Mustansiriyah Journal of Pure and Applied Sciences, Print ISSN: 2957-9910. Online ISSN: 2957-9929, Vol. 4, No. 1, 2026, Pages 139-156
DOI: 10.47831/mjpas.v4i1.322

MJPAS MUSTANSIRIYAH JOURNAL OF PURE AND APPLIED SCIENCES

Journal homepage:
https://mjpas.uomustansiriyah.edu.iq/index.php/mjpas

RESEARCH ARTICLE – COMPUTER SCIENCE

A Comparative Study on User Authentication Methods

Shaimaa Sattar Abood[1], Ekhlas Abbas Albahrani [2]

[1]Department of Computer Science, Ibn-Al Haithem College, University of Baghdad, Baghdad, Iraq
[2]Department of Computer Science, Mustansiriyah University, Baghdad, Iraq

E-mail: shaimaa_sattar@uomustansiriyah.edu.iq ; akhlas abas@uomustansiriyah.edu.iq

Article Info.

Article history:

Received
16 September 2024

Accepted
9 October 2024

Publishing
30 March 2026

Abstract

Everyone needs security, to use the internet, systems, and applications safely, protect their information and data, and prevent undesirable access. Authentication plays a critical role in security. There are many types of authentications, each one produces a unique method to confirm a user's identity. Password-based authentication is the most popular method, despite vulnerabilities and breaches. In this paper, a brief overview of traditional user authentication methods (Passwords, Smart-Card Authentication, and Digital Certificate Authentication) and Biometric Methods are provided. In addition, the Strengths and the Vulnerabilities of each technique are described. Biometric authentication is based on a unique physiological or behavioral character like the user's fingerprint, voice, retinas, and facial features. It provides powerful security depending on unique characteristics and features that are difficult to replicate or steal. Thus, biometric authentication provides more reliable user identification than other methods despite that traditional method like passwords are prevalent, biometric authentication offers highly reliable performance in security. The basis of the biometric system is a model recognition system.

The official journal published by the College of Education at Mustansiriyah University

***Keywords**:* Authentication, Security, Biometric, Identification, Recognition.

1. Introduction

Computer networks have been growing at an explosive rate. In a wide scope of environments, such networks have become an important tool. Organizations are developing networks on larger scales, and connectivity with the global Internet has become essential. That's led to an explosion in the use of computer networks as a means of illegitimate access to computer systems, and with the increasing amounts of personal information on the Web, it is necessary to remain cautious of the risks of easy access to our private details [1]. Everyone needs security because it enables people to use security systems safely and prevent undesirable things to be happen. The safety system should be strong, flexible, cheap, and work without being limited by working hours [2]. Privacy and security are the major challenges for everyone, organizations, persons, and companies to prevent the growing number of data breaches. User authentication is essential to protect sensitive data and prevent unauthorized users from gaining access [3]. Authentication is a method of validating the identity of an individual or something. It uses details given to the authenticator to determine whether an individual or something is who or what it is declared to be. In computing systems either private or public, like computer networks the authentication process involves someone, who is usually the user, using to logon the provided password by the system administrator. To demonstrate that the user is knowledgeable about something that no one else could be, he enters this password at login. Authentication requires in General the presenting credentials information or elements of value to prove the claim of who one is [4]. Authentication is a significant means to prevent various common attacks and to protect personal data, valuable data, and important information from unauthorized access. There is a broad assortment of authentication methods extending from knowledge-based (e.g. passwords) to biometric (e.g. fingerprint) to token-based (e.g. chip cards) has been sophisticated [5]. If there is no right, implementation of an authentication algorithm in the network then an attacker can earn access and steal important information, credentials, and secret special data which can harm to the network or the user. So, Authentication is

one of the significant security elements for networks, systems, and individuals, based on which various devices and users can do communication with each other and can share data safely [6]. Users are specified using different authentication methods. The authentication procedure in security system examines provided information from a user with the database. If there was a match between the provided information by the user and the database information, then the user earned access to the security system. There are three variables used for authentication: something you know which is user name and password, something you have which is using a smart card, and something you are, which is a set of physiological or behavioral characteristics, and that means using biometrics methods [7]. Traditional systems based on the use of passwords and identity cards cannot achieve always secure authentication functions because they have a lot of weaknesses. the password can be forgotten or decoded by another person and the identity card or key may be lost or stolen. Biometric systems are a good alternative solution to the two previous authentication methods. Biometrics involves identifying a person from one or more physiological characteristics (fingerprints, face, iris, hand geometry, retina, palmprint, etc.), or behavioral characteristics (signature, gait, keystroke dynamic, etc.) [8]. The technicality for determining and verifying an individual's identification based on one or more physical or behavioral merits is called biometric technology. In other words, it turns personal features or attributes into a password to enable access to information systems. People can be identified essentially from features that can be cleared up as physiological or behavioral features. These technologies work just as the backbone of extremely secure systems for the identification of personages [9].

Because there aren't enough sources to discuss all types of user authentication, as well as how to design and build them, this paper aims to conduct a comprehensive study on user authentication methods to gain a clearer insight into their security and usability, as well as how they mitigate risks and what threats are still possible to endanger users' credentials.

The remaining sections of the paper are structured as follows. The User authentication requirement, evaluation, and security analysis are covered in Section 2; the performance estimation and measurements of password and Biometric authentication systems are given in Section 3. Authentication types are provided in Section 4. Final Section 5 offers a succinct conclusion

2. User Authentication Requirement, Evaluation, and Security Analysis

There are three basic requirements authentication systems are supposed to meet which are availability, integrity, and confidentiality, contra different attacks [10].

- **Availability:** - is the first requirement which means the availability of system resources to genuine users. The main target for denial-of-service attacks is compromising the availability, by preventing legitimate users from gain access to their resources.
- **System integrity**: - is the second requirement which means ensuring the authorized users are connected to their actions, and it implies the intruder defeats and rejects his request to transact with system resources and defeat the insider users' threat.
- **Confidentiality**: - is the third requirement which means warranty of the user's privacy and confidentiality. This requirement aims to function creep threats which allow the stealing of the features of the user authenticating to control of resources and another system.

2.1 The Entities of Authentication Methods

The authentication process implies the following entities [1]:

1. The claimer entity is the one that authenticates to the system to use the services. The claimer entity could be an information system or an individual.
2. The observer or the security system that provides the authentication service, confirms or rejects the claimer's identity and checks if can admit him or her to use the required services
3. The Information System supplies services, such as an entry to an application, a computer account, and a network printer. If the observer authenticated the claimer correctly, he or she can use the Information System services.

2.2 The General Basic Procedures for Authentication

There are three basic procedures for the authentication method [1]:

1. Initial phase: the claimer is unauthenticated.
2. Connection phase: the claimer demands the Information System to use the function that requires authentication. The Information System asks the observer to authenticate the claimer.
3. Authenticated phase: authenticated the claimer and a session is opened. The Information System provides the needed functions for the user.

When a time out or the user does an action, this phase is initiated, which is user disconnects or is disconnected and returns to the initial phase [1].

For enhancing security mechanisms, a different authentication method has been proposed, each method has its advantages and limitations

1. **Usability:** - is one of the important obstacles in usability of authentication methods. To protect the network system, the authentication method must be secure enough to renitent the different security and privacy threats, and the authentication method must be easy to use. Authentication methods are more complicated and less easy to use when designed with a great focus on security. The authentication method with high usability is biometric authentication in contrast to the password that needs effort to remember or memorize.
2. **Security:** is critical in estimating the authentication methods. It meant the ability to withstand attacks, traditional password-based systems and biometric-based systems are vulnerable to different types of attacks.
3. **Privacy:** - it's also critical in estimating the authentication methods. The problems concerned with security and privacy like insecure access, changing or deleting information, and gaining critical data can be reduced by using an appropriate authentication process [11].

2.3 Security Analysis

There are many different kinds of attacks and breaches through forged accounts or learning data. Hackers can larceny personal data and accounts or change the gain data. The major challenge of security is surmising the passwords of the accounts. Biometrics are easy to use compared to traditional authentication methods, cannot be shared, are convenient, cannot be forgotten or missing, are trustworthy, and are easy to use. Biometric authentication compared to other authentication methods is highly reliable because it's harder to forge the physical human tiers than the password, cards, codes, and hardware keys. There are many various challenges when secure systems are designed to recognize and defend averse to impendence, attacks, and exploitable vulnerabilities. The most common results of capitalizing on vulnerability are security breaches [2].

- **Brute force attack**: Traditional systems that are based on passwords are prone to brute force attacks and dictionary attacks. In a brute force attack, the attacker has a try to enter all potential passwords in a dictionary defined by a user. This type of attack avails the vulnerability that users do when they choose the passwords: simple, easy, and short-length passwords to remember them easily and rapidly. In biometric systems, until successful recognition, the attacker sends off all potential combinations of secured information to the decision-making module [12][13]. There some defense mechanisms and security measures to protect against brute force attacks in user authentication systems have been proposed, like:
  1. Automated Turing Test (ATT), this test can distinguish between people and machines. The general forms of ATT tests are SMS authentication codes and challenge questions
  2. Account locking, which is done by determining the number of incorrect login times.
  3. Key space examination, the key space size should be large sufficiency, to prevent brute-force attack [12].
- **Guess attack:** this type is more efficient than the brute force attack to identify a user's password because most passwords are based on the preferences, knowledge, and experiences of the user. Accordingly, if the attacker knows the target user the guess attack will be easy.

- **Shoulder-surfing attack:** This attack is prevalent in our diurnal lives, easy to perform, and it may cost nothing for meddlers. When individuals enter their personal information into computers or mobile phones, their actions can easily be observed over their shoulders by other people or by registration the entering process of passwords ply an unobserved camera. There are various authentication schemas to prevent shoulder surfing attacks, such as familiar safe keypad schemes including qwertybased, ABC based, Touch and Slide Secure Keypad, etc. But conventional solutions are not enough safe. Some defense mechanisms are safe but harsh to use because they demand composite procedures like Tic-Toc PIN which has high security with low usability. The Revolving Flywheel PIN Entry Scheme (CaRP) is a powerful authentication procedure to defend against guessing passwords through shoulder surfing which denies attackers from guessing complete contents or passwords. It consists of three layers (outside, middle, and inner) and provides several authentication schemas to users which ensure authorized access, security, and usability [12].
- **Phishing attack:** Phishing persuades users to visit forged websites by downfall them with forged emails and that allows attackers to gain users' sensitive information, like passwords, PINs, and credit card information. To guard against phishing attacks, users must be cautious about spam emails and use technical defense procedures such as using spam filters, observing networks, meliorative web security by using biometrics or hardware devices, and installing anti-phishing software [12].
- **Hill-climbing attack:** A forge model of biometrics is sent iteratively by an attacker to the decision-making module until its recognition. At each attempt, the attacker receives feedback to modify the forge model.

While biometric authentication gives a high point of security, it is still far from the perfect solution. since no user authentication method achieves all the demands in every operational ambiance, so as a result to defeat such problems we need more than one authentication method and many biometric characteristics of a personage to be used to obtain a strict performance warranty needed by actual-universe implementations [13].

Table 1. Synopsis of existent attacks on authentication systems [12]

Attacks	Knowledge	Target	Strength
Brute force attack	F	P	Mod
Guess attack	Mod	P	Mod
Shoulder-surfing	Mod	P	Mod
Phishing Attack	F	P	S

F=Few; Mod= Moderate; P=Password; S=strong

The techniques known as biometric template protection or biometric information protection supply protected data that conceals crucial details about the user's identity or the original biometric data. The protected information is renovated, by revoking and renovating randomly formed extra information, which is used in these ways to conduct protection. Random number generators must therefore be secure and have little computational overhead for applications involving biometric systems. Physical unclonable functions are therefore a great way to produce safe random data. Generally, there are approaches based on hardware and software to protect the biometric systems, while biometric template protection techniques are software-based. Thereafter, a biometric system can perform:

a. liveliness certification.
b. a safe channel amidst the user interface and processing unit.
c. an expert hardware processing unit.
d. biometric template protection techniques with secret and unrivaled random number generation on every integrated circuit.
e. a biometric system can perform physical separation of the database.

There are three forms in the enrollment phase for stockpiling protected information:

1. Online or central database: On a single storage device the protected information of all users, like cloud storage.
2. Offline or Local database: every user has a personal storage which is a storage device with their protected information. The storage device can be a USB, chip, smart card, magnetic strip, smartphone, smartwatch, etc.
3. Hybrid database: In a central database a proportion of the protected information is stored and in a local database the rest is part of the information.

The information in the hybrid database is on several devices, accordingly, this database improves security, and the partial liability of the users is the domination of the information. The administration of cancellation of protected information is simpler with a central database. Furthermore, a private key is used by the hybrid storage to decrypt data, and avert vulnerability when the storage device is exposed [13].

3. Performance Estimation and measurements of Password and Biometric Authentication Systems

There are many different mensuration to gauge the power of the password, its length, difficulty to memory, policy compliance, user contentment, and persuasiveness as these tools "Password Meter" and "How Secure is my Password?" which compute password strength by appending points if the password meets requirements and subtracting points if not. According to the complexity of a password the “Password Meter" tool classifies the passwords giving scores with a maximal score of 100%, so the password strength will be classified as:

1. Very weak password if ($0\% \leq$ password score $< 20\%$).
2. Weakly password if ($20\% \leq$ password score $< 40\%$).
3. Good password if ($40\% \leq$ password score $< 60\%$).
4. Strong password if ($60\% \leq$ password score $< 80\%$).
5. Very strong password if ($80\% \leq$ password score ≤ 100).

The "How Secure is my Password?" tool measures the computer cracking time of passwords, with consideration of password length, if the password appearance as dictionary word, and character variation. Participants' passwords were estimated based on strength and cracking time. Password policy compliance is another measurement tool, where the entrants should follow the specified password policy rules, Passwords were given scores: (0) indicates that the specific rules had not been applied, (1) indicates that the specific rules had been applied by the entrant [14].

A performance evaluation technique is often used to estimate the correctness of the recognition infrastructure in biometrics, and there are common performance pointers which are False Accept Rate (FAR), False Reject Rate (FRR), and Equal Error Rate (EER).

1. **False Acceptance Rate (FAR):** - This performance pointer which is also known as the false match rate (FMR) is specified from the percentage of how frequently authentication methods accepted an imposter as a valid user. It is evaluated by equation no. (1)

$$\text{FAR}\ (\%) = \frac{\text{Number of false accept}}{\text{Number of imposters tested}} \times\ 100 \qquad (1)$$

2. **False Rejection Rate (FRR):** - A performance pointer also known as the false nonmatch rate (FNMR) can be determined from the percentage of how frequently authentication methods decline a valid user as an imposter user, it is computed by equation no. (2)

$$\text{FRR}(\%) = \frac{\text{Number of rejections}}{\text{Total number of users tested}} \times\ 100 \qquad (2)$$

3. **Equal Error Rate (EER):** - This performance pointer value also known as the intersection rate or intersection error rate displays the relationship between the balance of false acceptances and false rejections. The lower the EFR value, the better the performance of the biometric authentication method. The EER is evaluated by equation no. (3)

EER = FAR where FAR = FRR (3)

4. **Genuine accept rate (GAR):** - It is specified as the proportion of digits of genuine recorded users is validated by the authentication infrastructure. It can be computed by using (4) and (5) equations

$$GAR = \frac{\text{Number of genuine user accepted}}{\text{Total number of genuine trials}} \quad (4)$$

GAR (%) = 100 – FRR (%) (5)

The Equal Error Rate (EER) is the point where the proportion of both false acceptances and rejections is equivalent. Decreasing the FAR can increment the FRR, making the authentication method less secure. Contrariwise, decreasing the FRR can ameliorate user acceptability, making the system less secure. The Receiver Operating Characteristic (ROC) curve is known as a plot of FRR (or GAR) versus the function of FAR. When the axes of such a plot are on the norm veer scale, this plot is indicated as a Detection Error Trade-off (DET). The biometric method execution can be summarized with one digit, expressed as an operating mark. The mark wherever the FAR amounts to the FRR and is known as the Equal Error Rate (EER) is the operating point [15].

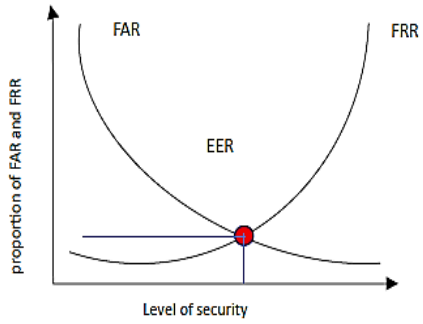


Figure (1): FRR and FAR versus the level of security of a biometric authentication system

4.Common Types of Authentications

4.1 Password Authentication

This type is known as a single factor/knowledge-based authentication and it's the most generality form of user authentication technicality used in diverse implementations like banking websites, ATMs, login to operating systems, and mobile phones. Password authentication requires the user to enter the user's name and the password which can be words, numbers, or a combination of words and numbers, then the system examines the user identity and the entered password by matching its secure list of known identities and passwords [16]. Table 2 shows the strengths and vulnerabilities of password authentication.

Table 2: The strengths and vulnerabilities of password authentication

Strength of Password Authentication	Vulnerabilities of Password Authentication:
when a password is a long string with a series of small and capital state, numbers and distinguished characters it will be a strong password and it is difficult to break.	a. The large number of passwords a person needs to remember, thus a long and difficult password can easily be forgotten. b. users often have to juggle many different passwords, which makes it difficult to create and maintain powerful and unrivaled passwords per account. c. the increasing of cybercriminals makes password-cracking tools and techniques more

	advanced, allowing attackers to easily brute-force or guess weak passwords [17].

S. Subangan and V. Senthooran in 2019 [16] introduced a study about a secure authentication mechanism based on matrix and sector to counter password attacks. The sector-based approach presents high achievement and user satisfaction, classifying characters and changing the session passwords for each try. This approach assures privacy, and exclusiveness and rejects unauthorized access to resources. A paper by Amanpreet A. Kaur and Khurram K. Mustafa in 2019 [18] shows that the major problem with passwords is the cavity between usability and tool backing. Through password meters, robust passwords are obtained for significant accounts, while insignificant accounts are not. Users based on their behavior must be guided. In 2023 Verena Zimmermann, Karola Marky, and Karen Renaud [19] found that the password meters present a committed method to directing users to secure passwords, providing reaction nudges to increment strength and further information on making robust passwords. The experiential results display that using the Roberta algorithm for password complexity prediction owns the highest degree of precision and reliability. A more than 99% precision rate means that the model has a high degree of correctness in the prediction operation and can efficiently distinguish and determine password complexity. This will quietly boost users' attention and awareness towards personal information security problems and encourage them to take extra strong and efficient defense measures [20].

Table 3: Comparison of password authentication systems

Ref. no.	Resistance	Performance	User Convenient
16	-High Resistance to shoulder surfing, interception, keylogging, and phishing. -Moderate Resistance to brute forcing and dictionary attack	High	High
18	High Resistance, very hard to guess	High	High
19	High	High	-
20	High Resistance to: -guess attack - user impersonation attacks	High	-

4.2 Smart Card Authentication or Certificate Authentication:

In this type of authentication “something a user has” is a smart card which is a credit-card-sized card that a certificate has been embedded in, used to identify the holder. The smart card is inserted by the user at a smart card reader to confirm the individual. Smart cards are often used together with a PIN providing multi-factor authentication. So, the user has to own a smart card and know the PIN. Table 4 shows the strengths and vulnerabilities of Smart Card Authentication.

Table 4: The strengths and vulnerabilities of Smart Card Authentication

Strength of Smart Card Authentication	Vulnerabilities of Smart Card Authentication
a. The smart card comes in two varieties, firstly with a memory card to store data. Secondly, with a microprocessor, which makes it more powerful in two-factor authentication. b. If the pin is untrue after several endeavors, the smart card is locked. c. It prevents dictionary attacks.	a. For several users it is harsh to recollect the PIN, so they enter the PIN at the back of the card. b. The card can easily be penetration if it is stolen. After a certain number of incorrect attempts smart card can be locked. c. Because it is portable it can also be stolen. d. Some users can be victims of Phishing

d. It's portable and thus can be simply held by the user.	because of frequent purchases online. e. Sometimes PIN can be known [7].

In 2020 [20], Hsieh, Hung, and Min suggested an improved schema by using smart card authentication that suggested schema can defend the guessing identity offense and the user personation offense. In 2020 [21], Li Chen · Ke Zhang proposed a remote biometric authentication schema based on a smart card, it is secure because the aware of the privacy of e-health, treating security faults in multi-factor authentication schemas, and guarantees the preservation of user information and the sensitive health datum. A paper by Shyamalendu, Sumit, and Bibhas, presented a schema of remote user authentication utilizing smart cards for session key conventions and hared validation, computational demands, and security. They found that its potentially beneficial, in billing-intense milieus like multi-specialization hospitals [22].

Table 5: Comparison of smart card authentication approaches

Ref. no.	Resistance	Performance	cost
20	High Resistance to: - guess attack - user impersonation attacks	High	High
21	High Resistance to various attacks	High	-
22	High Resistance to many various attacks	High	High

4.3 Digital Certificate Authentication

The encryption technology that utilizes a piece of information about special and public keys to verify the sender's identity, assuring a secure connection and barring fraudulence on the internet is known as digital certificates. The digital certificates are Private, the private data is secured and protected by digital certificates, and the user- simply utilizes it, operational automatically and demanding minimum procedures from senders/receivers. In simple words, this type of authentication is an encryption technology that works like an Internet copy of a passport [7]. Table 6 shows the strengths and vulnerabilities of Digital Certificate Authentication.

Table 6: shows the strengths and vulnerabilities of Digital Certificate Authentication

Strength of Digital Certificate Authentication	Vulnerabilities of Digital Certificate Authentication
a. Using information about public and private keys, digital certificates essentially ensure to the receiver of a message that the message is coming from a specific person. b. It authenticates the identity of the sender to ensure safer communication. c. The biggest advantages of digital certificate-based authentication are privacy-based. d. protect private data by preventing unintended persons from seeing the information.	a. The intruders attacked the authorities that issued digital certificates and the certificate information was changed. b. Attackers pass the verification test by creating a phishing site and sending websites and emails that look like original [7].

In 2020 Kritsanapong and Mongkhon have suggested for e-certificate signing, an RSA's digital signature to prohibit forging. To manage an e-certificate there are some applications, one of these applications is the signing application to sign a sub-image inclusive only of the entrant’s name in the e-certificate. When every pixel of the entrant’s name matches the decrypted message portions. The

experiential results presented 100% accuracy, quick signing, and examining processes especially when using CRT techniques [23]. Bin, LiJun, and others suggested in 2020, three methods for dispensed certificate disclosure prepared to avert the mistreatment of certificates via harmful unknown users. The experiential outcome demonstrates that the suggested schema has strong defense capability contra connivance and node seize attacks [24]. James, Stephen, Corey, and others 2022 explain how a certificate-based authentication method can yet protect user exclusiveness and reduce the quantity of trust required, so a compromised certificate authority could not impersonate users. They utilized a security analysis to display how the system denies a diversity of threats [25].

Table 7: Comparison of Digital Certificate Authentication methods

Ref. no.	Performance	Accuracy	security	Notes
23	Very High	High	Strong	Best solutions to protect against the forgery of e-certificates
24	Moderate	High	ability against: -collusion - node capture attacks	excellent in: -communication and storage cost -detection rate.
25	High	Moderate	Strong	Has easier recovery from loss

4.4 Biometric Authentication

Biometric authentication points to a cybersecurity procedure that confirm a user's identification using their singular biological characteristics such as fingerprints, voices, retinas, and facial features. Because it is based on a collection of physiographic or behavioral features, biometrics provides the strongest authentication. With the increasing need for powerful authentication systems, the use of biometric authentication systems become widely spread. The human left and right five fingers have dissimilar mark patterns. The fingerprints and facial biometrics of every individual are unrivaled due to the encoded pattern at the interface between the dermis and epidermis. As a result, biometrics are unique, secure, and living passwords to verify the transaction's integrity [26]. Table 8: shows the strengths and vulnerabilities of Biometric authentication.

Table 8: shows the strengths and vulnerabilities of Biometric Authentication

Strength of Biometric Authentication	Vulnerabilities of Biometric Authentication
a. They are distinguished by aloft degree of convenience, reliability, and accuracy. b. Physiological elements are directly personally identifiable. c. They are very hard to compromise, and they equip affordability to prevalent inhabitance as they overcome struggles like users' illiteracy and language obstructions.	a. The possibility of datum infraction and also compromising biometrics database. b. The absence of universally agreeable technical and legal standards for systems interoperability and consumer biometric data protection. c. The need for of implementation advanced detectors and scanners that scan the merit's vitality. d. Biometric systems are prone to errors and they can be "spoofed" [27].

4.4.1 Biometric Methods

Biometrics can be classified as physiological and behavioral. Fingerprint, iris, and facial recognition are some of the biometric physiological modalities. The biometric behavioral modalities include voice and signature recognition, etc. Both these types produce unique characteristic features which make them necessary in the entire biometric process. Measuring an individual's performance on specific tasks is known as behavioral biometrics. The Physiological biometrics, if not all, are more common and accurate [2]. The entire process begins with the receiving of visional information to the giving out of the description of the scenery from what is stocked in the database; it is divided into five essential stages: [28]

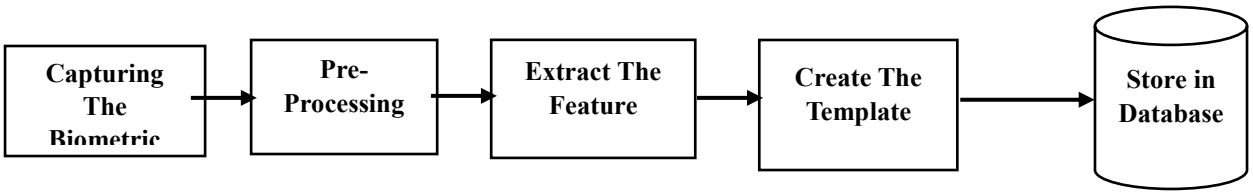


Figure 2: the entire process of enrollment

i. **Enrollment**: when an individual uses a biometric system for the first time called enrollment, where biometric information from an individual is captured to be stored.
ii. **Preprocessing**: all the obtained data are preprocessed to take off noise and enhance the features wanted for reference.
iii. **Feature extraction**: extraction from the biometric all the match points that can be applied for comparison.
iv. **Template creation:** by utilizing an algorithm, as match points the digital biometric data form is processed for comparison with inputs for identification or verification.
v. **A database to store** the information with certain merits is used to create a form that can be compared with the biometric data transmitted as an entry when a user attempts to obtain access [28].

4.4.2 Basic Biometric Authentication Modalities

Automatically a biometric system identifies an individual depending on two major biometric modalities:

- **Physiological Biometrics**: It's based on the identification of particular physical characteristics that are unique and permanent for any individual face, retina, DNA, iris, fingerprint, or hand geometry.
- **Behavioral biometrics**: It's based on an individual certain behavior analysis like his signature, gait, and keystroke dynamic [29]:

1. **Facial recognition:** It is an identification of the people technique based on face detection that works on Nodal Points, which are the endpoints that the camera or the sensor the measurement of points on the face for identification of an individual. This technique also measures the nose width and length, the lip's shape and size, and the cheekbone's size of an individual. The entire face recognition system contains two types, face recognition and face detection. In the biological composition of the face, there is a full structural similarity and various local variances. So, it is necessary to extract the main composition of the expression by the

expression detection operation and to seclude the faces from the related outline. This is a process of mining-controlled face pictures, and then difference and confirmation of identity, the resolution is to determine the trait of the face from the pictures [30]. This biometric modality identifies returning users speedily and effectively by detecting many spoof artifacts, like screens, pictures, masks, etc. And, it is easy to utilize even by phone. However, it can be hard to identify a person's face if there is a complicated background or poor lighting. Also, illness, aging, cosmetic surgery, and accidents cause to fail recognition.[31]

2. **Iris recognition:** The iris is the colored part of the eye; it is a highly reliable technique because it contains a measureless number of characteristic points, the structure of the iris features a complex pattern, and the iris texture of the right and left eyes which belongs to the same person are different. The iris is also called an optical fingerprint. The Iris of a person does not change over time; thus, because of all these reasons, it is possible to distinguish different people by the iris, even in the case of twins [29]. The Iris scanning uses infrared lights for scanning in addition of the technology of digital camera to capture a complicated and particular detailed iris. When an iris has light eradicated on it, the eye will recompense for the exposure and dilate. In the beginning, the scanner has to localize the inner and outer boundaries of the iris. The eyelids, eyelashes, and any shiny reflections that lock up parts of the iris are exposed and excluded by subsequent subroutines. The pixel collection including the iris is normalized via an elastic-sheet pattern to require pupil expansion or tightening. This is next analyzed to elicit a bit pattern encoding the datum required to compare two iris photographs [32]. The iris is an organ that is visible from the outside and is shielded from damage. It is easy to set up and utilize for authentication [31].

3. **Hand geometry:** In multimodal systems, hand geometry is highly often used, whom integrates attributes from sundry biometrics to enhance the implementation and warranty the prospect to authenticate also users for who one trait is missed or cannot metric. The hand geometry is fundamentally combined with palmprint and/or fingerprint, to get high discrimination accuracy, and with hand veins that are severe to spoof and too permit to reveal liveness. However, multimodal systems require more than one sensor to obtain the various traits, generating more convoluted and costly than unimodal ones [32]. This biometric modality is based on several measurements taken from the human hand, like shape, size, and width. Hand geometry is concerned with measuring the user’s hand and fingers which are physical characteristics, from a three-dimensional viewpoint. It measures and analyzes the overall structure, form, and proportions of the hand, including its length, width, and thickness, as well as its fingers, hand curvature, knuckle shape, distance between joints and bone structure, and translucency. It translates those details into a numerical template. To get and measure the hand geometry use a hand scanner, you simply put your hand on the flat surface and let your fingers align against several pegs to get an accurate reading. Then, a camera captures one or more pictures of your hand and the shadow it sheds. In a wide range of scenarios hand geometry readers are deployed, including time and presence recording where they have proved extremely popular. Hand geometry is attractive to many biometric projects because Ease of integration into other systems and processes, coupled with ease of use. The human hand is not unique, unlike fingerprints [9].

4. **Fingerprint Recognition:** A fingerprint is the oldest of all the biometric techniques it is an impression of the friction ridges of all or any part of the finger. It consists of a set of locally parallel lines forming an individual and different patterns for each person. fingerprint recognition was formally agreeable as a valid personal identification procedure and a basic method in forensic science. Because of the strong recognition performance and the low-cost personal computers, fingerprint biometric systems are becoming Very common and used in different applications. Worldwide fingerprinting agencies and criminal fingerprint databases have been created. Automatic fingerprint recognition technology has developed fast past

forensic implementations into civic implementations [8]. The most important benefit of fingerprint scanning is every person's fingerprint is unrivaled. Even for identical twins, the patterns and fingerprint ridges are different. Although fingerprints are easy to scan and unique which makes it hard to be a forgery, techniques for fabricating fingerprints have been developed by fraudsters who use them for unlawful purposes [31].

5. **Voice Recognition:** It is a way of voice communication, every person has a different pitch, Voice Recognition focuses on the vocal characteristics that produce speech. It analyzes distinct voice characteristics, like frequency, pitch flow, and natural accent, to create a unique biometric form for each person. Instead of listening to a voice, these systems excel at evaluating and analyzing the forms and the produced sound characteristics by a talker's mouth and throat to generate a unique signature. This technique eliminates the risk of attempted voice hiding or reproduction, besides the external strands such as ailment or era of day, that can impact a voice's heard qualities to a listener. A feature extraction is performed in the process of speaker recognition to obtain the main characteristics from the speech signal. Then these extracted features are utilized to produce speaker samples for individual speakers. The generated samples are stored in a voice database for later use. Various modeling techniques are employed to generate these speakers [34].

6. **DNA:** DNA provides the most reliable personal identification. It is digital naturally and does not change during a person’s life or after death The deoxyribonucleic acid (DNA) tool up the very trusty personal identification amongst the various types of biometric personal identification approaches. DNA does not change during a person’s life or after death. biometric systems DNA is very firm in crime detection and forensic sciences and thus will stay in the law enforcement field for the time being [2].

4.4.3 Basic assessment of Biometric features properties

The vast probable domain of biometric features has been submitted for comparison with the help of their feature that has been utilized as standards or indicators for comparison. The following seven properties in most studies authors use to describe the biometrics features:

1) **Universality:** the characteristic is included in every individual**.**
2) **Uniqueness:** the characteristic must be sufficiently different about two individuals.
3) **Permanence:** the characteristic must rest unchanged throughout the individual life
4) **Collectability:** indicate to the amount that a biometric characteristic is facilely measured.
5) **Performance:** refers to the achievable accuracy, robustness, and speed of the biometric characteristic. The False Acceptance Rate (FAR) and the False Rejection Rate (FRR)are the most common performance metrics. The FAR measures the scope to which a given biometric method will agree on an incorrect insert, and the FRR measures the scope to which a given biometric method will be unsuccessful in matching a correct insert.
6) **Acceptability:** refers to the degree of preparedness, of the individuals to use a biometric method and to present their biometric characteristics for identification/authentication.
7) **Circumvention:** relates to the simplicity with which the biometric method can be circumvented or fooled by deceptive processes.[26]

4.4.6 Related Works of Biometric Authentication

The keywords we used in this paper like authentication, biometrics, verification, face recognition, privacy, and so on. We learned that biometrics is divided into sub-parts, the first part is physiological biometrics based on the physical characteristics of humans. Such as fingerprints, hand geometry, face, iris, and so on. The second part is biological biometrics which is based on dynamic characteristics such

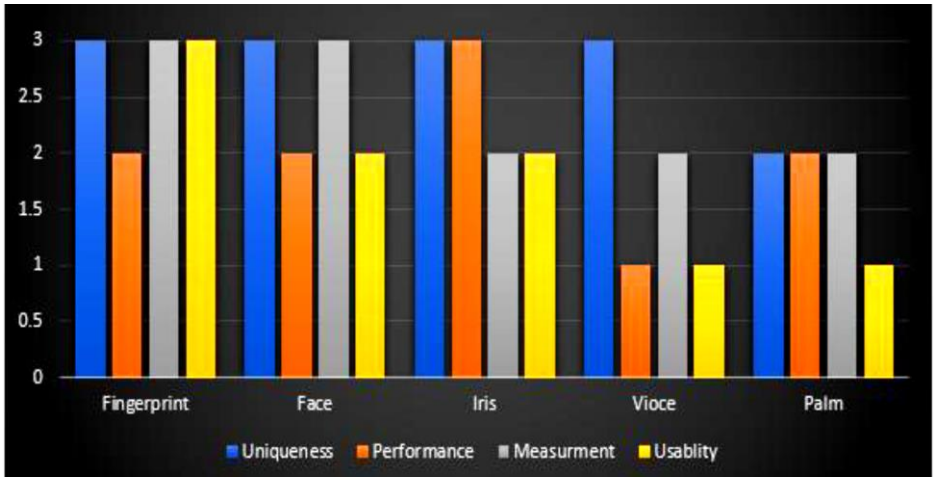
as signature, and voice. The biometric word consists of two words that come from the Greek language “bios” and “metrikos”. Bios means “life” and Metrikos means “measure”. Much research has been done on biometrics. Every researcher said something new about biometrics. In 2015 Silvia found after a basic measurement of the biometric authenticators with the seven criteria that the most appropriate biometric methods are -iris, face, and fingerprint [27]. In 2020 Shaveta and Munish introduced A Comprehensive Survey on the Biometric Recognition Systems based on Physiological and Behavioral Modalities, and they found that the technologies of 3D biometric methods compared with the 2D biometric processes are more secure. Which are designed to obtain high security, more acceptable to differences, high robustness, and provide a rich source of information. To enhance accuracy and reliability, the 3D biometric technologies can integrate with the 2D biometric technologies [38]. A comparative and analysis study of biometric systems was introduced by Ennaama, Benhida, and Boulahoual, they have investigated an analytical comparison of different biometric methods such as fingerprint, voice, retina, etc. They classified these methods based on several properties: Universality, Uniqueness, Permanency, Collectability, Acceptability, and performance. They reach to a result which is the fingerprint biometrics still the most vastly used method around the world and the most required in the universal market. This technique is reliable and intrusive. The iris method with the retina technique provides and ensure a high level of security. These three biometric methods need great cooperation from the users [8]. Rohit and Krishan in 2020 provide a comparative study basically focused on biometric methods and their applications which are used in our daily life. Graph 1 shows a biometric comparison according to Uniqueness, performance, measurement, and useability [30]. Al Rousan and Intrigila introduced a study thorough analysis of the different biometric methods, containing advantages and disadvantages and a comparison of the different biometric methods, and they found that fingerprint and facial recognition have greater precision with lower cost [26]. Alwahaishi and Zdrálek at 2020 introduced a short paper about biometric authentication security and they Concluded that biometric authentication can provide a high degree of security, but they are far from an ideal solution. Moreover, there is no biometric characteristic that satisfies all the needs and requirements in all operational environments, as a result, more than one biometric characteristic of an individual should be used to overcome such problems and to achieve a strict performance guarantee needed by several real-world applications [2]. Sumalatha, Prakasha, Prabhu, And Nayak, introduce a Comprehensive Review of Unimodal and Multimodal Fingerprint Biometric Authentication Systems, they analyze biometric traits used in biometric systems based on the seven properties, the study discloses that while some devices using dynamic biometrics need refinement, most have privacy and security faults. result level fusion is most beneficial for improving the accuracy of biometric authentication. By adding sensors, improving matching algorithms, handling noise errors, and analyzing data the Multimodal biometric frameworks can be improved [39,40]. An inclusive review of biometric authentication published works has been conducted by Alrawili, AlQahtani, Khan, in 2023. They illustrate a Comprehensive Evaluation of Authentication characteristics based on Assessment standards such as Uniqueness, Permanence, Collectability, etc. They list the results of a Comparative Analysis of Biometric Characteristics through Performance Indicators [36,41]. Waqas Safder in 2024 writes in his thesis a comparison of various biometric traits and found that iris, face, and DNA biometrics have high authentication accuracy [42].

Table 9. Comparison of Face, Iris, Hand geometry, Fingerprint, Voice, DNA biometric authenticators using seven categories of evaluation
Hh=High; Mod= Moderate; Lw= Low

Biometric traits	Reference-no.	Universality	Unique-ness	Permanence	Collect-ability	Performance	Accept-ability	Circumvention
Face	[27]	Hh	Lw	Mod	Hh	Lw	Hh	Hh
	[38]	Hh	Lw	Mod	Hh	Lw	Hh	-
	[8]	Hh	Lw	Mod	Hh	Mod	Hh	-
	[30]	Hh	Mod	-	Hh	Mod	Hh	-
	[2]	Hh	Lw	Mod	Hh	Lw	Hh	Hh
	[36]	Hh	Lw	Mod	Hh	Lw	Hh	Mod
	[26]	Hh	Lw	Mod	Hh	Lw	Hh	Hh
	[39]	Hh	Lw	Mod	Hh	Lw	Hh	Hh
Iris	[27]	Hh	Hh	Hh	Mod	Hh	Lw	Lw
	[38]	Hh	Hh	Hh	Mod	Mod	Lw	-
	[8]	Hh	Hh	Hh	Hh	Hh	Mod	-
	[30]	Hh	Hh	Hh	Hh	Hh	Hh	-
	[2]	Hh	Hh	Hh	Mod	Hh	Lw	Lw
	[36]	Hh	Hh	Hh	Mod	Hh	Mod	Lw
	[26]	Hh	Hh	Hh	Mod	Hh	Lw	Lw
	[39]	Hh	Hh	Hh	Mod	Mod	Lw	Lw
Hand geometry	[27]	Mod	Mod	Mod	Hh	Mod	Mod	Mod
	[38]	Mod	Mod	Mod	Hh	Mod	Mod	-
	[8]	Hh	Lw	Hh	Hh	Mod	Hh	-
	[2]	Mod	Mod	Mod	Hh	Mod	Mod	Mod
	[36]	Mod	Mod	Mod	Hh	Mod	Mod	Mod
	[26]	Mod	Mod	Mod	Hh	Mod	Mod	Mod
	[39]	Mod	Mod	Mod	Hh	Mod	Mod	Mod
Fingerprint	[27]	Mod	Hh	Hh	Mod	Hh	Mod	Low

	[38]	Mod	Hh	Hh	Mod	Hh	Mod	-
	[8]	Hh	Hh	Hh	Hh	Mod	Hh	-
	[30]	Hh	Mod	-	Hh	Mod	Hh	-
	[2]	Mod	Hh	Hh	Mod	Hh	Mod	Mod
	[36]	Mod	Hh	Hh	Mod	Hh	Mod	Mod
	[26]	Mod	Hh	Hh	Mod	Hh	Mod	Mod
	[39]	Mod	Hh	Hh	Mod	Hh	Mod	Mod
Voice	[27]	Mod	Lw	Lw	Mod	Lw	Hh	Hh
	[38]	Mod	Lw	Lw	Mod	Lw	Hh	-
	[8]	Hh	Hh	Mod	Hh	Mod	Hh	-
	[30]	Hh	Mod	-	Lw	Mod	Lw	-
	[2]	Mod	Lw	Lw	Mod	Lw	Hh	Hh
	[36]	Mod	Lw	Lw	Hh	Lw	Mod	Mod
	[26]	Mod	Lw	Lw	Mod	Lw	Hh	Hh
	[39]	Mod	Lw	Lw	Mod	Lw	Hh	Hh
	[27]	Mod	Lw	Lw	Mod	Lw	Hh	Hh
	[38]	Mod	Lw	Lw	Mod	Lw	Hh	-
DNA	[27]	Hh	Hh	Hh	Lw	Hh	Lw	Hh
	[38]	Hh	Hh	Hh	Lw	Lw	Lw	-
	[8]	Hh	Hh	Hh	Mod	Hh	Mod	-
	[2]	Hh	Hh	Hh	Lw	Hh	Lw	Lw
	[30]	Hh	Hh	Hh	Lw	Hh	Lw	Lw
	[39]	Hh	Hh	Hh	Lw	Lw	Lw	Lw

Graph1: shows a biometric comparison according to Uniqueness, performance, measurement, and usability [27]



5. Conclusion

To summarize, authentication systems appear simple at first glance. However, they are inherently complex in terms of security, usability, and availability. Because poorly chosen passwords could not adequately protect users, Biometric Authentication systems were introduced in various ways to improve authentication system reliability. This paper introduced an inclusive review of user authentication methods and their estimation, discussion through a literature review. Authentication by all different methods is an important procedure in every information system. Password should be very strong, as long as possible, and with various patterns. Digital certificates can be combined in authentication systems to earn stronger security. Smart cards are utilized jointly with PINs. Limited attempts should be specified for both passwords and PINs. The most secure authentication method is the biometrics. Biometric authentication is a powerful tool for increasing security for systems and individuals. More than one biometric method can be used to provide a highly reliable performance in security. Biometric authentication is a fundamental factor of safety for diverse applications, and fields, and our review has spotlighted the power points, and vulnerabilities of user authentication methods.

6. References

[1] S. Zulkarnain, S. Idrus, E. Cherrier, C. Rosenberger, and J.-J. Schwartzmann, “A Review on Authentication Methods,” 2013. [Online]. Available: https://hal.science/hal-00912435

[2] S. Alwahaishi and J. Zdralek, “Biometric Authentication Security: An Overview,” in Proceedings - 2020 IEEE International Conference on Cloud Computing in Emerging Markets, CCEM 2020, Institute of Electrical and Electronics Engineers Inc., Nov. 2020, pp. 87–91. doi: 10.1109/CCEM50674.2020.00027.

[3] S. Purkayastha, S. Goyal, B. Oluwalade, T. Phillips, H. Wu, and X. Zou, “Usability and Security of Different Authentication Methods for an Electronic Health Records System.”

[4] J. M. Kizza, “Authentication,” in Texts in Computer Science. Springer, Cham., 2024, pp. 215–238. doi: 10.1007/978-3-031-47549-8_10.

[5] V. Zimmermann and N. Gerber, “The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes,” International Journal of Human Computer Studies, vol. 133, pp. 26–44, Jan. 2020, doi: 10.1016/j.ijhcs.2019.08.006.

[6] M. Mehta, H. Baldaniya, and N. Goriya, "A Systematic Review of Authentication Methods for Internet of Things," in 2020 IEEE International Conference for Innovation in Technology, INOCON 2020, Institute of Electrical and Electronics Engineers Inc., Nov. 2020. doi: 10.1109/INOCON50539.2020.9298304.

[7] M. Farik, N. A. Lal, and S. Prasad, "A Review of Authentication Methods," Article in International Journal of Scientific & Technology Research, vol. 5, no. 11, 2016, [Online]. Available: www.ijstr.org

[8] F. Ennaama, K. Benhida, and A. Boulahoual, "COMPARATIVE AND ANALYSIS STUDY OF BIOMETRIC SYSTEMS," Journal of Theoretical and Applied Information Technology, vol. 30, no. 12, 2019, [Online]. Available: www.jatit.org

[9] B. Ogini and N. Oluwole, "A COMPARATIVE STUDY OF SOME BIOMETRIC SECURITY TECHNOLOGIES." [Online]. Available: http://sites.google.com/site/ijcsis/

[10] S. N. Abdulkader, A. Atia, and M.-S. M. Mostafa, "Authentication systems: principles and threats," Computer and Information Science, vol. 8, no. 3, Jul. 2015, doi: 10.5539/cis. v8n3p155.

[11] Manzoor, M. A. Shah, H. A. Khattak, I. U. Din, and M. K. Khan, "Multi-tier authentication schemes for fog computing: Architecture, security perspective, and challenges," International Journal of Communication Systems, vol. 35, no. 12, Aug. 2022, doi: 10.1002/dac.4033.

[12] X. Wang, Z. Yan, R. Zhang, and P. Zhang, "Attacks and defenses in user authentication systems: A survey," Journal of Network and Computer Applications, vol. 188. Academic Press, Aug. 15, 2021. doi: 10.1016/j.jnca.2021.103080.

[13] J. C. Bernal-Romero, J. M. Ramirez-Cortes, J. D. J. Rangel-Magdaleno, P. Gomez-Gil, H. Peregrina-Barreto, and I. Cruz-Vega, "A Review on Protection and Cancelable Techniques in Biometric Systems," IEEE Access, vol. 11. Institute of Electrical and Electronics Engineers Inc., pp. 8531–8568, 2023. doi: 10.1109/ACCESS.2023.3239387.

[14] M. Yıldırım and I. Mackie, "Encouraging users to improve password security and memorability," International Journal of Information Security, vol. 18, no. 6, pp. 741–759, Dec. 2019, doi: 10.1007/s10207-019-00429-y.

[15] A. Sarkar and B. K. Singh, "A review on performance, security and various biometric template protection schemes for biometric authentication systems," Multimedia Tools and Applications, vol. 79, no. 37–38, pp. 27721–27776, Oct. 2020, doi: 10.1007/s11042-020-09197-7.

[16] S. Subangan and V. Senthooran, "Secure Authentication Mechanism for Resistance to Password Attacks," 2019.

[17] A. A. Kaur and K. K. Mustafa, "A Critical appraisal on Password based Authentication," International Journal of Computer Network and Information Security, vol. 11, no. 1, pp. 47–61, Jan. 2019, doi: 10.5815/ijcnis.2019.01.05.

[18] V. Zimmermann, K. Marky, and K. Renaud, "Hybrid Password Meters for More Secure Passwords-A Comprehensive Study of Password Meters including Nudges and Password Information."

[19] Y. Mo, S. Li, Y. Dong, Z. Zhu, and Z. Li, "Password Complexity Prediction Based on RoBERTa Algorithm," Applied Science & Engineering Journal for Advanced Research Peer Reviewed and Refereed Journal ISSN, pp. 1–5, 2024, doi: 10.5281/zenodo.11180356.

[20] H.-T. Pan, H.-W. Yang, and M.-S. Hwang, "An Enhanced Secure Smart Card-based Password Authentication Scheme," International Journal of Network Security, vol. 22, no. 2, p. 358, 2020, doi: 10.6633/IJNS.202003.

[21] L. Chen and K. Zhang, "Privacy-aware smart card based biometric authentication scheme for e-health," Peer-to-Peer Networking and Applications, vol. 14, no. 3, pp. 1353–1365, May 2021, doi: 10.1007/s12083-020-01008-y.

[22] S. Kandar, S. Pal, and B. C. Dhara, "A Biometric based Remote User Authentication Technique Using Smart Card in Multi-Server Environment," Wireless Personal Communications, vol. 120, no. 2, pp. 1003–1026, Sep. 2021, doi: 10.1007/s11277-021-08501-4.

[23] K. Somsuk and M. Thakong, "Authentication system for e-certificate by using RSA's digital signature," Telkomnika (Telecommunication Computing Electronics and Control), vol. 18, no. 6, pp. 2948–2955, Dec. 2020, doi: 10.12928/TELKOMNIKA.v18i6.17278.

[24] B. Liu, L. Xiao, J. Long, M. Tang, and O. Hosam, "Secure Digital Certificate-Based Data Access Control Scheme in Blockchain," IEEE Access, vol. 8, pp. 91751–91760, 2020, doi: 10.1109/ACCESS.2020.2993921.

[25] J. Conners et al., "Let's Authenticate: Automated Certificates for User Authentication," in 29th Annual Network and Distributed System Security Symposium, NDSS 2022, The Internet Society, 2022. doi: 10.14722/ndss.2022.24272.

[26] M. AlRousan and B. Intrigila, "Multi-factor authentication for e-government services using a smartphone application and biometric identity verification," Journal of Computer Science, vol. 16, no. 2, pp. 217–224, 2020, doi: 10.3844/JCSSP.2020.217.224.

[27] S. Parusheva, "A comparative study on the application of biometric technologies for authentication in online banking," 2015. [Online]. Available: https://www.researchgate.net/publication/282653501

[28] B. Ogini and N. Oluwole, "A COMPARATIVE STUDY OF SOME BIOMETRIC SECURITY TECHNOLOGIES," 2013. [Online]. Available: http://sites.google.com/site/ijcsis/

[29] F. Ennaama, K. Benhida, and A. Boulahoual, "COMPARATIVE AND ANALYSIS STUDY OF BIOMETRIC SYSTEMS," Journal of Theoretical and Applied Information Technology, vol. 30, no. 12, 2019, [Online]. Available: www.jatit.org

[30] R. Chauhan and K. Kumar, "A Comparative Study and Analysis on Biometric Authentication," International Journal of Innovative Research in Science, Engineering and Technology, 2020, [Online]. Available: www.ijirset.com

[31] R. M. Ibrahim, M. M. Elkelany, and M. I. El-Afifi, "Trends in Biometric Authentication: A review," 2023. [Online]. Available: https://njccs.journals.ekb.eg

[32] J. Curran and K. Curran, "Biometric Authentication Techniques in Online Learning Environments," in Research Anthology on Developing Effective Online Learning Courses, IGI Global, 2021, pp. 867–879. doi: 10.4018/978-1-7998-8047-9.ch042.

[33] A. Iula, "Biometric recognition through 3D ultrasound hand geometry," Ultrasonics, vol. 111, Mar. 2021, doi: 10.1016/j.ultras.2020.106326.

[34] A. Prasad, "A Comparative Study of Passwordless Authentication," 2024, doi: 10.36227/techrxiv.171560547.71979752/v1.

[35] K. Bibi, S. Naz, and A. Rehman, "Biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities," Multimedia Tools and Applications, vol. 79, no. 1–2, pp. 289–340, Jan. 2020, doi: 10.1007/s11042-019-08022-0.

[36] R. Alrawili, A. Abdullah, S. Alqahtani, and M. Khurram Khan, "Comprehensive Survey: Biometric User Authentication Application, Evaluation, and Discussion," 2023.

[37] S. Parusheva, "A comparative study on the application of biometric technologies for authentication in online banking," 2015. [Online]. Available: https://www.researchgate.net/publication/282653501

[38] S. Dargan and M. Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities," Expert Systems with Applications, vol. 143. Elsevier Ltd, Apr. 01, 2020. doi: 10.1016/j.eswa.2019.113114.

[39] U. Sumalatha, K. K. Prakasha, S. Prabhu, and V. C. Nayak, "A Comprehensive Review of Unimodal and Multimodal Fingerprint Biometric Authentication Systems: Fusion, Attacks, and Template Protection," IEEE Access, vol. 12, pp. 64300–64334, 2024, doi: 10.1109/ACCESS.2024.3395417.

[40] Abdul Aziz Mahdi S., Hamoudi A. A.., and Ali Abbas S.., "A Novel Chaotic System for Color Image Coding", Mustansiriyah. Sci. Edu, Vol. 18, No. 1, pp. 147–162, 2020.

[41] Kazem Hamoud H.., Abdul Latif Abdul Jabbar. H.., Abdul Ali Abdul Kazem A.., and Hassan Hashem. S., "Adaptive Image Denoising Based on MACWM and NLEM Filters", Mustansiriyah.J. Sci.Edu, Vol. 16, No. 1, pp. 53–64, 2020.

[42] W. Safder, "DEGREE PROJECT PASSWORD SECURITY AN ANALYSIS OF AUTHENTICATION METHODS," 2024.