International Journal of Communication Networks and Information Security
ISSN: 2073-607X, 2076-0930
Volume 15 Issue 04 Year 2023

A Survey of Biometric Recognition Systems in E-Business Transactions

Tiyani Christopher Hlongwane*
Department of Information Technology, Tshwane University of Technology, South Africa
tiyanih@yahoo.com
Topside E. Mathonsi
Department of Information Technology, Tshwane University of Technology, South Africa
mathonsite@tut.ac.za
Deon Du Plessis
Department of Information Technology, Tshwane University of Technology, South Africa
duplessisdp@tut.ac.za
Tonderai Muchenje
Department of Information Technology, Tshwane University of Technology, South Africa
muchenjet@tut.ac.za

Article History

Received: 13 December 2023
Revised: 09 January 2024
Accepted: 28 February 2024

Abstract

The global expansion of e-business applications has introduced novel challenges, with an escalating number of security issues linked to online transactions, such as phishing attacks and identity theft. E-business involves conducting buying and selling activities online, facilitated by the Internet. The application of biometrics has been proposed as a solution to mitigate security concerns in e-business transactions. Biometric recognition involves the use of automated techniques to validate an individual's identity based on both physiological and behavioural characteristics. This research focuses specifically on implementing a multimodal biometric recognition system that incorporates face and fingerprint data to enhance the security of e-business transactions. In contrast to unimodal systems relying on a single biometric modality, this approach addresses limitations such as noise, universality, and variations in both interclass and intraclass scenarios. The study emphasizes the advantages of multimodal biometric systems while shedding light on vulnerabilities in biometrics within the e-business context. This in-depth analysis serves as a valuable resource for those exploring the intersection of e-business and biometrics, providing insights into the strengths, challenges, and best practices for stakeholders in this domain. Finally, the paper concludes with a summary and outlines potential avenues for future research.

Keywords: E-business, Phishing, Identity Theft, Biometric, Unimodal, Multimodal, Face, Fingerprint

1. Introduction

E-business is characterized as digitally facilitated business operations, encompassing activities like buying, selling, data sharing, and maintaining business relationships, all conducted through the Internet [1]. This system enables consumers to access both local and global markets from various

geographical locations, eliminating the need for physical store visits and queues. The evolution of the internet has transformed how tasks are performed, encompassing e-business, e-governance, and social interactions, breaking down geographical barriers and expanding the global market. The primary objective of e-business is to enhance business efficiency [1].

However, the increasing reliance on e-business systems raises security concerns during online transactions. Traditional authentication methods involving passwords and usernames have proven inefficient as they are susceptible to theft and forgery. The process of using usernames and passwords for access does not consistently verify the authentic user and is challenging to secure against threats like key-loggers and social engineering [2]. Numerous limitations and security issues, including identity theft, are associated with the conventional identification method of using a combination of usernames and passwords for access [3].

To address these security weaknesses inherent in usernames and passwords for e-business systems, there is a need for an alternative system that incorporates personal recognition technology. This shift is crucial for enhancing security measures and overcoming the limitations of traditional identification methods.

With the surge in fraudulent activities, particularly identity theft targeting banking and login details, there is an imperative need for robust authentication mechanisms. The global embrace of E-business is evident, and numerous studies emphasize the role of biometrics in countering security challenges like identity theft and phishing attacks within E-business transactions [4]. Biometric recognition emerges as a robust solution, effectively tackling diverse issues associated with identity theft and providing elevated levels of security and reliability.

Biometrics can be categorized into two main types: physiological and behavioural characteristics. Physiological characteristics involve identifiable physical traits such as hand geometry, retina, iris, fingerprint, and facial features. On the other hand, behavioural characteristics uniquely identify individuals based on their behaviour, encompassing traits like key-stroke dynamics, voice, and signature. Importantly, these traits cannot be easily stolen or forgotten. Fingerprint, iris, and facial features are recognized as some of the most effective biometric traits due to their simplicity of implementation [1]. Biometrics offer a dependable and robust means of authentication, thereby enhancing accuracy [3].

Unimodal biometric systems, reliant on a single biometric trait for personal recognition and authentication, are contrasted with multimodal biometric systems that employ multiple biometric traits [5]. Although biometrics offer superior recognition accuracy compared to traditional username and password systems, unimodal biometric systems face challenges such as vulnerability to spoofing attacks, non-universality, and susceptibility to noise [3].

Multimodal biometric systems, incorporating various physiological or behavioural traits, play a crucial role in improving personal recognition accuracy within e-business transactions. This strategy enhances universality and reduces susceptibility to spoofing attacks, making it more challenging for impostors to deceive the system by replicating multiple biometric traits [3]. Additionally, the utilization of multiple biometrics helps mitigate susceptibility to artefacts [6]. Various fusion levels, such as feature-level fusion, matching-level fusion, and decision-level fusion, can be strategically employed to effectively combine diverse biometric traits [7].

This study uniquely focuses on harnessing physical attributes, specifically fingerprints and facial features, to fortify e-business security and mitigate the threats of identity theft and spoofing attacks. By incorporating multimodal biometrics, the research aims to enhance the security of data transactions and improve system reliability [6]. The proposed multimodal biometric system, combining facial and fingerprint data, addresses e-business security vulnerabilities through active and real-time authentication processes, offering heightened reliability and performance compared to conventional identification systems. The approach will utilize the OpenCV library in Python for handling images and videos, combining biometric characteristics at the decision-making stage.

The structure of the paper is outlined as follows: Section 2 examines various biometric identifiers and their modes; Section 3 investigates the standard framework of biometric identification systems. Section 4 reviews the obstacles faced in e-commerce, whereas Section 5 addresses the latest advancements in biometric verification for e-commerce. The paper ends with Section 6, offering a recap and pointing out unresolved research questions.

2. Related Works

As security risks increase across various e-business areas, traditional identification approaches show their limitations, especially their vulnerability to spoofing and identity theft. Identity theft happens when someone's personal information is stolen and used without their consent [1]. Enhancing security protocols is necessary to tackle these issues. Recent studies highlight that integrating biometric identification effectively overcomes the drawbacks associated with traditional methods of personal recognition.

2.1 Classification of Biometrics

Biometric authentication leverages unique individual traits for security, protecting against unauthorized access and the misuse of identity through theft, duplication, or sharing [8]. This technique employs an automated process to recognize a person based on distinct physiological and behavioural characteristics [9]. According to the study by Arreymbi and colleagues [10], biometrics involves analyzing physical human attributes such as fingerprints, iris patterns, and facial features, which are crucial for identity verification in e-commerce and aiding law enforcement in identifying criminals. Biometrics involves technology for measuring and analyzing biological information, with traits being non-transferable and non-shareable [11], [12], enhancing the robustness and accuracy of systems built on biometrics [13]. Fingerprint recognition, characterized by automated verification of human fingerprint patterns, is considered highly secure and reliable due to continuous computing advancements [14].

Every person carries unique biometric identifiers, split into physiological and behavioural aspects, as shown in Figure 1. Biometric verification serves as a secure and precise identity verification method for online business dealings, providing protection against the falsification, loss, or theft of identifying traits [3]. Physiological identifiers are based on bodily attributes, including fingerprints, iris patterns, palm prints, and facial recognition. In contrast, behavioural identifiers capture distinct patterns in actions, such as voice, typing behaviour, and handwriting signatures [12].

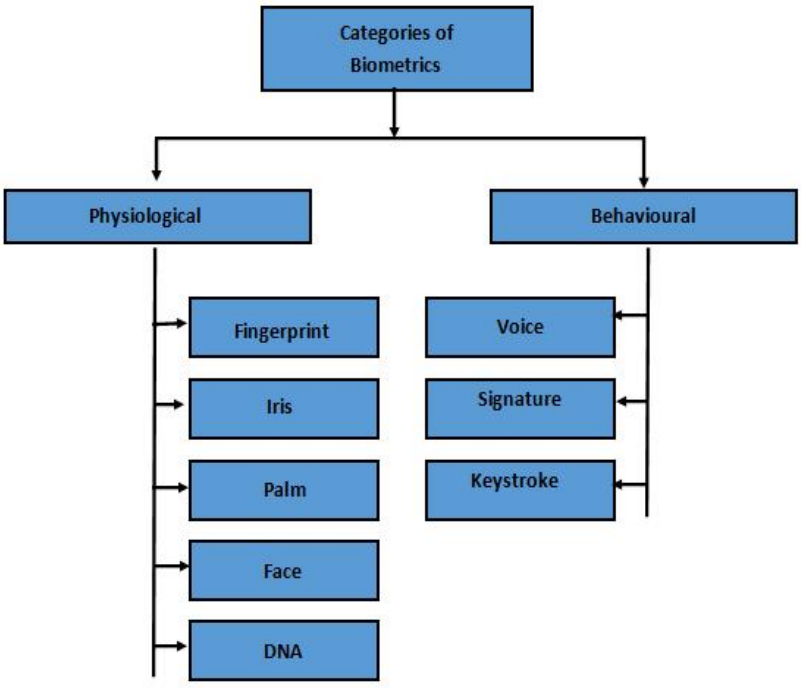


Figure 1. Categories of Biometrics [12]

Attaining perfect accuracy in biometric authentication is an elusive target, highlighting the need for biometric fusion to improve security within e-commerce systems. Various research supports the effectiveness of biometrics as a means for distinct identification, offering a strong system for recognizing individuals [12]. This particular research emphasizes combining fingerprint and face recognition features to create a more secure, multimodal biometric system.

Fingerprint recognition is an automated method for verifying fingerprint pattern matches. A 2002 survey by NTA revealed that a majority of users either recycle passwords or write them down,

posing a threat to system reliability when unauthorized individuals gain access. Fingerprint recognition serves as an effective solution to address issues related to the insecure handling of passwords. Fingerprints, located on the epidermal fingertips, are formed by ridges and valleys, with minutiae referring to the tip and bifurcation of ridges [15], [16].

Fingerprint identification uses two primary methods for capturing prints: live and offline scanning. Offline scanning involves the "ink method," where prints are transferred to paper and then digitized using a scanner. On the other hand, live scanning directly captures fingerprints through electronic scanners [15]. The process of registering fingerprints can utilize either ink-based prints or digital captures [17]. According to scholarly work, fingerprint identification is recognized as an effective means for verifying identity, with Henry's system classifying fingerprints into categories such as whorls, loops, and arches [16].

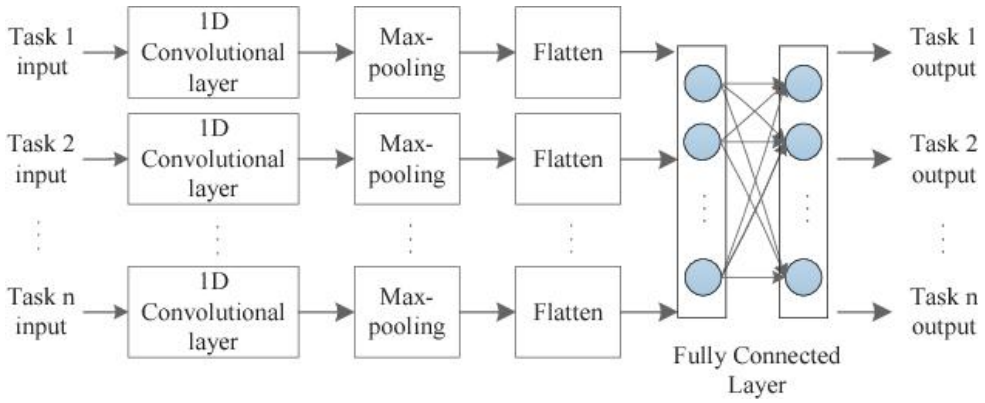


Figure 2. Deep Multi-task Learning Approach of ECG Data

Fingerprint characteristics, known as minutiae, serve as a unique identifier for individuals. The Automated Fingerprint Identification System (AFIS) is the technology framework used for fingerprint-based biometric authentication. This system operates in two phases: enrollment and recognition. During enrollment, biometric samples are captured via an electronic sensor and stored in a database for future reference. In the recognition phase, the system compares new sensor data with the previously stored data to verify the individual's identity. This phase is divided into two processes: identification and verification, each serving a distinct purpose in the authentication process [18].

Fingerprints offer a unique signature for every individual, maintaining their distinctiveness over a person's life. Recognized for its dependability in providing unique identification, fingerprint recognition is utilized across various fields, such as forensic analysis, border security, and financial dealings, encompassing online commerce. It is distinguished as the most extensively researched and developed biometric identification technique [16].

Research differentiates between online and offline methods for capturing images, yet issues like distorted fingerprint minutiae and the risk of duplicating fingerprints lack comprehensive examination regarding their effects on system accuracy and efficiency [15], [18]. Mustafa and colleagues [8] suggest adopting a durable fingerprint scanner designed to accurately read fingerprints even when they are smudged, moist, or damaged.

Barua and colleagues [19] in-depth research highlights the efficiency of online fingerprint recognition for quick individual identification, showcasing its advantages over traditional manual methods. The process of fingerprint recognition is broken down into four key phases: capturing the image, detecting edges, thinning for clarity, extracting features, and then classifying them. For precise identification, the methodology extends across five stages: capturing the image, enhancing it, converting it to binary for analysis, further thinning, and finally extracting distinctive features [16]. The study notably praises the Otsu algorithm's effectiveness in extracting fingerprint details following image capture. Online methods of image acquisition offer solutions to the limitations inherent in the conventional ink-based capture technique, such as issues in digitizing prints [4]. Fingerprint identification is lauded for its rapidity and robust security, attributed to the unique and unalterable nature of fingerprint patterns [19], [14].

In the process of collecting fingerprint images, subpar image quality can lead to the need for enhancement techniques to clarify unclear ridge patterns. Methods like the Discrete Fourier

Transform and Histogram Equalization are utilized during the enhancement phase to improve the quality of the initial images, facilitating the subsequent extraction of fingerprint images [16].

For more than a hundred years, fingerprints have been a dependable method of identification. This research emphasizes the difficulties faced by traditional manual fingerprint identification methods, including their expensive and labour-intensive aspects. Meanwhile, automated digital fingerprint recognition systems have gained popularity across multiple sectors, such as banking, online commerce, and facility access management.

The study systematically classifies fingerprint matching or recognition techniques into image-based and minutiae-based approaches. Techniques based on image analysis compare features across the entire fingerprint, whereas minutiae-focused methods concentrate on specific local details, like the ending points of ridges and points where they split. Despite the availability of both approaches, the literature indicates a prevalent usage of the minutiae-based technique in existing fingerprint recognition systems [14]. Fingerprint identification, recognized as a highly reliable method for authenticating individuals, is predominantly based on the minutiae features. While acknowledged as the most successful identification method, there is a notable gap in information regarding the effective handling of degraded and corrupted fingerprints [4].

The fingerprint recognition system stands as a mature technology with widespread applications across various societal domains to bolster security. The uniqueness of human fingerprints, with a probability of only 1 in 19*10^15 for two fingerprints being identical, sets it apart from other biometric identification methods such as keystroke dynamics, voice recognition, and facial recognition. Fingerprint features remain consistent over time and undergo minimal changes, ensuring a reliable and consistent means of identification [16], [20].

The extraction of fingerprints has been successfully implemented using the Python OpenCV library and the Otsu algorithm, known for its efficacy in digital image processing. The algorithm's robust calculations, which are resistant to blurriness and contrast variations in the image, have been validated through experiments on fingerprint identification using OpenCV and the Otsu algorithm [20]. Nevertheless, the study recommends the incorporation of image enhancement techniques, specifically Discrete Fourier Transform and Histogram Equalization, during the fingerprint recognition process. Histogram Equalization is used to improve local contrast in areas with lower visibility without altering the overall contrast significantly. Furthermore, the research recommends employing the Virtual C++ Program to perform minutiae extraction via the OpenCV Library [16].

The fingerprint capture process entails using a scanner to obtain the print and transforming it into a digital format for database storage. To refine the digital image and reduce noise, various strategies, such as Gabor filters, are employed. For fingerprint verification, the system performs a one-to-many match, comparing the new fingerprint against a database of stored prints. This research describes three primary matching methods: analysis based on minutiae, correlation, and measurement of Euclidean distances, highlighting the latter for its rapid processing capabilities. It advocates for the use of minutiae-focused identification methods, especially when employing the National Institutes of Standards and Technology (NIST) database for enhanced accuracy [21].

Facial recognition technology accurately identifies people by analyzing unique facial characteristics [22]. It's applied across numerous sectors, including finance, online commerce, border security, and monitoring. Jain and colleagues [22] assessed the effectiveness of a facial recognition system using a sample of 300 images featuring varied expressions. The study pinpointed several elements affecting recognition accuracy, such as expressions, lighting, and the angle of the face. Figure 3 demonstrates that developing a dependable facial recognition framework involves critical phases like detecting the face, extracting key features, and then recognizing the face.

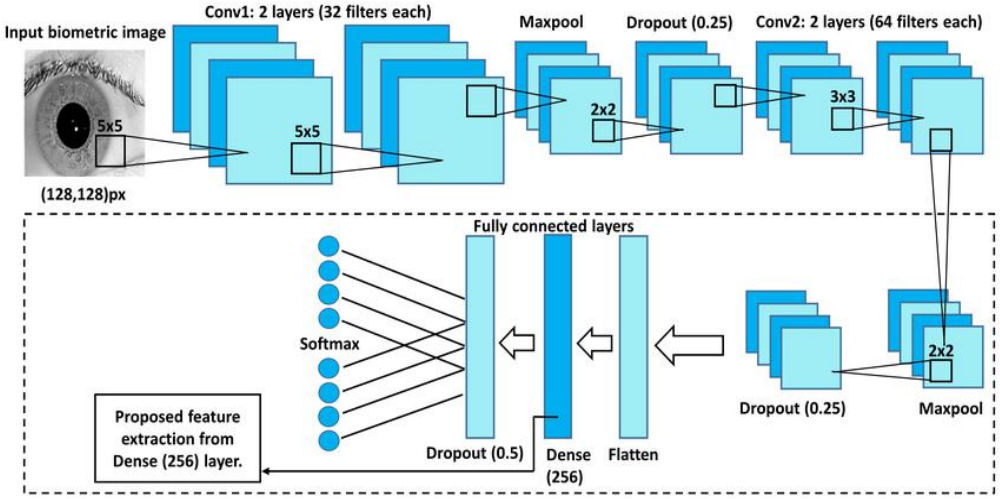


Figure 3. Biometrics Feature Detection and Recognition Flowchart [22]

The Viola-Jones method, integrated within OpenCV for facial detection as introduced by Ismael and Irina [23], is pivotal for biometric face identification. This research highlights face detection as the foundational step for a dependable facial recognition system, followed by critical decision processes based on facial image comparisons with a database. For genuine facial recognition, the registration phase is essential to capture and store unique facial details in the database [24]. To address obscured facial features, Vadlapati and co-authors [25] developed a facial recognition solution employing the Python Image Library (PIL), a freely available tool for image processing.

The study recommends the use of the Haar classifier, which is applicable to various objects, for detecting facial features within an image. The OpenCV library, in conjunction with the AdaBoost algorithm for facial detection in images or videos, has been proposed for real-time image processing. The AdaBoost algorithm, introduced in the mid-90s, follows distinct steps for authentic facial recognition: face detection to identify unique facial features, feature extraction to extract and store these features in a database, and template matching to compare the presented information at the login state with that stored in the database [24].

Facial recognition approaches include the holistic approach, which involves using the entire set of facial features, and the feature-based approach, which focuses on specific facial features like eyes, nose, mouth, and chin [25].

Employing Matrix Laboratory (MATLAB) for face recognition has been noted to demand significant computing power, unlike the OpenCV library, which functions efficiently on limited resources [26]. The Viola-Jones algorithm stands out in real-time facial identification tasks for its low CPU resource consumption, making it a preferred choice for efficient processing [24]. Notably, achieving accurate identification in under 30 seconds is emphasized as a noteworthy feature [27]. In scenarios where certain facial features are obstructed, the use of OpenCV and PIL for facial recognition is suggested. Experimentation in this study yielded an 80% accuracy rate, acknowledging challenges such as illumination and image noise, which led to some images being incorrectly recognized [25].

Table 1 below presents a detailed comparative analysis of OpenCV and MATLAB in terms of their operational capabilities.

Table 1. MATLAB and OpenCV Comparison [26], [27]

Category	MATLAB	OpenCV
Cost	Licensed software and costly	Free and open source
Processing speed	It takes a lot of time to process	Faster
Memory consumption	It consumes a huge memory	Less memory consumption
Code Simplicity	Easy to understand	Complex to understand

A thorough examination of existing literature reveals substantial research focused on improving security and user-friendliness in e-business transactions through facial and fingerprint recognition and authentication. However, despite this extensive research, the study does not present an efficient algorithm to counter identity theft attacks during these transactions. In response to security concerns, particularly identity theft and phishing attacks in e-business, this paper introduces an advanced multimodal biometric system utilizing facial and fingerprint recognition. The suggested system utilizes the open-source Python library, OpenCV, as an approach to tackle the security challenges linked with e-business transactions.

2.2 Biometric Modalities

Biometric systems are categorized into unimodal and multimodal types based on the number of biometric characteristics they incorporate.

2.2.1 The Unimodal Biometric Recognition System

Unimodal biometric systems identify individuals using a single type of biometric characteristics, such as fingerprints, facial features, iris patterns, or voice recognition. These systems rely exclusively on one attribute for identification purposes [8], [5], [13]. Their simplicity and cost-effectiveness make them particularly suitable for e-business applications [28].

However, an in-depth literature review has revealed limitations in unimodal biometric systems. These systems demonstrate lower reliability compared to multimodal counterparts concerning recognition accuracy, encountering challenges like noise, spoofing, universality, interclass variation, and similarities [29], [12]. To address these challenges, there is an acknowledged need to incorporate an increased number of biometric modalities [30]. Relying solely on a single biometric trait often falls short of achieving the required accuracy in real-world scenarios [31]. The issues associated with unimodal biometrics can be effectively addressed through the adoption of multimodal biometric systems [5]. Considering the highlighted challenges in unimodal biometrics, it is evident that proposing the utilization of multiple biometric modalities leads to the emergence of multimodal biometrics.

2.2.2 The Multimodal Biometric Recognition System

The application of biometrics has experienced substantial growth in security measures over the past decade. Numerous studies in the literature have raised inquiries regarding the potential enhancement of recognition performance through multimodal biometrics. Establishing a reliable recognition system is critical across various domains, including access control, commercial industries, and forensics.

Unimodal biometric systems, which depend on just one biometric characteristic for identification, encounter problems like vulnerability to spoofing, changes in pose and lighting, and limited applicability across populations. As a solution, multimodal biometric systems are gaining traction [33]. These systems use multiple biometric inputs to verify identity, offering enhanced security through layered authentication [30], [32].

Referred to as a fusion of biometric identifiers, multimodal biometric systems integrate multiple biometric modalities to enhance individual identification processes [7], [33]. This approach effectively addresses the limitations faced by unimodal biometric systems [34] by broadening the range and depth of biometric data used [12]. The integration of various biometric identifiers not only augments the overall system accuracy, security, and reliability but also significantly mitigates recognition error rates [31]. Multimodal biometric systems excel over unimodal systems by providing a fail-safe mechanism—should one identifier prove inadequate, another can compensate, ensuring robust authentication. These systems are increasingly employed across a spectrum of applications, including human-computer interaction, border security, locating missing individuals, banking, and e-commerce [8], [31].

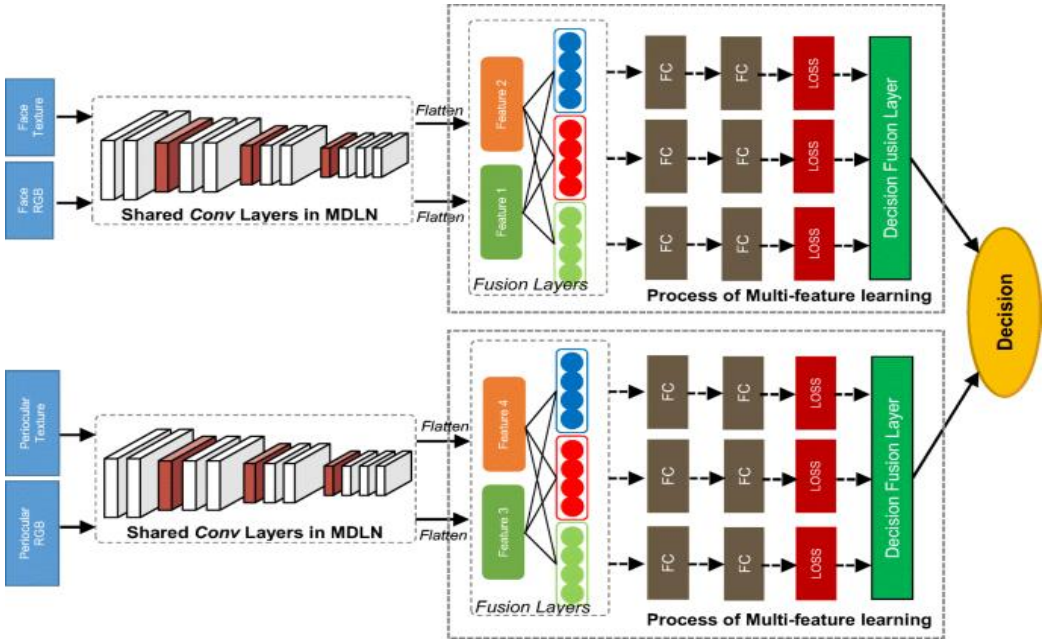


Figure 4. Implementation of Multi-model Biometric Recognition

The proposal advocates for the adoption of the BioDater Security Module (BDSM), which strengthens security through a dual-layer biometric framework that integrates both biometric information and time-stamping, providing an additional security dimension [10]. The proposed multimodal recognition framework offers five key benefits: improved security measures, heightened accuracy, wide applicability, cost efficiency, and the capability to detect live subjects [12].

Integrating a multimodal biometric framework significantly raises the barrier to unauthorized access by requiring the spoofing of several biometric indicators at once, thereby enhancing the system's accuracy and security [28]. This approach demonstrates the advantage of employing multiple biometric characteristics, which complicates efforts by impostors to deceive the system. Research by Hezil and Boukrouche [33] advocates for combining ear and palmprint biometrics, noting the distinctiveness of the human palm with its unique patterns of lines, ridges, and wrinkles, which make up the hand's inner surface.

In the context of multimodal biometric identification, different levels of integration are employed, such as fusion at the feature, matching, and decision stages [7]. It is expected that fusion at the feature stage will surpass the performance of decision-level fusion, as the latter might not utilize the entire range of information available [7], [35]. The aim of fusing multimodal biometric data is to merge the results from different biometric inputs, enhancing the overall reliability of the system [29].

Considerations outlined in studies emphasize factors such as the choice of biometric traits, the number of biometric traits, and the type of fusion level when designing and implementing multimodal biometric systems [17]. Several factors need to be considered in the design of multimodal recognition systems [7], including the following:

a) Choosing the types and number of biometric characteristics. b) Determining the integration stage for biometric data.

c) The approach for combining the data.

d) Assessment of matching efficacy and related expenses.

Research indicates an active investigation into the most effective strategies for combining multiple biometric indicators for enhanced recognition. Two main fusion strategies for multimodal biometric systems have been distinguished [34] [5]:

a) Pre-match fusion, including sensor and feature level methods, is critical for amalgamating various biometric characteristics or modalities before the matching process begins. This form of integration is utilized during both the enrollment and verification stages.

b) Post-match fusion - In this approach, the compiled matching scores provide a detailed dataset. Due to its adaptability, which facilitates the merging of scores from diverse modalities, many scholars advocate for post-match fusion. This fusion method is particularly relevant during the verification phase.

The three tiers of multimodal fusion identified are sensor level, feature level, and matching score level fusion. Sensor-level fusion merges biometric data collected from various sensors. Feature-level fusion amalgamates unique attributes, such as fingerprints and facial features. Matching score level fusion takes place after the biometric characteristics have been matched against templates in the database.

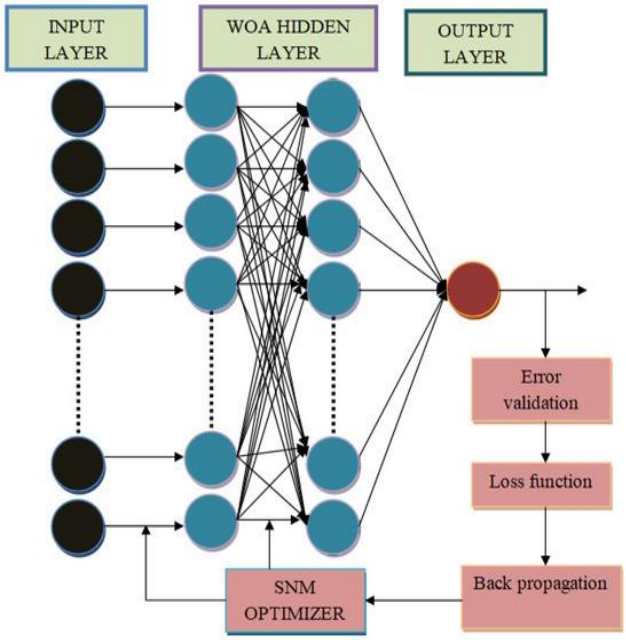


Figure 5. Decision Level Fusion Biometric System

Figure 5 depicts the different stages of integration, such as fusion at the feature level, matching score level, and decision level. Fusion at the feature level is highlighted as the most effective due to its high precision in collecting biometric data directly from the sensor, surpassing the performance of decision level and matching score-level fusions. At the matching score level, score normalization from various modalities is conducted. Methods like Linear Discriminant Analysis (LDA), the Bayes decision rule, and K-Nearest Neighbor (K-NN) are utilized to merge match scores.

The research introduces novel approaches for combining biometric characteristics and making decisions. For example, employing the Adaptive Neuro Fuzzy Interface System (ANFIS) for integrating facial and vocal biometrics is recommended. Additionally, a method combining facial and palmprint features using Gabor filters for feature extraction, followed by Principal Components Analysis (PCA) and Linear Discriminant Analysis (LDA) for reducing dimensions, is suggested. This technique undergoes evaluation on recognized datasets, such as the PolyU palmprint and the Olivetti Research Library databases. Further investigations delve into the enhancement of facial recognition through biometric integration, applying PCA for algorithmic analysis, Support Vector Machine (SVM) for classifying data, and estimating the interrelations among variables. This method, achieving a mean accuracy rate of 85.24%, is validated across six distinct database samples. Other research highlights the amalgamation of fingerprint and iris recognition technologies, leveraging the

Gray-Level Co-occurrence Matrix (GLCM) and K-Nearest Neighbor (KNN) for the extraction of features. The fingerprint is widely used as a physiological trait, while the iris is considered the most reliable trait due to its stability throughout an individual's lifetime. Biometric data fusion involves combining measured biometric data from different modalities with a minimum accuracy score required for positive recognition. Experimentation is conducted using the CASIA-Iris and FVC 2004 Fingerprint online public databases [8].

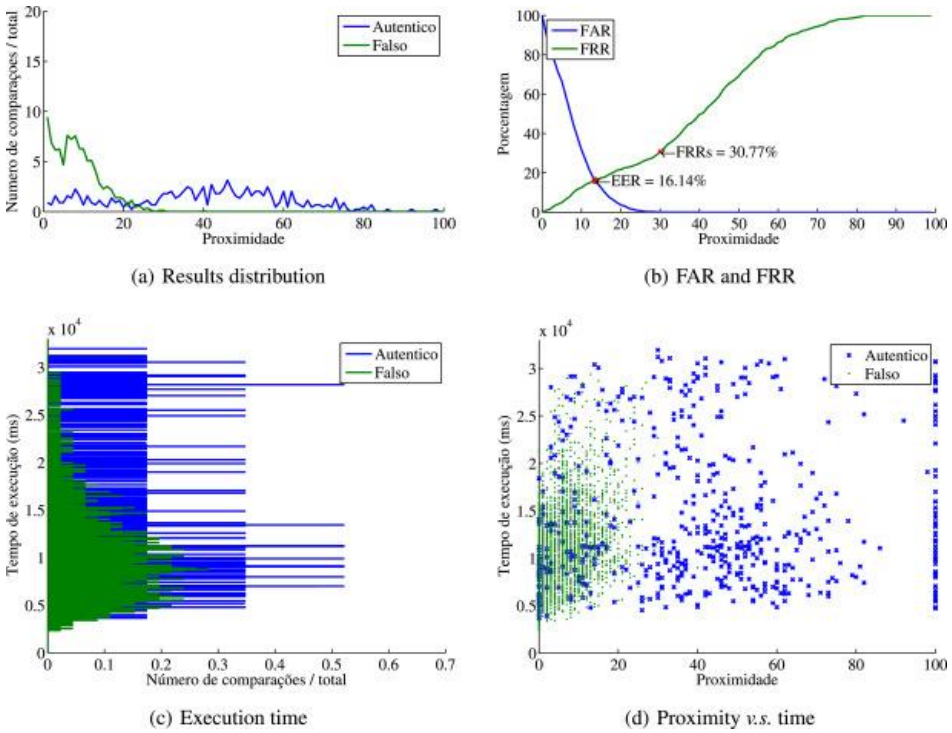
The proposal to integrate facial recognition and fingerprint biometric systems aims to overcome limitations associated with unimodal recognition, such as susceptibility to spoofing attacks. The precision of facial recognition is influenced by variables such as changes in pose, expressions, and lighting conditions. Similarly, fingerprint identification may be compromised through the creation of fake fingerprints from materials like rubber. Multimodal biometrics are suggested to enhance and increase accuracy rates to address challenges in unimodal systems. Experimental results from this study demonstrate that multimodal biometrics outperform unimodal systems [29].

Multimodal biometric recognition provides solutions to limitations observed in unimodal systems, including susceptibility to spoofing attacks and noisy data. This approach is applicable across multiple fields, including financial security, credit card operations, and online commerce. The research delineates two key stages for multimodal biometric systems: registration and verification. In the registration phase, the biometric characteristics of an individual are recorded and preserved in a database for future verification use. The verification stage entails comparing the biometric data obtained from an individual to the database entries in a one-to-many matching scenario [30].

Impostors find it challenging to spoof multiple biometric traits simultaneously. Integrating biometric information fusion at an early stage is shown to yield superior results. Feature-based level fusion is highlighted for producing better recognition outcomes, albeit with the challenge of combining incompatible data types [31].

The study conducted by Kumar and Farik [32] explores Krawczyk's proposed multimodal biometric recognition system designed to secure personal medical records. This framework promotes the amalgamation of biometric information from various attributes, enhancing its security, efficiency, and resistance to tampering. Several pieces of research highlight that integrating biometrics at the feature level leads to optimal outcomes, with precision levels reaching as high as 95%.

Figure 6 illustrates biometric accuracy rates obtained from various algorithms and modalities. The research by Vadlapati and colleagues [25] utilized OpenCV and PIL for identifying faces, whereas Jamdar and Boke [9] applied PCA and SVM techniques for facial recognition tasks.



(a) Results distribution (b) FAR and FRR

(c) Execution time (d) Proximity *v.s.* time

Figure 6. Biometric Accuracy Rate Comparison

The proposal to use the Open-Source Biometric Recognition (OpenBR) for still-image face recognition is made [36]. OpenBR provides functionalities like training models, assessing algorithms, performing cross-validation, and managing galleries, which improve algorithmic performance, evaluate recognition capabilities, and ease system integrations. Developed in C++, it is compatible with operating systems such as Windows, Linux, and macOS.

Although multimodal biometrics can achieve notable accuracy levels, it introduces complexities in both design and execution [32]. Siddiqui and colleagues [29] recommend a tiered structure that includes phases for enrollment, verification, and identification. Kumar and Farik [32] describe three operational stages for single-mode biometric systems: the enrollment stage, the verification stage, and the identification stage.

a) Enrollment stage - This initial phase involves recording an individual's biometric details in the system and utilizing scans and cameras to collect biometric data.

b) Verification and identification stages - These stages are sometimes used synonymously in academic discussions. The identification stage facilitates a one-to-many comparison, matching a newly captured image against existing ones in the database to assess similarity.

3. Typical Architecture of the Biometric Recognition System in E-Business

For an individual to be verified and gain access within a system, their biometric identification and authentication processes are essential. Biometric authentication technologies are applied across various sectors, including online commerce and finance. Utilizing biometric integration or multimodal biometrics, which combines multiple biometric identifiers, is deemed to offer enhanced security over single-mode (unimodal) systems that depend on just one biometric characteristic. This segment sheds light on the structure of biometric security systems [32]. In such a system, the key stages for carrying out e-commerce transactions involve the enrollment and authentication of biometric data [21].

The architecture of a biometric system is organized into four key stages: the enrollment stage, the processing stage, the feature comparison stage, and the decision stage. Some of these stages are integral to the operation of an e-commerce transaction system. The architecture is further broken down into the enrollment, verification, and identification stages as critical components of the system's framework [5], [6], [32]. The process flow for an e-commerce transaction is illustrated in Figure 7, which is divided into the mentioned phases:

a) Enrollment stage - involves collecting biometric information and converting it to a digital form.

b) Processing stage - employs algorithms to refine the image, identify unique characteristics, generate a biometric template, and save it in the biometric database for subsequent access. All personal biometric details are preserved in this database.

c) Feature comparison stage - engages in the algorithmic comparison of the captured biometric trait with the information held in the biometric database.

d) Decision phase - is responsible for the final determination of the system, drawing on the outcomes of the comparison stage.

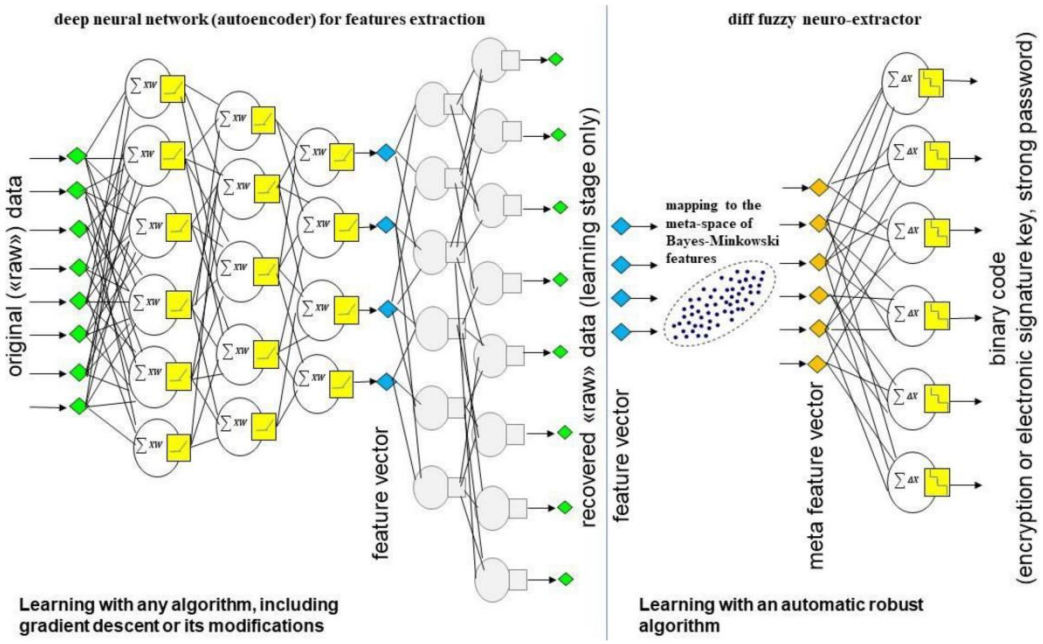


Figure 7. E-Business Transaction Flow Chart

Before users can engage in e-business transactions, several fundamental steps are required, with the enrollment phase being particularly crucial for acquiring personal biometric information from consumers. New users are allowed to enrol their biometric information, which is then stored in the database for future use. Existing users can present their biometric features on the system's scanner to log in. The biometric image is detected, unique features are extracted, and these are matched with the image template in the database. If the template matches, the user proceeds with the transaction; otherwise, access is denied, and the user is logged out. Figure 4 illustrates that only users with authentic biometric traits are granted access, enhancing recognition accuracy in e-business transactions.

Within the infrastructure of an e-commerce transaction system, four components function behind the scenes [30]:

a) Sensor component – This component is responsible for capturing biometric characteristics and converting them into digital images or data, which are then forwarded to the feature extraction component.

b) Feature extraction component – Here, unique biometric features are isolated from the data collected by the sensor component.

c) Comparison component – In this part, the features that have been isolated are evaluated against the biometric information stored in the database.

d) Decision component – Based on the outcomes from the comparison component, this section makes the final decision, either approving or denying the results.

3.1 Overview of the Biometrics Challenges in E-Business

Identity theft and phishing are considerable obstacles to the security of online businesses [10]. Lokhande, in 2013, pointed out the e-commerce sector's awareness of potential cyber threats [37]. In the 1800s, Alphonse Bertillon introduced the Bertillonage System for identifying individuals biometrically, which was eventually abandoned due to its unreliability and the absence of universal standards. Despite its utility in sectors like corporate security, financial services, border management, and criminal justice, biometric technology encounters ethical and legal concerns. Nonetheless, Erickson's research suggested that the advantages of biometric systems surpass the issues related to privacy and security. In the context of e-commerce, the safeguarding of biometric information remains a paramount concern, given the risk of database breaches leading to the misuse of sensitive data [10].

Users of online business platforms are susceptible to various malicious activities, including spyware and phishing, with spoofing attacks being a notable method for unauthorized access to systems. Studies have shown that traditional methods of authentication, such as usernames and passwords, are vulnerable to breaches [10]. Biometric authentication systems are recognized for their enhanced security reliability. With the increasing frequency of cyber-attacks targeting online business platforms, the protection of user data and assets is of paramount importance. The role of trust and security is crucial for the success of online businesses [38]. The conventional method of using usernames and Personal Identification Numbers (PINs) is found to be insufficient in addressing the security challenges posed by cybercrime. Integrating biometrics into e-business, however, may face challenges, as consumers might be uncomfortable with the traditional authentication processes, and issues related to hardware and software compatibility could hinder access to e-business sites [37].

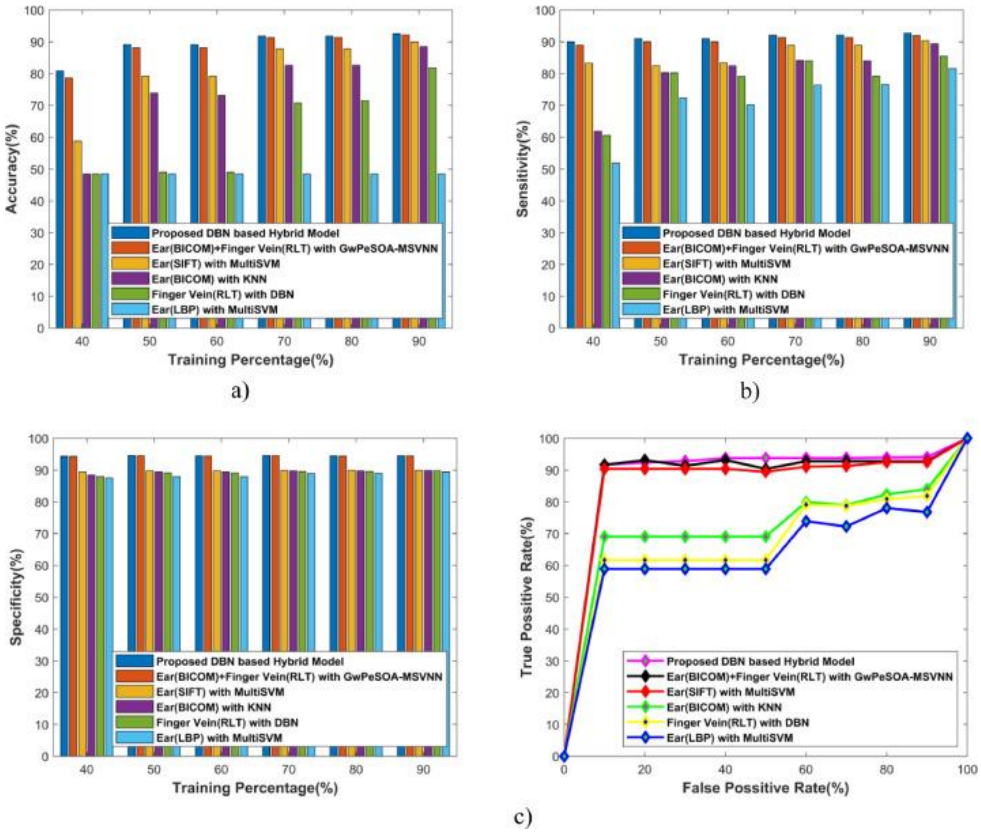


Figure 8. Deep Belief Network-based Hybrid Model for Biometric System

As security challenges in e-business increase, maintaining customer trust becomes challenging for businesses and other stakeholders. Numerous online business stakeholders are exploring biometric solutions as a means to counteract cybercrime. Biometric systems for identification and authentication play a key role in maintaining and enhancing customer trust.

In the course of online business dealings, individuals disclose confidential information, such as biometric identifiers, home addresses, credit card details, and financial data, which are then digitally collected and stored. The adoption of biometric technology in online business settings presents challenges concerning user consent, as some individuals may be apprehensive about sharing their personal details for verification purposes [1]. Security remains a pivotal concern in online commerce, and neglecting to adequately address these worries could result in consumer apprehension and reluctance to engage with online business platforms [38].

Biometric data, if stolen or intercepted, can be misused, necessitating methods for cancelling illegally captured biometric features. Four outlined methods for cancelling biometric features include biometric salting, bio-key generation, fuzzy scheme, and non-invertible transform [10].

Security in e-business is often characterized by three key aspects: confidentiality, integrity, and availability. Confidentiality ensures that data access is restricted to authorized users, integrity

guarantees the honesty and authenticity of data, and availability ensures that data is accessible when needed [38].

E-business systems face vulnerabilities to various attacks, including Denial of Service (DoS) and man-in-the-middle attacks. The e-business ecosystem involves multiple stakeholders, such as consumers, merchants, and third-party software vendors responsible for hosting merchant websites or applications [37].

Software defects contribute to security vulnerabilities in e-business systems, often stemming from inadequate System Development Life Cycle (SDLC) practices. Network sniffing represents a security risk in online business environments, enabling attackers to intercept sensitive information such as credit card details and login information during transmission from the user's computer to the server [38].

Pharming and malware pose significant threats to the security of online businesses. Pharming exploits the Domain Name System (DNS), manipulating the process of domain name resolution to divert users from authentic websites to fraudulent or duplicate ones [37]. Malware, on the other hand, is a software program designed to disrupt operations and gain unauthorized access to systems. Threats in e-business include imposters mimicking legitimate websites to obtain sensitive consumer data [38].

The theft of biometric information is a major hurdle to the widespread acceptance and success of online business activities [10]. The threat of identity theft significantly impacts consumer confidence and behaviour towards e-commerce, resulting in substantial financial losses for retailers in the realm of billions of dollars due to concerns about identity fraud. Establishing and sustaining trust among consumers is a significant challenge in the absence of a robust security framework for e-commerce systems [1]. Attacks on consumers' sensitive data in e-business have a profound impact on trust and faith in the system, with victims of identity theft spending substantial amounts annually to compensate for the effects of data breaches [37].

The research conducted by Tajpour and colleagues [1] outlines identity theft in two phases: initially, the acquisition or fabrication of a false identity occurs, followed by the illicit utilization of this counterfeit identity to unlawfully penetrate e-business platforms and engage in criminal activities. Challenges pertaining to the precision of biometric identification systems are recognized, highlighting elements that influence the accuracy of these systems. Such elements encompass variations in pose, expressions, and lighting conditions, which may lead to errors in authentication [25].

3.2 Biometrics Performance Measures

Different criteria are used to evaluate the performance of biometric systems [21].

a) False Rejection Rate (FRR): This metric is observed when the variation between classes is significant. It describes instances where the biometric information obtained during the authentication stage fails to correspond with the template data collected during the enrollment of an individual.

b) False Acceptance Rate (FAR): This metric emerges when the similarities between classes become pronounced. It pertains to the instances where the characteristic features of different individuals overlap.

FRR and FAR constitute the primary errors in biometric identification systems. FAR is noted when the system mistakenly confirms a match for an individual, whereas FRR occurs when a legitimate user is incorrectly denied access by the system.

4. State-of-the-Art Biometric Recognition in E-Business

This paper suggests a solution to address challenges in e-business through a proposed multimodal recognition system comprising four key steps. Initially, biometric traits are captured, and then, in step 2, unique features are extracted from these traits. Step 3 involves matching these features with those stored in a database during enrollment, and the final step (step 4) entails decision-making based on the matching score, determining access permission or denial. Notably, biometric fusion is executed at the decision level due to compatibility challenges in steps 2 and 3. The proposed algorithm, implemented using the Python OpenCV library, captures fingerprints and

face features for storage in the database. Feature fusion at the decision level aims to enhance system performance and eliminate flaws.

5. Conclusion and Open Research Issues

This article conducts an in-depth analysis of various research efforts within the fields of online commerce and biometric authentication, offering insights and methodologies to improve the security of online transactions. The use of biometric identification is widespread across numerous industries, including finance, facility access management, and digital commerce. Despite facing security hurdles, digital commerce has achieved global prominence, revolutionizing how businesses operate. This detailed review is intended to act as a valuable reference for newcomers to the field and the general audience interested in biometrics and digital commerce. Moving forward, it is recommended that scholars explore the adoption of multi-biometric systems to tackle the security challenges in digital commerce, thereby increasing the reliability and accuracy of authentication processes. Additionally, future research should focus on addressing ethical and legal concerns related to biometric data usage, ensuring compliance with ethical standards and legal regulations. Tackling issues such as e-business standards and interoperability is crucial for the widespread adoption of biometrics in e-business.

6. Acknowledgements

The authors extend their appreciation to Tshwane University of Technology for their essential support. They confirm that there are no conflicts of interest regarding the publication of this article.

References

[1] A. Tajpour, S. Ibrahim, and M. Zamani, "E-commerce and identity theft issues," *International Journal of Advancements in Computing Technology,* vol. 5, no. 14, p. 105, 2013.

[2] A. Gokhale and V. Waghmare, "A Study of Various Passwords Authentication Techniques," *International Journal of Computer Applications,* vol. 975, p. 8887, 2014.

[3] K. Mohamed Basheer and K. Haulath, "Multimodal Biometrics: An Enhanced Authentication," *International Journal of Computer Applications,* vol. 181, no. 16, p. 8887, 2018.

[4] V. Dhir, A. Acet, R. Kumar, and G. Singh, "Biometric recognition: A modern era for security," *International Journal of Engineering Science and Technology,* vol. 2, no. 8, pp. 3364-3380, 2010.

[5] R. Devi and P. Sujatha, "A study on biometric and multimodal biometric system modules, applications, techniques and challenges," in *2017 Conference on Emerging Devices and Smart Systems (ICEDSS)*, IEEE, 2017, pp. 267-271.

[6] A. Kumar, K. Patidar, and M. K. Yadav, "Multimodal Biometric System in Secure e-Transaction in Smart Phone," *International Journal of Computer Science and Information Technologies*, vol. 6, no. 6, pp. 5080-5084, 2015.

[7] A. Ross and A. K. Jain, "Multimodal biometrics: An overview," in *2004 12th European signal processing conference*, IEEE, 2004, pp. 1221-1224.

[8] A. S. Mustafa, A. J. Abdulelah, and A. K. Ahmed, "Multimodal biometric system iris and fingerprint recognition based on fusion technique," *International Journal of Advanced Science and Technology,* vol. 29, no. 3, pp. 7423-7432, 2020.

[9] C. Jamdar and A. Boke, "Multimodal biometric identification system using fusion level of matching score level in single modal to multimodal biometric system," in *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, IEEE, pp. 2277-2280, 2017.

[10] J. Arreymbi, V. Odiah, A. Ijeh, and A. A. Babatunde, "Using biometrics to improve internet e-business security: A new approach," in *ICIT 2011 The 5th International Conference on Information Technology*, 2011.

[11] M. Ghayoumi, "A review of multimodal biometric systems: Fusion methods and their applications," in *2015 IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS)*, IEEE, Jun. 2015, pp. 131-136.

[12] S. Barde, "A multimodal biometric system-aadhar card," *i-manager's Journal on Image Processing*, vol. 5, no. 2, p. 1, 2018.
[13] G. Iwasokun, S. Udoh, and O. Akinyokun, "Multimodal Biometrics: Applications, Strategies and Operations," *Global Journal of Computer Science and Technology,* vol. 15, no. 2, pp. 15-28, 2015.
[14] A. Tukur, "Fingerprint recognition and matching using Matlab," *The International Journal of Engineering and Science (IJES)*, vol. 4, no. 12, pp. 01-06, 2015.
[15] D. Nath, S. Ray, and S. K. Ghosh, "Fingerprint recognition system: design & analysis," in *conference international conference on scientific paradigm shift in information technology & management, SPSITM*, 2011.
[16] P. Bhowmik, K. Bhowmik, M. N. Azam, and M. W. Rony, "Fingerprint Image Enhancement And It" s Feature Extraction For Recognition," *International Journal Of Scientific & Technology Research,* vol. 1, no. 5, pp. 117-121, 2012.
[17] S. Kumar, S. Paul, and D. K. Shaw, "Real-Time Multimodal Biometric User Authentication for Web Application Access in Wireless LAN," *J. Comput. Sci.,* vol. 13, no. 12, pp. 680-693, 2017.
[18] V. Manju, "Fingerprint Recognition and its Advanced," *International Journal of Engineering Research & Technology (IJERT)*, vol. 9, no. 4, 2020.
[19] K. Barua, S. Bhattacharya, and K. Mali, "Fingerprint identification," *Global Journal of Computer Science and Technology,* vol. 11, no. 6, pp. 60-64, 2011.
[20] Y. Yaru and Z. Jialin, "Algorithm of fingerprint extraction and implementation based on OpenCV," in *2017 2nd International Conference on Image, Vision and Computing (ICIVC)*, IEEE, pp. 163-167, 2017.
[21] G. Kanimozhi and T. Chakravarthy, "Secure Biometric Authentication System Architecture Using Fingerprint Using FAR," *International Journal of Engineering Research & Technology (IJERT)*, vol. 2, no. 2, pp. 1-6, 2013.
[22] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on circuits and systems for video technology,* vol. 14, no. 1, pp. 4-20, 2004.
[23] M. S. Velmurugan, "Security and Trust in e-Business: Problems and Prospects," *International journal of electronic business management*, vol. 7, no. 3, 2009.
[24] P. Kumbhar, M. Attaullah, S. Dhere, and S. Hipparagi, "Real time face detection and tracking using OpenCV," *International journal for research in emerging science and technology,* vol. 4, no. 4, 2017.
[25] J. Vadlapati, S. S. Velan, and E. Varghese, "Facial Recognition using the OpenCV Libraries of Python for the Pictures of Human Faces Wearing Face Masks during the COVID-19 Pandemic," in *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, IEEE, 2021, pp. 1-5.
[26] K. Teoh, R. Ismail, S. Naziri, R. Hussin, M. Isa, and M. Basir, "Face recognition and identification using deep learning approach," in *Journal of Physics: Conference Series*, vol. 1755, no. 1: IOP Publishing, p. 012006, 2021.
[27] T. Dhawle, U. Ukey, and R. Choudante, "Face Detection and Recognition Using OpenCV and Python," *International Research Journal of Engineering and Technology (IRJET),* vol. 7, no. 10, 2020.
[28] C. Obed-Emeribe, "Multimodal biometric technology system framework and e-commerce in Emerging Markets," *International Journal of Advanced Computer Science and Applications,* vol. 4, no. 7, 2013.
[29] A. Siddiqui, R. Telgad, and P. D. Deshmukh, "Multimodal biometric systems: study to improve accuracy and performance," *International Journal of Current Engineering and Technology,* vol. 4, no. 1, pp. 165-171, 2014.
[30] P. Sanjekar and J. Patil, "An overview of multimodal biometrics," *Signal & Image Processing,* vol. 4, no. 1, p. 57, 2013.
[31] V. M. Mane and D. V. Jadhav, "Review of multimodal biometrics: applications, challenges and research areas," *International Journal of Biometrics and Bioinformatics (IJBB),* vol. 3, no. 5, pp. 90-95, 2009.

[32]K. Kumar and M. Farik, "A review of multimodal biometric authentication systems," *Int. J. Sci. Technol. Res,* vol. 5, no. 12, pp. 5-9, 2016.

[33]N. Hezil and A. Boukrouche, "Multimodal biometric recognition using human ear and palmprint," *IET Biometrics,* vol. 6, no. 5, pp. 351-359, 2017.

[34]D. T. Meva and C. Kumbharana, "Comparative study of different fusion techniques in multimodal biometric authentication," *International Journal of Computer Applications,* vol. 66, no. 19, pp. 16-19, 2013.

[35]M. I. Ahmad, W. L. Woo, and S. S. Dlay, "Multimodal biometric fusion at feature level: Face and palmprint," in *2010 7th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP 2010)*, IEEE, 2010, pp. 801-805.

[36]J. C. Klontz, B. F. Klare, S. Klum, A. K. Jain, and M. J. Burge, "Open source biometric recognition," in *2013 IEEE Sixth international conference on biometrics: theory, applications and systems (BTAS)*, IEEE, 2013, pp. 1-8.

[37]P. Lokhande, "E-commerce applications: Vulnerabilities, attacks and countermeasures," 2013.

[38]H. Patel, "E-Commerce Security Threats, Defenses Against Attacks and Improving Security," *Defenses Against Attacks and Improving* Security, vol. 9, no. 4(7), pp. 173-182, 2020.

[39]A. G. Khan, "Electronic commerce: A study on benefits and challenges in an emerging economy," *Global Journal of Management and Business Research*, vol. 16, no. 1, 2016.