International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

BIOMETRIC HASHING TEMPLATE PROTECTION

Author:

A .FAZIL
Department of Computer Applications
B. S. Abdur Rahman Crescent Institute of Science and Technology
Vandalur, Chennai-600048

Under the guidance of:

Dr. A. K. ASHFAUK AHAMED
Supervisor
Assistant Professor (Sr.Gr)
Department of Computer Applications
B. S. Abdur Rahman Crescent Institute of Science and Technology
Vandalur, Chennai-600048

Abstract

The main motivation of the project defines about the secure authentication of the modules that is multi core authentication of both the face and iris. The goal is to build a system that can handle more process concurrently, improving system performance in general. The system maintains HAAR cascades and Back Propagation Neural Network.The security can be added with Elliptical Curve Cryptography algorithm generation

Introduction

Biometric templates, digital representations of biometric features extracted from various modalities such as face and iris images, play a crucial role in biometric authentication systems. However, the storage and transmission of biometric templates pose significant security risks, as they can be vulnerable to unauthorized access or misuse. To mitigate these risks, researchers have proposed various techniques for biometric template protection, among which cancelable biometrics has gained considerable attention.Cancelable biometrics involves intentionally altering biometric features in a reversible manner to protect sensitive biometric data while maintaining its usability for authentication purposes. In this paper, we present a novel approach to biometric template protection using a combination of face and iris modalities, enhanced with cryptographic security based on Elliptic Curve Cryptography (ECC). By encrypting the extracted biometric features and incorporating chaos-based hashing techniques, our proposed system ensures the confidentiality and integrity of biometric templates, thereby safeguarding them from unauthorized access or tampering.

The key objective of our research is to design an enrollment scheme that not only strengthens the authentication process but also guarantees the safety of biometric data. By leveraging biometric cryptosystems, we aim to enhance the security of sensitive transactions, such as ATM access, by providing robust protection against cyber attacks and identity theft. Overall, our proposed system offers a promising solution to the evolving security

challenges in biometric authentication, paving the way for safer and more reliable authentication mechanisms in various domains, including finance, healthcare, and law enforcement.

Literature survey

A SECURE AND COMPACT MULTIMODAL BIOMETRIC AUTHENTICATION SCHEME USING DEEP HASHING

P. Sivakumar; B. Ruthu Rathnam; S. Divakar; M. Anil Teja; R. Rajendra Prasad

IEEE - 2021

Unimodal biometrics-based authentication systems are trending and applied to various real-time applications since biometrics is difficult to forge than traditional password-based access systems. These systems are also having the challenges like protecting biometrics from identity theft and database compromise. Multimodal biometric systems have several advantages, including lower error rates, higher accuracy, and larger population coverage. However, multimodal systems have an increased demand for integrity and privacy because they must store multiple biometric traits associated with each user. Even though multimodal biometric system provides reasonable advantages, but still, there is a significant requirement for secure multimodal biometric template protection schemes to protect the multimodal biometric templates. In this paper, a deep hashing framework for feature-level fusion that generates an advanced secure multimodal template from each user's finger and finger-vein biometrics is proposed. The matching performance will get improved due to the fusion of multiple biometrics. Furthermore, the proposed approach also provides cancelability and unlinkability of the templates along with improved privacy of the biometric data to protect from the different attacks. It is for integrating multimodal fusion, deep hashing, and biometric security, with an emphasis on structural data from modalities like fingerprint and finger-vein. VGG-19 is used for feature extraction and experiments were conducted using standard datasets of fingerprint and finger vein images. This system achieved an accuracy of 95%.

Techniques used: VGG -19

Advantages: Multimodel Biometric Hashing Mechanism with hashing mechanism

Disadvantages: The cancelable data maintenance is done in this paper

[2] EFFICIENT KNOWN-SAMPLE ATTACK FOR DISTANCE-PRESERVING HASHING BIOMETRIC TEMPLATE PROTECTION SCHEMES

Yenlung Lai; Zhe Jin; KokSheik Wong; Massimo Tistarelli

IEEE - 2021

The rapid deployment of biometric authentication systems raises concern over user privacy and security. A biometric template protection scheme emerges as a solution to protect individual biometric templates stored in a database. Among all available protection schemes, a template protection scheme that relies on distance-preserving hashing has received much attention due to its simplicity and efficiency in offering privacy protection while archiving decent authentication performance. In this work, we introduce an efficient attack called known sample attack and demonstrate that most state-of-art template protection schemes that utilize distance-preserving hashing can be compromised in practice (within few seconds), especially when the output is significantly smaller than the original input sample size. These findings further motivated our subsequent work in proposing a secure authentication mechanism to resist such an attack with proper study over the distribution of the input samples. Furthermore, we conducted revocability, unlinkability analysis to demonstrate the satisfactory of general biometric template protection

requirements; and showed the resistance of various security and privacy attacks, i.e., false acceptance attack, and attack via record multiplicity.

Techniques used: Distance Preserving Hashing system

Advantages: The distance variability analysis can be preceded in this hashing system

Disadvantages: The system can be verified with a normal authentication level

[3] SECURE DATA RETRIEVAL SYSTEM USING BIOMETRIC IDENTIFICATION
J Anand Babu; H P Neha; Kushala S Babu; Rishal Nishma Pinto

IEEE - 2022

With the continuous dependence of using electronic media has drastically impacted our communications, with most of them currently taking place digitally. Users frequently have to logon to distant workstations, yet the adversarial Internet world can put users & service providers on risk. Biometric identification have grown in popularity in current times. With the rapid evolution of decentralized computation, data base owners are attempting to disperse the massive amount of biometric data as well as ID allocation to the cloud server in order to eliminate the high expenses of storage and computation. Biometric authentication technologies are becoming more popular as a method of verifying individual's identity. Because of the many benefits that biometric credentials offer over traditional authenticating approaches, biometrics has become widely prominent as a way of verifying persons (e.g., password-based authentication). The inherent significant relation among the user with his/her biometric information is the main distinguishing aspect of such an authentication system. Yet, if the biometric feature is exploited, this very same favorable aspect creates major personal & safety problems. The major complex problems that must be considered while creating secure & privacy-preserving biometric authentication systems (PP-BAS) are discussed in this paper. Further we specifically outline the major challenges to secure & PP-BAS and provide recommendations for potential solutions in attempt to create S-PP BAS in cloud computing.

Techniques used: Password based authentication

Advantages: Normal authentication system is done in the maintenance of password system

Disadvantages: The normal password mechanism is not enough

[4] CANCELABLE MULTI-BIOMETRIC APPROACH USING FUZZY EXTRACTOR AND NOVEL BIT-WISE ENCRYPTION

Donghoon Chang; Surabhi Garg; Munawar Hasan; Sweta Mishra

IEEE - 2020

The widespread deployment of multi-biometrics to authenticate users prompts the need for biometric systems with high recognition performance. Further, the biometric data, once leaked or stolen, remains compromised forever. Hence biometric security is of utmost importance. Existing biometric template protection schemes either degrade the recognition performance or they have issues with security and speed. We propose a cancelable multi-biometric authentication approach where a novel bit-wise encryption scheme transforms a biometric template to a protected template using a secret key generated from another biometric template. It fully preserves the number of bit-errors in the original and the protected template to ensure recognition performance equivalent to the performance of the unprotected systems. We introduce Algorithm I and Algorithm II for bit-wise encryption; both are defined over cryptographic-primitives- block cipher based encryption and keyed-hash function. We profile these algorithms on various hardware architectures to calculate the efficiency in terms of the time taken during enrolment and

authentication phase. For Algorithm II, we observe that a 3.3 GHz desktop architecture takes about 18 milliseconds on an average of over 200 runs to authenticate a user. Additionally, we provide mathematical proof to show that the proposed scheme guarantees secrecy and irreversibility. The results of comparisons with the existing biometric template protection schemes on the various face and iris databases show that the proposed work provides significantly good recognition performance and efficiency, while it achieves high security. Finally, the bit-wise encryption scheme can be built over the commercial-off-the-shelf systems to achieve security with equivalent high performance.

Techniques used: Fuzzy Extraction and bit wise encryption

Advantages: The hash function based identification can be done with the system

Disadvantages: Still more accuracy can be enhanced in this implementation

Existing system

The existing system of normal authentication typically revolves around the use of passwords as the primary method for verifying user identities. Here's an overview of how it works:

Username and Password:

Users are required to create an account with a system, service, or application by providing a username and a password. The username serves as a unique identifier, while the password serves as a secret credential known only to the user.

Authentication Process:

When users attempt to access the system or log in to their account, they enter their username and password through a login interface.

The system compares the provided username and password against the stored credentials in its database.

If the username and password match the records in the database, the user is granted access to the system, and they can proceed to use the services or access the resources.

Storage of Passwords:

Passwords are typically stored in the system's database in hashed or encrypted form to protect them from unauthorized access in case of a data breach.

During the authentication process, the system hashes or encrypts the entered password and compares it with the stored hashed or encrypted password.

Security Measures:

To enhance security, systems may enforce password complexity requirements (e.g., minimum length, inclusion of uppercase letters, numbers, and special characters).

Users may be prompted to change their passwords periodically to mitigate the risk of password compromise.

Account lockout policies may be implemented to prevent brute-force attacks, where multiple failed login attempts result in temporary account suspension.

Limitations and Challenges:

Password-based authentication is vulnerable to various security threats, including password guessing, phishing attacks, and credential stuffing.

Users often struggle to remember complex passwords, leading to password reuse or writing down passwords, which compromises security.

Password-based authentication may not provide sufficient security for highly sensitive systems or applications, especially in the face of sophisticated cyber threats.

Drawbacks of existing system

- ✓ Maintenance of the normal fingerprint access will be not more accurate
- ✓ Data access without encryption make a open problem in cloud data integrity
- ✓ Multiple level of authentication access require over patient data

Proposed system

A proposed system for face and iris biometric authentication could integrate the strengths of both modalities to enhance security and accuracy in identity verification. Here's an outline of the proposed system:

Data Acquisition:

Users' face and iris biometric data are captured using specialized biometric sensors or cameras. High-resolution images of the face and iris are obtained for analysis.

Feature Extraction:

Feature extraction algorithms are applied to the captured biometric images to extract unique features and patterns. For face biometrics, facial landmarks, textures, and contours are extracted. For iris biometrics, iris texture, patterns, and characteristics such as crypts and furrows are extracted.

Biometric Template Creation:

Biometric templates are generated based on the extracted features from the face and iris data. Templates are compact representations of the biometric features that can be securely stored and compared during authentication.

Template Matching and Verification:

During authentication, the user presents their face and iris for verification. The captured biometric data is processed to generate templates. Template matching algorithms compare the templates generated from the presented biometric data with the stored templates in the database. Matching scores are computed to determine the degree of similarity between the presented biometric data and the stored templates.

Decision Making:

A decision threshold is applied to the matching scores to determine whether the authentication attempt is accepted or rejected. If the matching score exceeds the threshold for both face and iris biometrics, the user is successfully authenticated. If the matching score falls below the threshold for either modality, the authentication attempt is rejected.

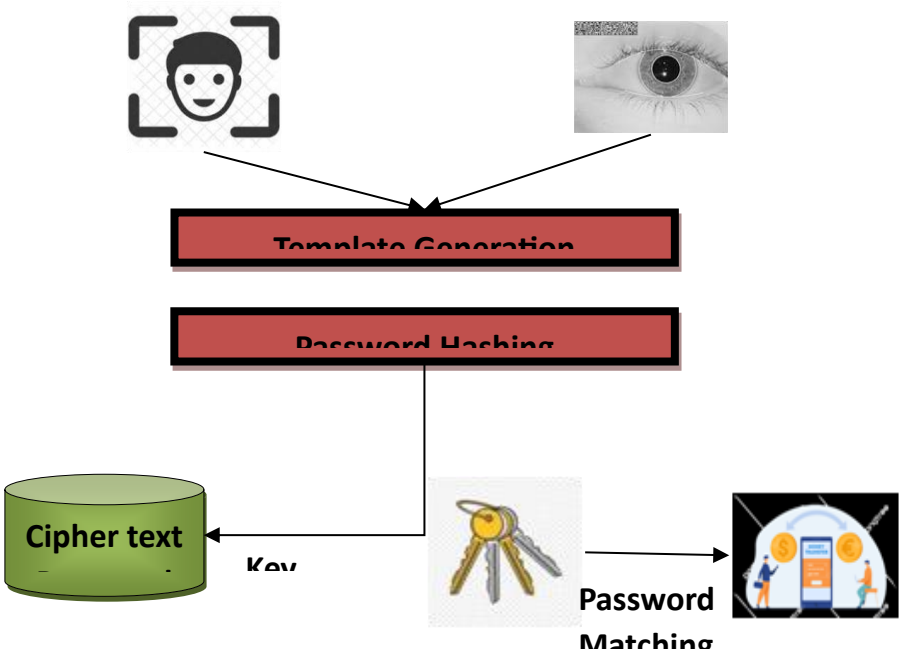
Robust encryption techniques are employed to secure biometric templates during storage and transmission. Privacy-preserving methods, such as biometric hashing, may be used to protect users' biometric data from unauthorized access or disclosure. Strict access controls and authentication mechanisms are implemented to prevent unauthorized access to the biometric authentication system.

By combining face and iris biometric authentication in a unified system, the proposed system offers enhanced security, accuracy, and reliability in identity verification, making it suitable for various applications requiring stringent authentication measures.

Advantage of proposed system

- ✓ The first feature of developing biometric cryptosystems was to a good approach
- ✓ They can also be utilized as a safeguard for templates.
- ✓ The two primary kinds of template protection techniques that have been proposed with transformed feature
- ✓ Using biometrics public information about the cryptosystem there is a biometric template saved.

Overall Architecture:



Methodology:

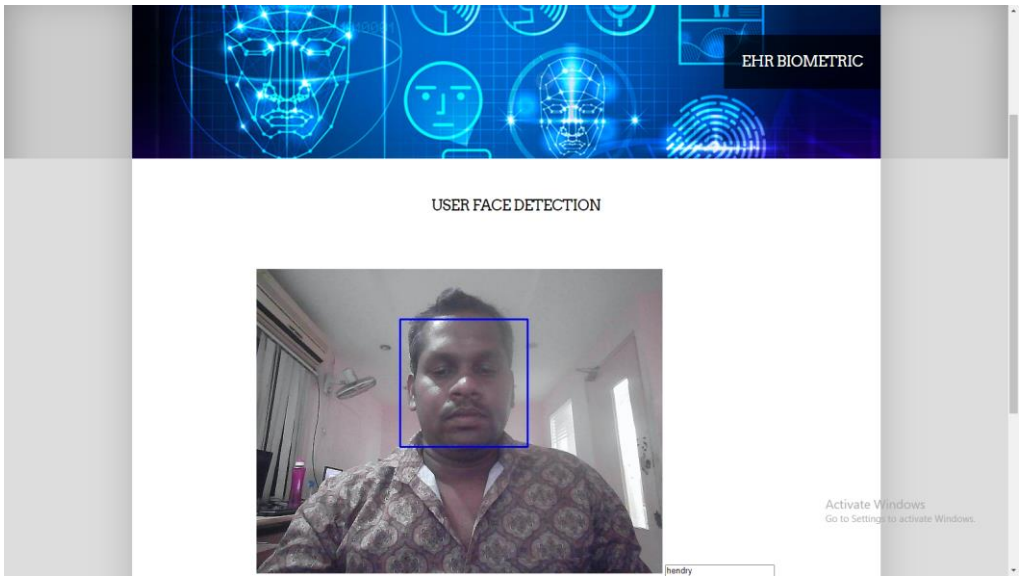
FACE DETECTION

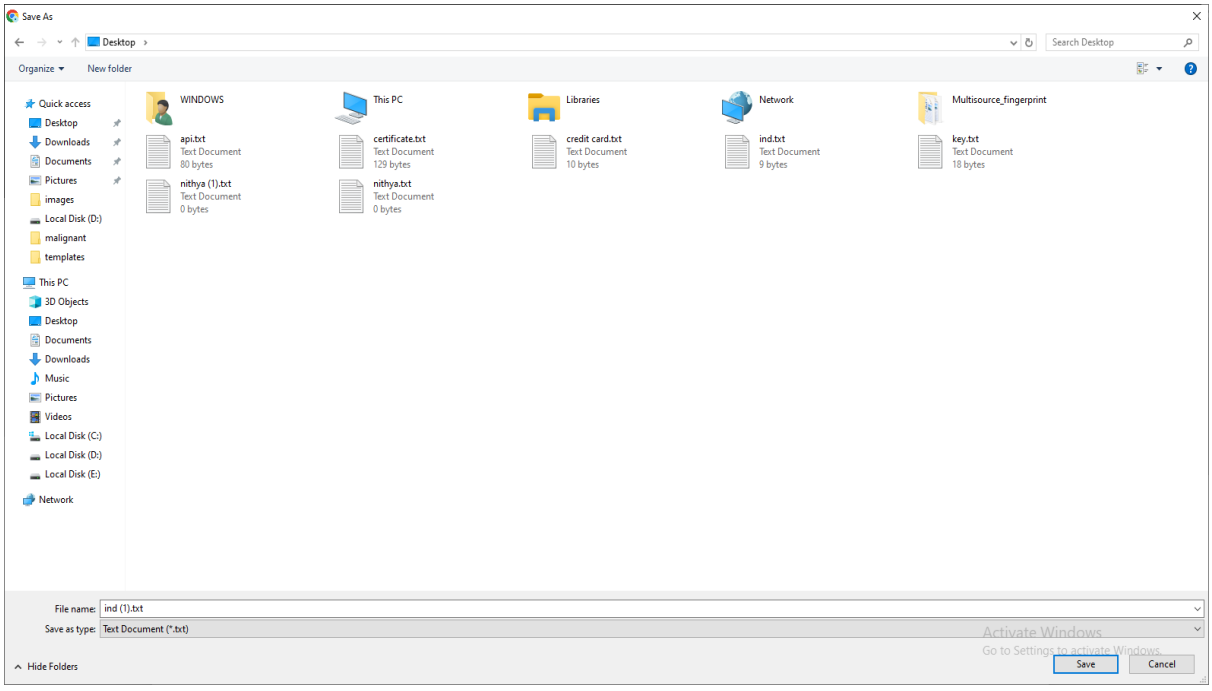
Facial detection via the Viola-Jones algorithm is a common method used due to its high detection rate and fast processing speed. The algorithm can be summed up in four steps: feature selection, feature evaluation, feature learning to create a classifier, and cascading classifiers. Simple features are used, inspired by Haar basis functions, which are essentially rectangular features in various configurations. A two-rectangle feature represents the difference between the sum of the pixels in two adjacent regions of identical shape and size. This idea can be extended to the three-rectangle and four-rectangle features. In order to quickly compute these rectangle features, an alternate representation of the input image is required, called an integral image.

The learning portion of the face detection algorithm uses Adaboost which basically uses a linear combination of weak classification functions to create a strong classifier. Each classification function is determined by the perceptron which produces the lowest error. However, this is characterized as a weak learner since the classification function does not classify the data well. In order to improve results, a strong classifier is created after multiple rounds of re-weighting a set weak classification functions. These weights of the weak classification functions are inversely proportional to their errors. The goal of this stage is to train the most relevant features of the face and to disregard redundant features. The last step of the Viola-Jones algorithm is a cascade of classifiers. The classifiers constructed in the previous step form a cascade. In this set up structure, the goal is to minimize the computation time and achieve high detection rate. Sub-windows of the input image will be determined a face or non-face with classifiers of increasing complexity. If a there is a positive result from the first classifier, it then gets evaluated by a second more complex classifier, and so on and so forth until the sub-window is rejected. By doing this, the structure utilizes the early stages of the cascade in order to reject as many negatives as possible

Here the face detection technique is enhanced using the extracted features of the human. Face detection is further classified as face detection in images and real-time face detection. In this project we will attempt to detect faces in video based detection system. To do this it would be useful to study the Haar cascades face detection. In this research, we implement Haar Cascade Classifier to detect human faces using an Open Source Computer Vision Library. For human face detection, haar features are the main part of haar cascade classifier.

Output screenshot:





Conclusion:

Here, the proposed system has discussed various types of attacks that can be launched against an iris recognition system. The issue can be rectified using biometric hashing template process of hashing both face and iris of the user for secure bank transformation. And also various types of iris template protection techniques that can be used for a secure iris recognition system. The proposed system has specifically highlighted techniques that can be used to protect the contents of an iris and face template and secure the system for personal authentication. The main motivation of the project defines about the secure authentication of the modules that is multi core authentication of both the face and fingerprint. The goal is to build a system that can handle more process concurrently, improving system performance in general.

References:

[1] A. K. Jain, A Ross, and S. Pankanti, "Biometrics: a tool for in-formation security," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125–143, 2020.

[2] C. Roberts, "Biometric attack vectors and defences," Computers and Security, vol. 26, no. 1, pp. 14–25, 2021.

[3] M1.4 Ad Hoc Group on Biometric in E-Authentication ,"Study report on biometrics in E-authentication," Tech.Rep. INCITS M1/07-0185rev, International Committee for In-formation Technology Standards (INCITS), Washington, DC,USA, August 2021.

[4] I.Buhan and P. Hartel, "The state of the art in abuse of biometrics," Tech. Rep. TR-CTIT-05-41, Centre for Telematics and Information Technology, University of Twente, Twente, The Netherlands, December 2023.

[5] A. K.Jain, A. Ross, and U Uludag,"Biometric template security: challenges and solutions," in Proceedings of the European Signal Processing Conference (EUSIPCO '05), Antalya, Turkey, September 2022.