Biometric Identification: Iris Recognition, Biometric Cryptography

Rawan Alrasheddi, Zainab Alawami, Maryam Hazazi, Reema Abu Alsaud, and Ruba Alobaidi
2170002618@iau.edu.sa, 2180004406@iau.edu.sa, 2180000618@iau.edu.sa, 2180003294@iau.edu.sa, 2180002836@iau.edu.sa
IAU University, saudi Arabia , Supervised By: Dr. Naya Nagy.

Abstract
Biometrics is an application of biometric authentication and identification techniques that are used for security. Where people can be identified by physical or behavioral features such as iris, fingerprints, or even voice. Biometrics with cryptography can be used in a variety of applications such as issuing, generating, or associating biometric keys. Biometric identification and cryptography are used in many institutions and high-security systems due to the difficulty of tampering or forgery by hackers. In this paper, literature reviews on biometric identification and cryptography are presented and discussed. In addition to a comparison of techniques in the literature reviews, identifying its strengths and weaknesses, and providing an initial proposal for biometrics and cryptography.

Keywords:
Reverse engineering, Code obfuscation, Byte code, Disassembler, and assembly.

1. Background

The safeguard of confidential data from being disclosed or altered is an immense challenge around the globe. It is because several industries are moving to digitization, and as a result, extensive security protection is needed. Ordinary cryptographic methods to ensure authentication and privacy are not efficient anymore since the password can be compromised easily or sniffed. Biometrics-based cryptography is used to overcome the deficiencies found in the usual techniques. Mechanisms like iris-based and fingerprint-based cryptosystems have proved their capabilities when it comes to authentication and key negotiation.

2. Problem Statement

There are several issues regarding biometric identification. One of the issues is the lack of privacy, face features and fingerprints are publicly available to everyone. Anyone can see someone's face, voice, or prints, obtain a high-resolution sample of it and use it to hack into the victim's account. In addition, if biometrics were hacked, it will be almost impossible to change them, unlike passwords. Another significant issue is the false positive and negative rates. False positives happen when the identification system wrongly identifies a person's characteristics as a match with another characteristic. False negatives happen when the identification system is unable to correctly detect a match between the input and the characteristics template. These false rates can affect the accuracy of the identification system. Fortunately, there are many cryptography schemes proposed to prevent such issues from happening.

3. Literature Review

A. AlSaggaf [1] proposes a secure cryptographic authentication method based on the discrete logarithms problem. The security study of the proposed method shows that its security properties are important to the discrete logarithm problem. The provided scheme was used to develop a biometric cryptosystem. The proposed method was evaluated on 70 different eyes, each wyes having 7 samples, from the database of CASIA iris. Setup, commit, and open are the three processes that are implemented in the suggested method. The sender, recipient, and trustworthy third party are the other three parties. The following are the steps of the strategy in brief:

- The sender will commence the setup procedure, which will result in the system settings being posted to both parties.
- After that, the sender encrypts the message, chooses a random witness, calculates the commitment, and delivers it to the recipient.
- The receiver calculates the commitment and examines if it fails; if it does not, the commitment is successfully opened, and the hidden message is acquired.

The results of the experiments demonstrate that the proposed method is more accurate, capable of coping with up to 21.41% of mistake bits in an iris code and

Manuscript received May 5, 2023
Manuscript revised May 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.5.6

producing up to 98 bits of the cryptographic key from the iris codes. Furthermore, in terms of mechanical concealment and arithmetic binding, two security characteristics of the proposed technique have been described. The concealment feature works by preventing an opponent receiver from figuring out either the secret word or the witness. By showing that the variance vector provides a receiver with almost no statistical benefit over the committed secret phrase or witness. The binding property, on the other hand, protects against the receiver's efforts to extract a secret word for a number picked at random.

According to A. Alsulami et al. [2,] combining iris biometric technology with cryptography will result in high-security identification and productivity. An iris-based cryptosystem may be the safest technique for creating a key and authenticating users along with other biometric identifying methods such as voice and fingerprint because of the unpredictable, uniqueness, and stability of the Iris. The authors present great biometric security techniques for iris recognition systems with high confidence and performance, and they also improve security by employing the fuzzy vault scheme, which is based on two criteria: a 128-bit AES cryptographic key and biometric data. As a result, if one criterion, such as a key pair, is compromised, the attacker still has no knowledge what the other factor is. Due to their complete independence, the attackers are unlikely to get both of these different input factors.

Ren and D. Zhang [3], proposed a biometric identification scheme using visual cryptography to provide a secure and private way to keep the biometric features in different databases. The proposed scheme is divided into two main stages. First, the friendly visual cryptography scheme (EVCS) is used to solve noise shares weakness and pixel expansion. The normal VC has a traditional pixel-by-pixel encryption method called pixel-by-pixel encryption, which uses two corresponding matrix collections, C0 and C1, to represent a white (w) or black (b) pixel in the secret image. n * m binary values make up C0 or C1. The algorithm encrypts data by randomly choosing a matrix from C0 or C1 and assigning each row of pixels to the corresponding share. Rows are composed of m subpixels each interpreted as a recovery) w) or (b) pixel. Moreover, one drawback of the VC is that the images generated look like meaningless noise even though these images cannot disclose secret image information. Hence, EVCS is better in that it considers the color of shares generated as well as the wanted secret image. In EVCS, 4 subpixels are expanded from every pixel whether black or white. Furthermore, to encrypt a black pixel, the subpixels will be all black (0000) while encrypting a white pixel will give a result of one white subpixel and three black subpixels (1000). In order to solve the expansion problem, the block-wise process is used by splitting the grey level image into black blocks and white blocks. In the second main stage, a new scheme is introduced to identify face images. The neural network is used to match the images and transform them to weights in the network. After that, the weights can be sent to other neural networks by using transfer learning. Moreover, a loss function is used to produce an efficient model that can work as a classifier to find identical images. In the training phase, two samples are chosen, the positive and the negative in addition to the anchor of both samples. For a great performance, the three samples have to be carefully chosen. the model will classify the result as 0 if the distance between the positive and negative samples is larger than the threshold. In addition, the image is divided into two or more images to provide biometric privacy. The features of these images are extracted using the deep neural network to be fed to the loss function and then the model. Back to the identification process, the identification system will send the shares to the servers. Then, the system will eliminate the produced private image. Consequently, the private image can only be decrypted while in use due to the fact that the biometrics information is hidden from the servers. Finally, the proposed scheme was examined and showed high efficiency, accuracy, and good performance.

S. Kalsoom and S. Ziauddin [4], Iris recognition is considered one of the most important and popular biometric authentication techniques. The iris recognition system performs three important steps which are iris segmentation, iris normalization and iris feature encoding, so that it can capture and identify the human eye using the infrared iris sensor. The main objective of this paper is to identify and classify the problems related to this technology in terms of security. As for the security of the iris recognition system, since the loss of biometrics is associated with the loss of a person's identity, it is divided into several sections.

1) Traditional biometric systems: they store user templates in the database without using encryption and in an explicit form, this affects security and privacy.
2) Biometric key release: These systems secure the encryption keys, but they do not protect the template itself, which exposes it to security problems.
3) Cancelable biometrics: This system does not store the main template in the database, but rather implements a function on the template and then stores this template in the database after conversion. When the converted template is exposed to danger, the main template is not affected.
4) Biometric key generation: In this system, neither the biometric template nor the encryption key is stored in clear text.

A. Ross [5], This paper suggested five modules that help in decision-making in iris recognition systems:

1) Acquisition module: It obtains a two-dimensional image by using a CCD camera that is sensitive to the NIR spectrum, and then takes a series of images so that he can choose a single high-quality image that contains sufficient information about the iris.
2) Segmentation module: This module isolates the spatial extent of the iris from the rest of the other structures, such as the pupil, eyelids, sclera, and eyelashes.
3) Normalization module: This unit converts a segmented iris image from Cartesian coordinates to polar coordinates by invoking a geometric normalization scheme. This unit has many advantages such as:
    - Considering the difference in the size of the pupil that occurs due to changes in external lighting.
    - During the matching stage, he makes it possible to record the iris of the eye through a simple translation process that enables it to calculate the rotation of the eye.
4) Encoding module: makes a protein to extract features to encode the content of the iris. Then he performs a multiple analysis of the iris using encrypted algorithms.
5) Matching module: This unit determines how well the code that was produced matches the encrypted features that are stored in the database.

Chen et al [6], Proposed a biometrics-based system to secure the E-Health systems. The suggested solution covers different security issues in the functionality of E-health systems, including local and public communication and terminal and server preprocessing. Biometrics-based fuzzy & key negotiation (BFAKN) and fingerprint-based authority access mechanism (FAAM) are the proposed security schemes to attain data confidentiality and integrity of the health records. The fuzzy vault secure sketch technique is used for authentication and key negotiation. The secure sketch consists of SS and Rec algorithms; the SS algorithm is used to generate a vault that calls S to the receiver by acquiring the biological signals from the sender to extract w, which is a noisy input, while the Rec algorithm is used to recover the w` that is used to generate the key. After implementing this, there will be a mutual authentication between sensors & terminal and server & terminal which will result in solving local and public communication issues. FAAM is implemented to obtain different access ranges from various authorities since the E-Health is made of different authority levels. The terminal can be accessed if there is a match in the fingerprint; otherwise, the request will be denied. In conclusion, the accuracy rate related to the proposed system is 93.5 %, with a false rejection rate equal to 6.4 %.

To ensure the security of the electronic health system, Kausar [7] proposed an iris-based cancelable cryptosystem. The proposed scheme overcomes several security-related issues, including cross-matching, brute-force, and masquerade attacks. The implementation of the system is divided into two stages an encryption phase and a decryption phase. The encryption stage takes the human trait as an input, the encryption key, and health data related to the patient; the output of this stage is the hash of the encrypted key and the encrypted health data of the dedicated person; the outturn of this stage is saved in

a smart card. The smart card is an ideal choice since the attackers can't get any information about the secret key or the patient's data when the card is lost. The decryption stage is utilized to get the encrypted data through the smart card without providing the key used for the encryption; it only takes an image of the patient's iris and data from the smart card. The suggested system solves the key management problem since it uses symmetric key encryption that allows both patients and healthcare providers to share the same key. The testing phase was done using the CASIA-IrisV3-Lamp database that holds 411 user's images of left and right eyes; the testing was done on 100 samples utilizing the left eye; the false rejection rate (FRR) was 7% when the key size was equal to 256 bits.

The goal of the proposed system by Prasad et al [8], is to raise the level of biometric security to a higher level. The system can be used to log in as an administrator to log in and manage information or as a client with low permissions. The system uses a combination of fingerprint scanner, encryption, and the use of OTP on mobile phone and mail too. The fingerprint of each user is stored in a database and retrieved for authentication. The AES algorithm is used for encryption and data retrieval. It also uses the TOTP algorithm (TIME-BASED ONE-TIME PASSWORD) which is free and simple, where passwords are generated by the user, not the server, and this It helps to create a different password and argument all the time.

4. Strengths and Weaknesses

Based As for the strengths and weaknesses of the purifications, in the literature review, we find a diversity between the systems, and each system has certain advantages and strengths in a particular field, and it has weaknesses in another. Among the most important strengths of some literature reviews S. Kalsoom et al [4], discussed, many popular beliefs about security, reliability, stability, and performance of iris recognition systems are not correct and need to be revisited. As explained by A. Ross [5], the main strengths of biometrics are that the iris's complex texture and its apparent stability hold tremendous promise for leveraging iris recognition in diverse application scenarios, such as border control, forensic investigations, and cryptosystems. In addition, the proposed solution by Chen et al [6], helps in dealing with several problems, including the public and local communication issues. Also, it uses many techniques to ensure authentication and data confidentiality. The suggested solution done by Kausar [7], can overcome several security attacks, including brute-force and masquerading attacks. In addition to the system strength in Ren and D. Zhang [3], the proposed scheme can reduce the complexity of the traditional cryptographic schemes and solves the issues of pixel expansion and noisy-like images. The proposed system by Prasad et al [8], had a strong point on the diversity of systems in addition to biometrics because the system uses a combination of the fingerprint scanner, encryption, and the use of OTP on mobile phones and mail too.

One of the major weaknesses of the literature review is the proposed system by S. Kalsoom and S. Ziauddin [4], could lead to a design of a multi-biometric system that overcomes the weaknesses of one by the strength of another biometric. The problem in the suggested system by Chen et al [6], is that there is nothing mentioned about its strength against different security attacks. There is a downside to the Fuzzy Vault approach by Alsulami et al [2], once the sender has encrypted the vault and sent it to the recipient along with the user's public key The vault will be obtained by decrypting the message with the user's private key. As a result, the recipient has the ability to impersonate the originator.

5. Comparison

The comparison is done based on what the literature reviews examined. Most of the papers had the following criteria in common. Efficiency is used to describe how fast the technique can give the wanted results with few resources. Effectivity describes how the techniques always provide wanted results in a reasonable time. Accuracy refers to the correctness of the results. Performance refers to how the techniques perform tasks in the desired way. Lastly, Security is how the biometrics are encrypted and secured from unauthorized parties.

Table 1: Comparison Table

Reference	Efficiency	Effectivity	Accuracy	Performance	Security
[1]	More efficient compared with other techniques.	-	High accuracy rate.	Low performance.	Security is improved by adding an encryption key.
[2]	Encrypting the iris is an effective method of encryption	Effective.	Depends on human factors.	Depends on pupil dilation	Enhanced by adding a Fuzzy Vault System.
[3]	Efficiently send private information in plaintext.	The system recognizes effectively.	High precision and accuracy.	The system performance is good but not the best due to the noise.	The system is secure and private.
[4]	-	Not effective.	Not completely accurate due to dilation effect.	Low performance.	The system had an issue in term of security.
[5]	Efficiency especially in military applications that demand rapid identification of individuals.	Effective.	High accuracy rate.	High performance.	The system is secure.
[6]	The technique is quite Efficient since it uses several techniques sequentially to do the authentication.	Effective in term of key negotiation.	High precision and accuracy.	High performance.	The technique achieves high level of privacy and security.
[7]	Efficiently uses the proposed techniques to do an iris- based cryptosystem to do authentication.	The system works on authenticate patients based on their iris image effectively.	High accuracy rate.	The performance is quite good when it comes to the time complexing calculated during the testing phase.	Strong enough to overcome serious attacks including masquerading attacks.
[8]	Through applying the digest, it is increasing the efficiency	Effective	Using of biometric, increase the accuracy	High performance.	bio-metric provides a security to sensitive data, and identification

6. Proposed solution

Iris recognition is one of the most widely used and most reliable methods among all biometric solutions such as fingerprint, facial etc. Accordingly, it was difficult to search for alternative solutions to this technology because it is much easier than all previous technologies, fast and does not have physical contact, as it is healthier when used in health care and is also captured from a distance. Therefore, the solutions proposed by the researchers are to reduce the defects that exist in it, which includes not using the regular camera and that it is expensive. Also, the person must be stationary when moving in front of the iris scanner, which is considered difficult in most cases, so scientists are currently working on the limitations of the iris recognition technology.

7. Conclusion and Future work

In this paper, literature reviews on biometric identification and cryptography are presented and discussed. Furthermore, we made a comparison between the techniques mentioned in literature reviews based on the common criteria (such as effectivity, accuracy, performance, and security), identifying their strengths and limitations, and making the first suggestion for biometrics and cryptography. As a result, a high level of security is required. Ordinary cryptographic approaches for ensuring authenticity and privacy are no longer effective since passwords may be readily compromised or sniffed. Biometric identification raises several concerns. One of the concerns is the lack of privacy, face characteristics and fingerprints are publicly available to everyone. So, we suggest developing a scheme that combines the biometric identification system with the cryptographic key in future where we can raise the level of biometric security to a higher level because the system can be used to log in as an administrator and manage information or as a client with his permissions.

References

[1] Al-Saggaf, A., 2018. Secure Method for Combining Cryptography with Iris Biometrics. Dammam: Journal of Universal Computer Science.

[2] Alsulami, A., Darren, T. and Weiyi, H., 2012. Combining Iris Biometric System and Cryptography Provide a Strong Security Authentication. Australia: American Research Journal of Computer Science and Information Technology (ARJCSIT).

[3] L. Ren and D. Zhang, "A Privacy-Preserving Biometric Recognition System with Visual Cryptography," Advances in Multimedia, vol. 2022, 2022.

[4] S. Kalsoom and S. Ziauddin, “Iris Recognition: Existing Methods and Open Issues,” 2012. [Online]. Available: http://personales.upv.es/thinkmind/PATTERNS/PATTERNS_2012/index.html. [Accessed: 09-May-2022].

[5] A. Ross, “Iris recognition: The path forward,” IEEE Xplore, 12-Mar-2010. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5410705. [Accessed: 09-May-2022].

[6] Chen, H., Ding, D., Su, S. and Yin, J., 2020. Biometrics-based cryptography scheme for E-Health systems. Journal of Physics: Conference Series, 1550(2), p.022039.

[7] Kausar, F., 2021. Iris based cancelable biometric cryptosystem for secure healthcare smart card. Egyptian Informatics Journal, 22(4), pp.447-453.

[8] P. Pawar, S. Datar, N. Ranade, K. Thorat, and P. A. N. Gharu, “Canteen Automation System using Android - IJIRT ,” International Journal of Innovative Research in Technology, 2019. [Online]. Available: https://ijirt.org/master/publishedpaper/IJIRT147528_PAPER.pdf. [Accessed: 09-May-2022].