Online Security and Optimization Powered by Fingerprint in Online Voting System

Saji M G[1] , Renju Kalarikkal[2]
[1]Lecturer in Computer Engineering, Central Polytechnic College, Thiruvananthapuram, Kerala
[2]Lecturer in Computer Engineering, Central Polytechnic College, Thiruvananthapuram, Kerala

Abstract
Election is a process in which voters choose their representatives and express their preferences for the way that they will be governed. Using the decade old voting system to collect votes is no longer considered efficient due to the various recurring errors. The advancement of information and telecommunications technologies allow for a fully automated online computerized election process. An electronic voting system defines rules for valid voting and gives an efficient method of counting votes, which are aggregated to yield a result. Moreover, electronic voting systems can improve voter identification process by utilizing biometric recognition which provides more security. Biometrics is becoming an essential component of personal identification solutions, since biometric identifiers cannot be shared or misplaced, and they represent any individual's identity. Fingerprint matching is a significant part of this process. The value of democracy is voting. The importance of voting is trust that each vote is recorded and tallied with an accuracy and impartiality.

Key Words: Anti-spoofing measures, Feature extraction, online voting system, Image acquisition.

I.INTRODUCTION

In an increasingly digital world, reliable personal authentication has become an important human computer interface activity. National security, e-commerce, and access to computer networks are some examples where establishing a person's identity is vital. Existing security measures rely on knowledge-based approaches like passwords or token-based approaches such as swipe cards and passports to control access to physical and virtual spaces. Elections allow the people to choose their representatives and express their choices for how they will be governed. Generally, the integrity of the election process is fundamental to the democracy with integrity itself.
.

II. TYPES OF VOTING

SYSTEM OF PAPER VOTING

A paper-based voting system is a traditional method of conducting elections where eligible voters cast their votes on paper ballots. The paper ballots are usually preprinted with the names of the candidates or issues being voted on, and voters mark their preferences by making a physical mark, such as a tick or a cross, next to their chosen
candidate or option. After the voting period ends, the paper ballots are collected and counted manually by election officials. This process can be time-consuming, and errors can occur, leading to delays and disputes over the accuracy of the results. However, some paper-based voting systems also use electronic counting machines to speed up the process and minimize errors. convenient for voters who may have to travel to a polling station to cast their vote.

ELECTRONIC VOTING SYSTEM

An electronic voting system is a method of conducting elections that uses electronic equipment and technology to record, tabulate and report votes. The electronic voting system can be classified into two main categories: Direct Recording Electronic (DRE) voting machines and Optical Scan voting systems. DRE voting machines are electronic devices that allow voters to make their choices by touching a screen or pressing buttons. Once the voter has made their choices, the machine records the vote and stores it electronically. At the end of the voting period, the results are tabulated automatically and reported to election officials. DRE voting machines can also be

equipped with additional security features, such as paper trails, to ensure the accuracy and transparency of the process.

Optical Scan voting systems, on the other hand, use paper ballots that are marked by voters using pens or pencils. The ballots are then scanned by an optical scanner that reads and records the votes electronically. The results are tabulated automatically and reported to election officials.

ONLINE VOTING SYSTEM

An online voting system is a method of conducting elections that allows eligible voters to cast their votes remotely over the internet, using a computer, smartphone, or other digital device. Online voting systems can offer several advantages over traditional paper-based voting systems, including increased accessibility, convenience, and speed.

In an online voting system, eligible voters are first required to register with the online voting platform, typically by providing their personal information and proof of identity. Once registered, voters can log in to the online voting platform using their credentials and cast their vote using a secure and user-friendly interface. Online voting systems can use various types of authentication methods to verify the identity of voters, such as usernames and passwords, security tokens, or biometric data such as fingerprints or facial recognition.

III. ONLINE VOTING THROUGH FINGERPRINT

An online voting system that uses fingerprint authentication is a type of electronic voting system that allows eligible voters to cast their votes remotely over the internet, using their fingerprints to authenticate their identity. This system uses biometric technology to verify the identity of voters and ensure the integrity of the voting process. In this system, voters would first need to register with the online voting platform by providing their personal information, including their name, address, and a scanned copy of their fingerprint. The voter's identity would then be authenticated each time they log in to the voting platform to cast their vote by scanning their fingerprint using a fingerprint scanner attached to their device. The use of fingerprint authentication in online voting systems offers several advantages. First, it is a highly secure and reliable method of authentication, as each person's fingerprints are unique and difficult to forge. This helps to prevent voter fraud and ensure that only eligible voters can cast their votes.

Second, the use of fingerprint authentication can make the online voting process more convenient and accessible, particularly for people who may have difficulty remembering complex passwords or using other forms of authentication. Additionally, fingerprint authentication can be used to provide an added layer of security to other aspects of the online voting process, such as the transmission and storage of voting data. However, there are also some concerns about the use of fingerprint authentication in online voting systems. One concern is that the use of biometric data raises privacy concerns, as fingerprints are personal and sensitive information. Additionally, there is a risk that fingerprint data could be hacked or stolen, which could compromise the security of the online voting system. Overall, the use of fingerprint authentication in online voting systems has the potential to enhance the security, convenience, and accessibility of the voting process, but careful consideration must be given to ensure that the system is secure, reliable, and respects the privacy of voters.

IV. FINGERPRINT AUTHENTICATION IN ONLINE VOTING

Levels of Fingerprint Authentication:

Level 1: feature comprises these global patterns and morphological information. They alone do not contain sufficient information to uniquely identify fingerprints but are used for broad classification of fingerprints.

At level 1, a fingerprint authentication system typically involves basic image acquisition, preprocessing, and matching steps. Here are the main components and functionalities of a level 1 fingerprint authentication system:

1. Image acquisition: The system captures a high-quality image of the user's fingerprint using a sensor or scanner. The image should have sufficient resolution and contrast to capture the unique ridge patterns and minutiae features of the fingerprint.

2. Preprocessing: The system applies basic preprocessing steps to enhance the quality and clarity of the fingerprint image. This may include noise reduction, image normalization, contrast enhancement, and feature extraction.

3. Feature extraction: The system extracts the distinctive features of the fingerprint, such as the ridge patterns and minutiae points, using simple algorithms such as thresholding and filtering. The features are represented in a standardized format that can be compared with a reference database.

4. Matching: The system compares the extracted features of the user's fingerprint with the stored reference database to determine whether there is a match or not. The matching algorithm may be based on simple distance metrics, such as Euclidean or Hamming distance, or more advanced techniques such as correlation-based matching or support vector machines.

5. Decision-making: The system decides based on the matching score or confidence level of the comparison. If the matching score exceeds a certain threshold or falls within a certain range, the system grants access to the user. Otherwise, the system denies access and may trigger an alarm or notification. A level 1 fingerprint authentication system is relatively simple and may be suitable for low security applications such as unlocking a personal device or accessing a personal account.

However, it may not be sufficiently reliable or robust for high-security applications that require more advanced features such as liveness detection, multi-factor authentication, or encryption.

Level 2, a fingerprint authentication system would typically involve additional security measures and advanced features to enhance the accuracy, robustness, and reliability of the system. Here are some of the key features that may be included in a level 2 fingerprint authentication system:

1. Multimodal biometric authentication: A level 2 fingerprint authentication system may use multiple biometric modalities, such as face recognition or iris recognition, to improve the accuracy and security of the authentication process. The system may require the user to provide multiple biometric samples, such as a fingerprint and a face image, and verify their identity based on the combined information from the different modalities.

2. Liveness detection: To prevent spoofing attacks using fake or artificial fingerprints, a level 2 fingerprint authentication system may include liveness detection features that can detect the presence of a live finger and distinguish it from a fake or static finger. Liveness detection can be achieved using various techniques, such as detecting the blood flow or the thermal characteristics of the finger.

3. Anti-spoofing measures: In addition to liveness detection, a level 2 fingerprint authentication system may incorporate other anti-spoofing measures, such as detecting unusual patterns or artifacts in the fingerprint image, or using machine learning models to identify and reject fake or manipulated fingerprints.

4. Template protection: To prevent the theft or misuse of the stored fingerprint templates, a level 2 fingerprint authentication system may use template protection mechanisms, such as encryption or obfuscation, to secure the templates and prevent unauthorized access or tampering.

5. Secure communication and storage: A level 2 fingerprint authentication system may ensure the secure communication and storage of the biometric data and authentication results, using encryption, secure protocols, and access controls. The system may also implement audit and logging mechanisms to track and monitor the usage and access to the sensitive data.

Level 3 fingerprint authentication system is a highly secure system that provides advanced features for protecting the privacy and integrity of the fingerprint data, as well as for ensuring the reliability and accuracy of the authentication process. Here are some of the key features and components of a level 3 fingerprint authentication system:

1. Biometric data protection: A level 3 system employs strong encryption and hashing techniques to protect the biometric data, such as the fingerprint templates and images, from unauthorized access or tampering. The system should also have robust access controls and audit trails to monitor and track the usage of the biometric data.

2. Anti-spoofing measures: A level 3 system should incorporate advanced anti-spoofing measures, such as liveness detection and multi-factor authentication, to prevent the use of fake or artificial fingerprints for authentication. The system should also be able to detect and alert the user or the administrator of any suspicious activities or attacks.

3. Quality assessment: A level 3 system should perform thorough quality assessment and error detection on the captured fingerprint images and features, to ensure that the data is of sufficient quality and consistency for reliable authentication. The system should also provide feedback and guidance to the users for improving the quality of their fingerprints.

4. Performance optimization: A level 3 system should employ advanced algorithms and techniques for optimizing the performance and efficiency of the authentication process, such as parallel processing, feature fusion, and adaptive thresholding. The system should also be able to handle a large volume of users and transactions, and should have a scalable and robust architecture.

5. Compliance and certification: A level 3 system should adhere to the relevant industry standards and regulations for biometric authentication, such as ISO/IEC 19794-2 and FIDO, and should undergo rigorous testing and certification by independent third-party organizations, such as NIST or IAFIS. Overall, a level 3 fingerprint authentication system provides a high level of security and reliability for applications that require strong authentication and protection of sensitive data, such as banking, healthcare, and government systems.

Fingerprint recognition system

I. Image Acquisition

In fingerprint recognition, image acquisition is the process of capturing an image of a person's fingerprint. The image is then used as the input for fingerprint recognition algorithms that analyze the unique patterns and ridges on the fingerprint to determine its identity.

There are several different methods for acquiring fingerprint images, including:

1. Optical scanners: These scanners use light to capture an image of the fingerprint. The fingerprint is placed on a glass surface, and a light source illuminates the finger from below. The reflection of the light creates a high-contrast image of the fingerprint, which is then captured by a camera.

2. Capacitive scanners: These scanners use a small electrical current to capture an image of the fingerprint. The fingerprint is placed on a sensor surface that is charged with a small electrical current. The ridges on the fingerprint cause changes in the electrical field, which are then used to create an image of the fingerprint.

3. Ultrasonic scanners: These scanners use sound waves to capture an image of the fingerprint. The fingerprint is placed on a sensor surface that emits high-frequency sound waves. The sound waves bounce off the ridges and valleys of the fingerprint and are then used to create an image of the fingerprint.

Regardless of the method used, it is important to ensure that the fingerprint image is of high quality and free from distortion or artifacts that could affect the accuracy of the fingerprint recognition algorithm. This is typically achieved through proper positioning and pressure of the finger on the scanner, as well as through software algorithms that can correct for any distortions or artifacts in the image.

II. Edge Detection

Edge detection is an essential step in fingerprint recognition, as it helps to extract the unique ridge patterns and ridge endings present in a fingerprint image. The process of edge detection aims to identify the boundaries between different regions in the image where there are significant changes in intensity or texture. These boundaries correspond to the ridges and valleys in a fingerprint.

There are several algorithms and techniques commonly used for edge detection in fingerprint recognition. Here are a few examples:

1. Canny edge detection: The Canny edge detection algorithm is widely used in various image processing applications, including fingerprint recognition. It involves several steps, including noise reduction, gradient calculation, non-maximum suppression, and thresholding. The result is a binary image highlighting the edges in the fingerprint.

2. Sobel operator: The Sobel operator is a popular method for edge detection. It involves convolving the

fingerprint image with a small filter to calculate the gradient at each pixel. The gradient represents the rate of change of intensity in the image, and regions with high gradients typically correspond to edges.

3. Laplacian of Gaussian (LoG): The LoG operator combines the smoothing effect of a Gaussian filter with the edge-detection capability of the Laplacian operator. It detects edges by identifying zero-crossings in the second derivative of the image after applying Gaussian smoothing.

Once the edges are detected, further processing steps are typically performed to refine the extracted ridge information and eliminate false edges or artifacts. These steps may include thinning the ridge lines, removing spurious branches, and connecting broken ridges to form a continuous representation of the fingerprint.

Edge detection plays a crucial role in fingerprint recognition systems, as it helps to extract the distinctive features necessary for matching and identification purposes. The resulting edge map can be used as input for subsequent steps in the fingerprint recognition pipeline, such as feature extraction and matching against a reference database of fingerprints.

III. Thinning

Thinning is a process in fingerprint recognition that aims to reduce the width of the extracted ridge lines in a fingerprint image while preserving their connectivity. The purposeof thinning is to obtain a more accurate and compact representation of the fingerprint pattern, which can facilitate comparison and matching against reference templates in a fingerprint recognition system.

IV. Feature Extraction

Feature extraction is a crucial step in fingerprint recognition that involves identifying and extracting the unique characteristics or features of a fingerprint that can be used for matching and identification purposes. The goal of feature extraction is to reduce the dimensionality of the fingerprint data while preserving its discriminatory information, so that it can be efficiently compared against a reference database of fingerprints.

V. Classifier

A classifier in fingerprint recognition is a model or algorithm that is used to compare and match the extracted features of a test fingerprint against a reference database of fingerprints. The goal of the classifier is to determine the degree of similarity or dissimilarity between the test fingerprint and the stored fingerprints and to identify the closest match or matches in the database.

Selecting Algorithm

There are several matching algorithm such as minute extraction, global search and correlation based etc. Matching algorithm applied to the original image fingerprint.

I. SIFT algorithm

1 Scale-space extreme detection: searches over all scales and image locations by making use of difference-of-Gaussian function to identify strongly interest points that are invariant to scale and orientation.

2 Keypoint localization: At each candidate location a detailed model is fit to determine location and scale. Keypoints selected on measures of their stability.

3 Orientation assignments: there is One or more orientations are assigned to each keypoint location based on local image gradient directions.

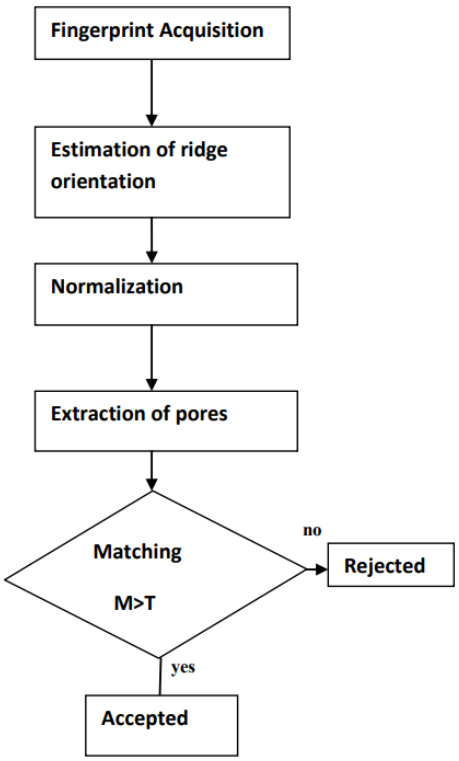
4 Key point descriptor: The local image gradients are measured at the selected scale in the region around each keypoint.

4. Enrollment and Verification process

V. PROPOSED SYSTEM

This chapter converse the proposed approach and pores matching using SIFT algorithm. The basics of SIFT technique is described in the previous chapter.

Block diagram



Fingerprint Acquisition

The first step in the proposed approach is to acquire fingerprint image of good quality. Thus, Hamster II is use for acquiring fingerprint image. Hamster II is optical fingerprint scanner and use for scanning the finger. Hamster II is used for creating fingerprint database. This database is use for analysing the accuracy of proposed algorithm and execute the results on the basis of analyse.

Estimation of ridge orientation

The local ridge orientation is determined by the least square estimate method. This data is utilized later in the representation of pores. It can be stated that segmentation is the critical stage of fingerprint pores recognition, since areas that are wrongly identified as pores regions will corrupt biometric templates resulting in very poor recognition.

Normalization

To compensate for the variations in lighting, contrast, and other inconsistencies, normalization process is used. Gaussian blurring is used to remove any noise introduced by the sensor. The lighting inconsistencies are adjusted by using sliding-window contrast adjustment on the Gaussian blurred image. To further enhance the ridges and valley a final intensity correction is made by using Histogram-based Intensity Level Adjustment.

The image can divide into small processing blocks (32 by 32 pixels) and perform the Fourier transform according to:

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) \times exp\left\{-j2\pi \times \left(\frac{ux}{M} - \frac{vy}{N}\right)\right\}$$

.....(4.1)

For u = 0, 1, 2... 31 and v = 0, 1, 2... 31.

Get the enhanced block according to

$$g(x,y) = F^{-1}\{F(u,v) \times |F(u,v)|^{k}\} \quad \text{..... (4.2)}$$

Where $F^{-1}(F(u, v))$ is done by:

$$F(x,y) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) \times exp\left\{-j2\pi \times \left(\frac{ux}{M} - \frac{vy}{N}\right)\right\}$$

..... (4.3)

For x = 0, 1, 2... 31 and y = 0, 1, 2... 31.

The k in formula (ii) is an experimentally determined constant, which can choose k=0.45 to calculate. While having a higher "k" improves the appearance of the ridges, filling up small holes in ridges, having too high a "k" can result in false joining of ridges. Thus, a termination might become a bifurcation.

Extracted pores

Extract level 3 features in ROI. The pores are distributed over ridges and using orientation detail can provide additional information for matching. During tracing, the algorithm classifies the contour information into pores and ridges.

VI CONCLUSION AND FUTURE WORK

Online voting system through finger print will give secure more powerful structure to polling by applying Fingerprint level 3 features extraction and matching approach which is a novel approach, its characteristics, design issues and applications. Using SIFT algorithm in online fingerprint matching with level3 fingerprint increases result of this analysing process, we can conclude that, as the threshold value is increases, false rejection rate is also Increases. These comparison

graph will so a much better result for this proposed approach False rejection ratio FRR =Number of genuine fingerprints rejected divided by Total number of genuine tests. Also increasing threshold energy false acceptance ratios (FAR) will decrease which will show on result while implementing.

Genuine acceptance rate will improve. It also describes an overview of level 1 and level 2 features, in the literature and their functionalities Future work will also characterize the performance of level-3 features on a comprehensive large-scale database which contains fingerprint images of varying size, quality and other environmental factors. Since the level 3 features are unique so it may give more security with minimal error to defence corporate & other major organizations.

REFERENCES

[1] D. Ashok Kumar#1, T. Ummal Sariba Begum#2 "A novel Approach Design Of Electronic Voting System Using Fingerprint‖

[2] M. Ray, P. Meenen, and R. Adhami, ―A novel approach to fingerprint pore, extraction. ‖ Southeastern Symposium on System Theory, page no. 282–286, 2005.

[3] McGraw, Gary and Greg Morrisett., ―Attacking Malicious Code: A Report to the Infosec Research Council. ‖ IEEE Software. September/October 2000.

[4]The Implementation of Electronic Voting in the UK research summary. 2002. ―http://www.dca.gov.uk/elections/e-voting/pdf/esummary.pdf. ‖ 21.01.2007.

[5] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, and A.K. Jain. FVC2000: Fingerprint Verification Competition. IEEE Transactions on Pattern Analysis and Machine Intelligence, 24(3):402–412, 2002.

[6] Qijun Zhao, Lei Zhang, David Zhang, Nan Luo, ―Adaptive Pore Model for Fingerprint Pore Extraction. ‖ Proc. IEEE, 978-1-4244-2175-6/08, 2008.

[7]. Moheb R. Girgis, Tarek M. Mahmoud, and Tarek AbdEl-Hafeez, ―An Approach to Image Extraction and Accurate Skin Detection from Web Pages.‖ World academy of Science, Engineering and Technology, page no. 27, 2007.

[8] Manvjeet Kaur, Mukhwinder Singh, Akshay Girdhar, and Parvinder S. Sandhu, ―Fingerprint Verification System using Minutiae Extraction Technique. ‖ World academy of Science, Engineering and Technology, page no. 46, 2010.

[9] Hoi Le, The Duy Bui, ―Online fingerprint identification with a fast and distortion tolerant hashing. ‖ Journal of Information Assurance and Security 4 page no. 117-123, 2009.

[10] Anil Jain, Yi Chen, and Meltem Demirkus, ―Pores and Ridges: Fingerprint Matching Using Level 3 Features. ‖ Pattern recognition letters, page no. 2221-2224, 2007.