,Erode.
nishamani94@gmail.com

Abstract

Biometrics has pervaded other aspects of security applications that can be listed under the topic of "Biometric Cryptosystems". The popularity of biometrics and its widespread use introduces privacy risks. To mitigate these risks, solutions such as the helper-data system, fuzzy vault, fuzzy extractors, and unimodel biometrics were introduced, also known as the field of template protection. In parallel to these developments, fusion of multiple sources of biometric information has shown to improve the verification performance of the biometric system. Propose the first practical and secure way to integrate the multi biometric into cryptographic applications. A repeatable binary string from templates, which call a cryptography key, is a fusion value generated reliably from genuine fingerprint, iris and face features codes. In particular, our goal is to design cryptographic protocols for multi biometrics in the framework of a realistic security model with a security reduction .Protocols are designed for multi biometric based encryption, signature and remote authentication. This project deals with three approaches of extracting ridge features points, texture features, and ROI (Region of Interest) properties from fingerprint, face and iris and gives the optimal solution. Then, the extracted features are fused at the feature level to obtain the multi-biometric template. Finally, a multi-biometric template is used for generating an m-bit cryptographic key.

I. INTRODUCTION

Biometric-based authentication systems are widely considered to be more reliable than personal identification number (PIN) or password systems for verifying individuals and ensuring they are who they say they are. Lack of security technologies and weak authentication methods often causes devastating financial data breaches, leading to significant financial losses to customers and large regulatory fines levied on financial organizations. So *b*iometric cryptosystems (BCSs) are designed to securely bind a digital key to a biometric or generate a digital key from biometric offering solutions to biometric dependent key-release and biometric template protection. Replacing password-based key-release, BCSs brings about substantial security benefits. It is significantly more difficult to forge, copy, share, and distribute biometrics compared to passwords. Most biometric characteristics provide an equal level of security across a user-group (physiological biometric characteristics are not user selected). Due to biometric variance, conventional biometric systems perform "fuzzy comparisons" by applying decision thresholds which are set up based on score distributions between genuine and non-genuine subjects. In contrast, BCSs are designed to output stable keys which are required to match a 100% at authentication. Original biometric templates are replaced through biometric-dependent public information which assists the key-release process. Online banking is now very popular among consumers because it provides a convenient way to perform transactions from anywhere using smart devices like a laptop, computer, and even smart phones. However, these emerging online banking transactions are highly vulnerable because identity thieves are using high-tech methods to gain access to user information such as passwords, PINs and security questions. Even tokens are not safe to perform online transactions! Implementing a biometric authentication system in the online banking system will help this industry to protect customer's identity and financial information by providing stronger authentication methods like fingerprint scanning, facial recognition, and voice recognition. Due to the fact that biometrics are unique for every individual and cannot be easily forged, it will protect customer information from being compromised by fraudsters. Many computers, laptops, and even smart phones already have webcams, microphones, and fingerprint scanners, offering flexibility for banks to easily adopt biometric authentication for online banking services. The security of the online banking application is addressed at three levels. The first concern is the security of customer authentication information as it is sent from the customer's to the web server. The second area concerns the security of the environment in which the online banking server and customer information database reside. Finally, security measures are in place to prevent unauthorized users from attempting to log into the online banking section of the Web site. To implement this security system currently facing some problems like noisy sensor data, non-universality and/or lack of distinctiveness of the biometric trait, unacceptable error rates, and spoof attacks affects biometric systems which utilize a single trait for recognition (i.e., unimodal biometric systems). This can be surmounted via multimodal biometric systems (a probable improvement of biometrics technology) and this is achieved by strengthening the proof attained from diverse sources. Multimodal biometric system utilizes a minimum of two and more than two single modalities. Some examples are face, gait, Iris and fingerprint, to enhance the recognition accuracy of conventional unimodal methods. By bestowing supplementary useful information to the classifier, multiple biometric modalities have shown decreased error rates. Diverse characteristics can be utilized by an individual system or independent systems which can function separately and their decisions may be combined. In disparity to unimodal biometric authentication, the security and efficiency can be increased using the multimodal-based authentication and therefore for an opponent to spoof the system would be of very complex owing to a pair of distinct biometrics traits.

II. EXISTING SYSTEM

The privacy of the communications between user (user browser) and bank servers is ensured using encryption (cryptography). Encryption scrambles messages exchanged between user browser and online banking server. Unfortunately due to severe online attacks several encryption methods leaked the data's so move on to biometric cryptosystems. Methods of fingerprint recognition can be classified into two main categories: texture-based and minutiae-based. The first method extracts patterns of valleys and ridges of fingerprint images as the distinctive features of an individual while the second method uses minutiae information (referred to ridge ending and ridge bifurcation) to identify and verify users. In comparison, minutiae-based matching methods are more reliable, thus being widely-studied in the past decade.

2.1 Drawbacks

- Pre-alignment is only acceptable in research but not practical in real-life applications because of the original template’s inaccessibility in the encrypted domain.

- As a result, matching based on automatic alignment may lead to a high FRR (false rejection rate).

  Reference points may leak some information about the original template.

  An attacker distinguish between genuine and chaff points in a fuzzy vault, which reduces system security.

  Recognition accuracy of existing alignment-free fingerprint cryptosystems is insufficiently satisfying.

  Attacker obtains the helper data (the vault or sketch), he can bypass this filter and directly recover the key/template.

III. PROPOSED STSTEM

Biometric identification methods are automated and provide fast and accurate customer authentication. Due to the fact that biometric systems can provide optimal identification accuracy and security, the technology is already in use with several application. As a reliable security tool, biometrics in banking can eliminate loopholes of a banking system that criminals can exploit and has the versatility to secure all financial transactions such as branch banking, internet banking, mobile banking, and ATM networks. Adopting biometrics for customer identification in a banking system secures transactions and brings numerous benefits and a positive impact in this industry. Considering the issues in existing work propose a security-enhanced alignment-free fuzzy vault-based fingerprint cryptosystem using pair-polar (P-P) minutiae structures. Fuzzy vault is a practical and promising scheme, which can protect biometric templates and perform secure key management simultaneously.

3.1 Advantages

- As this design removes the probability that a query feature matches multiple points in the vault, decoding time is significantly reduced.

  The fine quantization used in our system can largely retain information about a fingerprint template of user and enables the direct use of a traditional, well-established minutiae matcher in bank server.

  The experimental results on a wide selection of publicly available databases show that the proposed system outperforms other similar systems while providing strong security i.e strong user authentication.

  Adopting a biometric banking system can provide a convenient way for banks to quickly and accurately authorize customer identities.

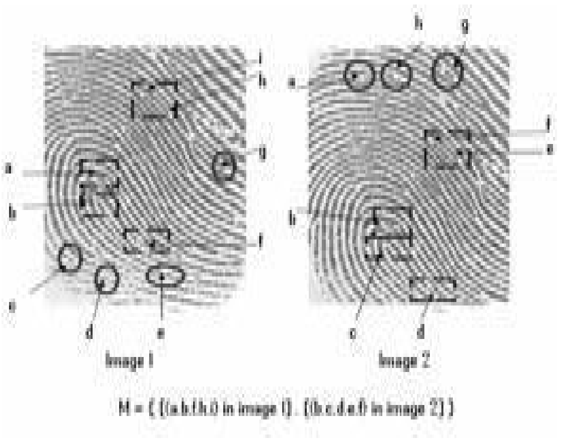
IV. ALGORITHM DESCRIPTION

4.1 Voronoi Diagram Algorithm

A Voronoi diagram decomposes a space into disjoint polygons (cells) based on the set of generators (i.e., data points). Given a set of generators S in the Euclidean space, Voronoi diagram associates all locations in the plane to their closest generator. Each generator s has a Voronoi cell consisting of all points closer to s than other generators.

4.2 Fingerprint Matching Algorithm

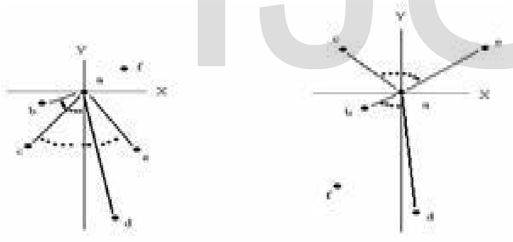
A fingerprint matching algorithm that initially identifies the candidate common unique (minutiae)points in both the base and the input images using ratios of relative distances as the comparing function**.**



Fingerprint Matching Algorithm

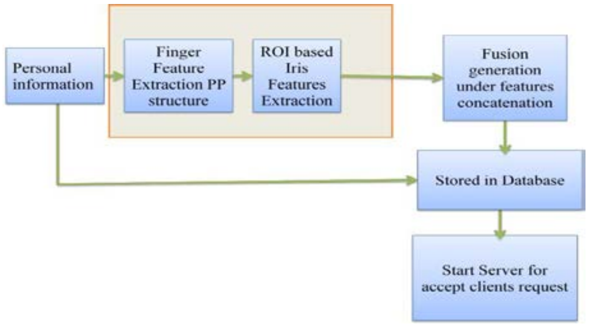
4.3 Five Nearest Neighbors Algorithm

Five nearest neighbors algorithm. In pattern recognition, the Five Nearest Neighbors algorithm (or k-NN for short) is a non-parametric method used for classification and regression. In both cases, the input consists of the k closest training examples in the feature space.

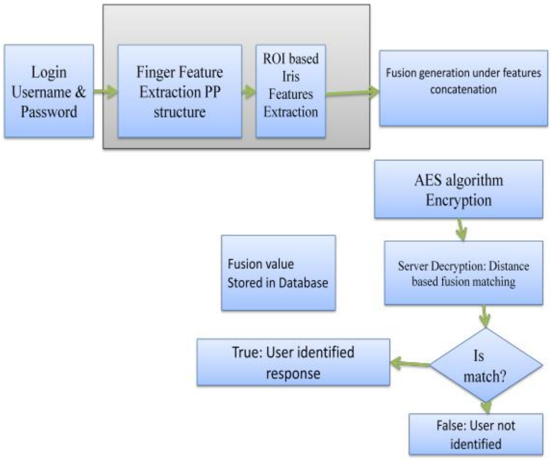


Five Nearest Neighbors Algorithm

V. SYSTEM ARCHITECTURE


Personal information
Finger Feature Extraction PP structure
ROI based Iris Features Extraction
Fusion generation under features concatenation
Stored in Database
Start Server for accept clients request

Sever side-User Registration


Login Username & Password
Finger Feature Extraction PP structure
ROI based Iris Features Extraction
Fusion generation under features concatenation
AES algorithm Encryption
Fusion value Stored in Database
Server Decryption: Distance based fusion matching
True: User identified response
Is match?
False: User not identified

Client side – User Verification

5.1 Server Based User Account Registration

Create new account at server side with required fields in the tables and the raw biometric data is captured. Depending on the proposed system, the data captured could be a finger image, face image and iris image with respect to unique account number. Required proof details are registered with personal details of the applicant. Account number and PIN number will be issued to the applicant and able to deposit amount to particular account.

5.2 Multi Biometric Template Extraction

This sub module describes the process of extracting the minutiae points from the fingerprint image. By use Color models such as RGB with certain range of color pixels, skin region is detected. After getting the skin region, facial features viz. Eyes and Mouth are extracted. The image obtained after applying skin color statistics is subjected to binarization. Iris recognition system captures an image of an individual’s eye, the iris in the image is then meant for segmentation and normalized for iris template extraction process.

5.3 Template Level Fusion Generation

The next step is to fuse the three sets of features at the feature level to obtain a multimodal biometric template that can perform biometric authentication. A decision template-level fusion algorithm resulting in a unified biometric descriptor and integrating fingerprint, iris and face features is presented.

5.4 Client Based Authentication And Crypto Fusion Matching Request

As per procedure client need to clears the login access for to access account thus send the fusion value which generated from multi biometric images given at client side. Send the fusion value as key with encrypted identity data to the server.

5.5 Server Based Fusion Matching And User Verification

After getting packet from the client, server extracts the data with proper decryption and gets the respective user fusion value from the database then proceeds the decision level fusion matching. Server system provides a matching score indicating the proximity of the feature vector with the template vector. These scores can be combined to assert the veracity of the claimed identity. If match success client forward to net banking access else authentication failed.

VI. CONCLUSION

A recent progress in biometrics is biometric cryptosystems which is nothing but the combination of both cryptography and biometrics that benefits from the strengths of both fields. Therefore, researchers, for a long time period, have been investigating ways to use biometric features of the user rather than memorable password or pass phrase, in an attempt to produce tough and repeatable cryptographic keys. To increase the strength of the fuzzy vault scheme in terms of template protection construct a fusion value based multi biometric cryptosystem. Our research work with security analysis will provides stronger security and better authentication accuracy compared with a cryptosystem based on single biometric.

REFERENCES

[1]. Ahmad T, Hu J, and Wang S, (2011), “Pair-polar coordinate-based cancelable fingerprint templates,” Pattern Recognit., vol. 44, nos. 10–11, pp. 2555–2564.

[2]. Chen X, Tian J, Yang X, and Zhang Y, (2006), “An algorithm for distorted fingerprint matching based on local triangle feature set,” IEEE Trans. Inf. Forensics Security, vol. 1, no. 2, pp. 169–177.

[3]. Chen C, Veldhuis R N J, Kevenaar T A M, and Akkermans A H M, (2007),“Multi-bits biometric string generation based on the likelihood atio,” in Proc. IEEE Int. Conf. Biometrics, Theory, Appl., System, pp. 1–6.

[4]. Dodis Y , Reyzin L, and Smith A, (2004), “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” in Proc. Int. Conf.Theory Appl. Cryptogr. Techn., pp. 523–540.

[5]. Jiang X and Yau W Y, (2000), “Fingerprint minutiae matching based on the local and global structures,” in Proc. 15th ICPR, pp. 1038–1041.

[6]. Juels A and Sudan M, (2006) “A fuzzy vault scheme,” Designs, Codes Cryptogr., vol. 38, no. 2, pp. 237–257.

[7]. Juels A and Wattenberg M, (1999), “A fuzzy commitment scheme,” in Proc. 6th ACM CCS, pp. 28–36.

[8]. Lee C, Choi J Y, Toh K A , Lee S, and Kim J, (2007), “Alignment-free cancelable fingerprint templates based on local minutiae information,” IEEE Trans. Syst.,

Man, Cybern. B, Cybern., vol. 37, no. 4, pp. 980–992.

[9]. Ratha N K, Chikkerur S, Connell J H, and Bolle R M, (2007), “Generating cancelable fingerprint templates,” IEEE Trans. Pattern Anal. Mach.Intell., vol. 29, no. 4, pp. 561–572.

[10].Ratha N K, Pandit V D , Bolle R M, and Vaish V, (2000), “Robust fingerprint authentication using local structural similarity,” in Proc. 5th IEEEWACV, pp. 29–34.

[11].Uludag U, Pankanti S, Prabhakar S, and Jain A K, (2004), “Biometric cryptosystems: Issues and challenges,” Proc. IEEE, vol. 92, no. 6, pp. 948– 960.

[12].Wang S and Hu J, (2012), “Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (DITOM) approach,” PatternRecognit., vol. 45, no. 12, pp. 4129–4137.

[13].Xi K and Hu J, (2009), “Dual layer structure check (DLSC) fingerprint verification scheme designed for biometric mobile template protection,” in Proc. 4th ICIEA, pp. 630–635.

[14]. Zhang W and Wang Y, (2002), “Core-based structure matchingalgorithm of fingerprint verification,” in Proc. 16th ICPR, pp. 70–74.

[15]. Zhong W B, Ning X B, and Wei C J, (2008), “A fingerprint matching algorithm based on relative topological relationship among minutiae,” in Proc. ICNNSP,pp. 225–228.