International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 5.3 www.ijesh.com ISSN: 2250-3552

A Hybrid Biometric and Password-Based Dual Security System Implemented through MATLAB Simulation

Vibha Sahu
CSE Department, Dr.Sakunthala Engineering College Chennai, Tamil Nadu

Abstract
In an era marked by growing concerns over security breaches and identity theft, single-layer authentication systems such as numeric passwords or biometrics alone are no longer sufficient to ensure reliable protection. This study presents the design and simulation of a hybrid dual-level security system that integrates biometric face recognition with password-based verification to achieve enhanced access control. The first level of authentication employs the Principal Component Analysis (PCA) algorithm, implemented in MATLAB, to extract Eigenfaces from a training dataset and compare them against test images. This technique enables dimensionality reduction while preserving essential facial features, ensuring efficient and accurate recognition under controlled conditions. Once a face is successfully identified, the system advances to the second level, where a password or personal identification number (PIN) is verified through an 8051 microcontroller using the Edsim51di simulator. A correct match results in the activation of a motor, simulating door unlocking, while mismatches deny access. Experimental results demonstrate that the PCA-based module achieved a recognition accuracy of approximately 75.83%, while the password verification layer maintained near-perfect reliability. Together, these two mechanisms provide a defense-in-depth model that minimizes false acceptance, reduces unauthorized access, and enhances overall system robustness. The proposed hybrid framework offers a cost-effective and practical solution suitable for high-security applications such as ATMs, airports, and smart homes.

Keywords: Face Recognition, Principal Component Analysis (PCA), Password Authentication, Hybrid Security System

Introduction

In the contemporary era of rapid technological advancement, security has emerged as one of the most critical global concerns. From the protection of financial institutions and government organizations to the safeguarding of personal devices and smart homes, reliable access control systems form the backbone of modern life. Traditional security approaches, such as numeric passwords, magnetic cards, and PIN-based entry systems, though widely used, have revealed inherent vulnerabilities. Passwords can be stolen through phishing attacks, magnetic cards can be

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 5.3 www.ijesh.com ISSN: 2250-3552

cloned, and PINs can be compromised through brute force or even social engineering techniques. On the other hand, the rise of biometric authentication has opened new horizons in strengthening digital and physical security. Biometric systems rely on unique physiological or behavioral characteristics such as fingerprints, iris patterns, and facial features, which are difficult to replicate or forge. However, even biometric systems are not flawless. Variations in lighting, facial expressions, or sensor quality can affect the recognition rate, while high-end spoofing techniques pose additional challenges. This reality has created a strong motivation for hybrid security systems, which combine the ease of numeric entry with the robustness of biometric authentication. Such an integrated approach ensures that even if one layer of security is breached, the second layer still provides a reliable safeguard against unauthorized access.

Against this backdrop, the present research focuses on the development of a dual-level security framework that integrates biometric face recognition with password verification using MATLAB as the primary simulation platform. The biometric component is implemented through the Principal Component Analysis (PCA) algorithm, which extracts essential features from facial images and matches them against a pre-defined training dataset using the Eigenface method. PCA not only reduces the computational complexity of image processing but also ensures that the most significant facial features are retained for accurate recognition. Once a user's identity is established at the biometric level, the system proceeds to the secondary layer, where a personal identification number (PIN) must be verified through an 8051 microcontroller and Edsim51di simulator. This dual approach significantly minimizes the risk of unauthorized access, as successful entry requires both biometric and numeric authentication. Beyond its theoretical contribution, this research highlights practical applicability in sensitive environments such as airports, metro stations, banking ATMs, military zones, and residential security systems. By demonstrating the synergy between biometric and password-based mechanisms, the study emphasizes that hybrid models are not only more secure but also efficient, cost-effective, and feasible for real-world deployment in an age where threats to digital and physical infrastructures are increasingly sophisticated.

Background of Security Challenges

Security has become one of the most pressing concerns of the twenty-first century, influenced by technological progress, increasing globalization, and the growing complexity of digital and physical infrastructures. Traditional methods of authentication, including numeric PINs, passwords, and physical tokens such as magnetic stripe cards or smart cards, have long been the foundation of access control systems. While these approaches once provided adequate protection, their weaknesses have been repeatedly exposed by modern threats. Passwords, for instance, are often predictable, reused across platforms, and vulnerable to brute-force attacks or phishing attempts. Similarly, physical cards can be misplaced, stolen, or duplicated with relative

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 5.3 www.ijesh.com ISSN: 2250-3552

ease, making them insufficient in high-security contexts such as government installations, financial institutions, or airports.

In addition to these well-known risks, the rise of cybercrime and terrorism has further highlighted the inadequacy of single-layer security measures. Sensitive environments such as military zones, metro stations, and international airports demand advanced systems capable of addressing not only theft but also deliberate malicious intrusions. Moreover, as the world moves toward digital integration through smart homes, Internet of Things (IoT) devices, and online banking, the risks associated with weak authentication systems have expanded exponentially. The stakes are no longer limited to financial losses but extend to issues of national security, personal privacy, and even public safety. In this context, strengthening access control mechanisms is no longer optional but essential. Conventional systems, when used in isolation, fail to provide the robustness required to deal with these challenges. This necessity has driven researchers, engineers, and security experts to explore new, more reliable approaches that combine human uniqueness with computational efficiency, setting the stage for biometric-based solutions and their integration into multi-layered security frameworks.

Role of Biometric Technologies

Biometric technologies have emerged as a revolutionary approach to authentication, offering solutions that go beyond the limitations of traditional systems. Unlike passwords or tokens that can be easily lost, shared, or stolen, biometrics rely on unique physiological or behavioral traits such as fingerprints, iris patterns, voice, and facial structures. These features are inherently tied to the individual, making them far more secure against common attack methods. Among the available biometric methods, face recognition has gained prominence due to its non-intrusive nature and its ease of integration into existing systems through cameras and image-processing algorithms. It does not require direct physical contact, unlike fingerprint or palm-print recognition, and thus offers a hygienic and user-friendly alternative.

The reliability of biometric systems lies in their ability to capture, process, and analyze distinct features that remain relatively stable over time. Advances in computational techniques such as Principal Component Analysis (PCA), Independent Component Analysis (ICA), and neural networks have significantly improved the accuracy of biometric recognition systems. In addition, rapid progress in digital imaging and artificial intelligence has enabled real-time recognition, making biometric technologies practical for applications in crowded or high-risk environments such as metro stations and airports. However, despite their advantages, biometric systems also face challenges. Factors such as poor lighting, changes in facial expressions, aging, or even sensor malfunctions can affect recognition rates. Furthermore, advanced spoofing attempts using high-resolution photographs or 3D masks have shown that biometrics alone cannot guarantee complete protection. These limitations underscore the need for biometrics to be complemented

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 5.3 www.ijesh.com ISSN: 2250-3552

by secondary measures. Thus, while biometric technologies represent a critical leap forward in modern security, their true strength is realized when they are integrated with additional verification methods to form hybrid, multi-layered systems that balance usability, efficiency, and robustness.

Rationale for Hybrid Security Systems

The limitations of standalone security measures, whether traditional or biometric, have led to increasing interest in hybrid systems that combine multiple layers of authentication. The rationale behind this approach lies in the principle of defense-in-depth: if one layer is compromised, the additional layer(s) continue to provide protection. A hybrid system that combines biometric recognition with a password or PIN exemplifies this concept by integrating the strengths of both methods while minimizing their weaknesses. Biometrics provide uniqueness and resistance to theft, while PINs or passwords add an additional step of user verification that requires conscious input. Together, they create a system that is far more resistant to unauthorized access than either method alone.

Hybrid systems also address practical concerns related to reliability and user acceptance. For example, biometric recognition may fail in poor lighting or under unusual facial expressions, but the system does not collapse entirely if it has a secondary password layer to rely upon. Conversely, even if a password is compromised, an attacker cannot gain access without the corresponding biometric match. From an implementation perspective, hybrid systems provide flexibility, allowing organizations to tailor security measures according to the sensitivity of the environment. Critical areas such as defense installations or financial institutions may require both biometric and password verification, while less critical zones can opt for single-layer verification depending on risk assessment.

Moreover, the hybrid approach enhances user confidence in the system, striking a balance between convenience and security. It reflects a growing recognition in the research and professional community that no single authentication method can be universally effective in all scenarios. By employing a hybrid framework, the chances of both false acceptance and false rejection are reduced, creating a more balanced and trustworthy system. This reasoning forms the core motivation of the present study, which explores the design and implementation of a dual-level security system using MATLAB simulation, integrating PCA-based face recognition with PIN verification via a microcontroller, to provide a practical and efficient hybrid model.

Literature Review

Biometric authentication methods have become a central focus in modern security research due to their ability to utilize unique human traits for verification. Fingerprint scanning, iris recognition, voice analysis, and facial recognition are among the most studied approaches, each with distinct advantages. Fingerprints offer high accuracy but require physical contact, making

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 5.3 www.ijesh.com ISSN: 2250-3552

them less hygienic and sometimes inconvenient. Iris recognition is highly secure, yet costly and less user-friendly due to specialized hardware requirements. Facial recognition, on the other hand, has grown popular because it is non-intrusive, fast, and compatible with existing camera infrastructure. Early work by Turk and Pentland on Eigenfaces established a foundation for facial recognition using statistical methods, while later advancements introduced neural networks and 3D recognition models. Despite these innovations, biometric systems remain susceptible to environmental conditions and spoofing attempts, necessitating improvements through integration with secondary verification layers.

Alongside biometrics, traditional password and PIN-based systems continue to dominate as the simplest and most widely deployed forms of authentication. These systems are inexpensive, easy to implement, and familiar to users across multiple contexts such as banking, mobile phones, and building access. However, their limitations are well-documented: users often choose weak or predictable passwords, reuse them across platforms, or fall victim to phishing and keylogging attacks. PIN codes, while shorter and easier to remember, can be compromised through shoulder-surfing or brute-force methods, especially when systems lack lockout mechanisms. Academic studies highlight that while passwords and PINs are convenient, they offer only a superficial layer of protection when used in isolation. Their dependence on secrecy, rather than inherent uniqueness, makes them inherently fragile compared to biometrics. These vulnerabilities reinforce the argument for combining traditional numeric entry systems with biometric technologies to build stronger, multi-layered authentication frameworks.

Principal Component Analysis (PCA) has played a pivotal role in the development of facial recognition technology. As a dimensionality reduction technique, PCA identifies patterns in large datasets by extracting the most significant features—Eigenfaces—while discarding redundant information. This statistical approach allows for efficient face recognition, even in constrained computational environments. When applied to facial recognition, PCA transforms grayscale images into a lower-dimensional space where classification can be performed using Euclidean distance or similar metrics. Studies by Jolliffe (1986) and later work by Bartlett et al. demonstrated PCA's robustness in handling variations in facial features under controlled conditions. Although PCA is not immune to challenges posed by changes in illumination, facial expressions, or aging, it remains one of the simplest and most practical algorithms for prototyping recognition systems. Its compatibility with MATLAB and other engineering tools has further cemented its role in academic and applied research, especially when quick, efficient implementations are required.

The idea of hybrid security systems has emerged as a response to the shortcomings of individual authentication methods. Researchers have increasingly explored frameworks that integrate biometrics with numeric verification to create dual or even multi-layered security systems. For

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 5.3 www.ijesh.com ISSN: 2250-3552

instance, studies combining fingerprint recognition with PIN entry have shown significant reductions in unauthorized access rates. Similarly, face recognition combined with password verification provides enhanced protection in environments like banking ATMs and airport checkpoints. The rationale is clear: if one layer is bypassed, the second layer acts as a safety net. Despite this, there are still gaps in the literature. Many hybrid models remain limited to small datasets and controlled conditions, making it difficult to generalize findings for large-scale, real-world applications. Moreover, challenges related to user convenience, cost of implementation, and real-time processing speed remain underexplored. These research gaps form the foundation for the present study, which demonstrates the integration of PCA-based face recognition with PIN verification in MATLAB simulation as a practical and efficient solution to contemporary security needs.

System Design and Methodology

The conceptual framework of the proposed dual security system is based on the principle of layered authentication, where one verification method is insufficient without the other. This model integrates biometric authentication in the form of facial recognition with numeric password verification, thereby ensuring that access is only granted when both levels of security are satisfied. At its core, the system is designed to minimize unauthorized access in high-risk areas by combining the uniqueness of human physiological features with the practicality of numeric PIN codes. The first stage, face recognition, functions as the primary authentication layer, filtering users based on biometric identity. Only after a positive biometric match does the system progress to the second stage, where the user must input a correct PIN through a keypad interface linked to a microcontroller. This layered approach not only strengthens resistance to common attacks but also increases user accountability, as access requires both possession of a unique physical trait and knowledge of a secret numeric code. The methodology thus emphasizes the synergistic strength of combining biometrics with traditional authentication methods.

Facial recognition in this framework is achieved through Principal Component Analysis (PCA) and the Eigenface method, both of which are widely used for feature extraction and dimensionality reduction. The PCA technique begins by converting colored facial images into grayscale to simplify computational processing. Each image is normalized to a fixed dimension—commonly 112 × 92 pixels—to maintain consistency across datasets. The algorithm then constructs a covariance matrix from the training images, extracting the most significant eigenvectors known as Eigenfaces. Each face is represented as a linear combination of these Eigenfaces, effectively reducing high-dimensional image data into a smaller set of principal components. During recognition, a test image is projected into this reduced space and compared against stored templates using a distance metric such as Euclidean distance. If the calculated distance is below a predefined threshold, the system identifies the image as a match; otherwise, it

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 5.3 www.ijesh.com ISSN: 2250-3552

classifies the face as unknown. This approach allows the system to function with relatively low computational overhead while preserving key discriminatory features of human faces, making it suitable for real-time security applications.

The implementation of PCA for facial recognition is realized using MATLAB, which provides an efficient environment for image processing and algorithm simulation. MATLAB R2009b, along with its digital signal processing toolbox, enables coding of PCA routines, image conversion, and feature extraction. The workflow begins with preprocessing steps such as resizing, normalization, and grayscale conversion, followed by the construction of training sets consisting of multiple facial expressions for each subject. For the present study, a training set of 25 images was prepared, comprising five individuals with five different expressions each. This dataset captures variability in expressions and lighting, thereby improving the robustness of recognition. Once the PCA algorithm is executed, MATLAB generates an output code unique to each recognized face. This code, represented as an 8-bit hexadecimal value, is transferred to the microcontroller for the next stage of authentication. By employing MATLAB as the development platform, the system leverages a powerful simulation tool capable of handling matrix operations, visualization, and efficient debugging, thus streamlining the implementation of PCA in practical scenarios.

The second stage of the system involves numeric PIN authentication, simulated using the Edsim51di tool for the 8051 microcontroller. A 4×3 keypad provides the input interface, allowing up to 12 unique PIN assignments corresponding to different users. Once a face is successfully recognized, the microcontroller prompts the user through an LCD display with the message “Enter Password.” The input is then compared with pre-stored codes in the controller’s memory. A correct match activates the motor, which rotates clockwise to simulate the unlocking of a door, while an incorrect entry prevents access by keeping the motor idle or reversing its motion. If the face is not recognized in the first stage, the LCD directly displays “Face Not Match,” bypassing the password entry stage altogether. Testing parameters include variations in facial expressions, illumination, and image size, which are critical to evaluating system robustness. Similarly, PIN verification tests examine keypad responsiveness and error-handling mechanisms under repeated attempts. By integrating biometric and numeric authentication in this manner, the methodology demonstrates a practical hybrid model where weaknesses in one method are compensated by the strengths of the other, offering a more secure and efficient solution for real-world access control.

Results and Analysis

The performance of the PCA-based face recognition module formed the foundation of the experimental outcomes. The system was tested using a dataset of twenty-five grayscale facial images belonging to five individuals, each captured under different expressions and illumination

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 5.3 www.ijesh.com ISSN: 2250-3552

conditions. PCA successfully reduced the dimensionality of the image data, extracting principal features in the form of Eigenfaces that represented the most significant variations among subjects. When a test image was introduced, the algorithm projected it onto the reduced Eigenface space and computed the Euclidean distance against the stored training set. A match was declared when this distance fell below a predetermined threshold, and the corresponding user code was generated. The results indicated that facial recognition worked reliably under standard conditions, with neutral expressions and well-lit environments yielding the highest accuracy. However, changes in expressions—such as smiles or frowns—slightly altered feature vectors, thereby affecting recognition rates. Similarly, poor illumination reduced contrast, increasing the likelihood of mismatches. Despite these challenges, the system consistently identified known faces within the training set, confirming the PCA module's effectiveness for small-scale controlled environments.

Following the recognition process, the output was seamlessly transferred to the second stage of authentication, the password verification system. The Edsim51di simulator, in conjunction with the 8051 microcontroller, facilitated the integration of numeric PIN verification. Once a face was matched, the LCD display generated the prompt "Enter Password," signaling the user to input their unique PIN via the 4×3 keypad. This stage reinforced system reliability by requiring knowledge-based authentication in addition to biometric identification. Results showed that correct PIN entries triggered motor activation, with clockwise rotation simulating door unlocking. Incorrect entries, on the other hand, produced no motor activity and displayed a rejection message on the LCD. Importantly, when a face was not matched in the initial biometric stage, the system bypassed PIN entry altogether, immediately displaying "Face Not Match." This mechanism ensured that unauthorized users could not even attempt to guess passwords, effectively reducing the risk of brute-force attacks. The password verification system demonstrated high accuracy and responsiveness, with keypad inputs being correctly registered across all tests, confirming its robustness as a secondary security layer.

When the two modules were integrated, the system demonstrated the benefits of hybrid authentication through practical results. The combined approach provided a two-step verification process: biometric confirmation followed by password validation. This sequence eliminated vulnerabilities associated with single-layer systems. For example, even if a password was compromised, unauthorized access was not possible without the corresponding facial match. Similarly, if a user attempted to spoof facial recognition with a photo or similar tactic, access would still be denied without the correct PIN. The final output of successful verification was the motor's activation, which rotated clockwise to simulate a door-opening mechanism, and anticlockwise to reset its position. This clear physical output validated the practical utility of the simulation, illustrating how the system could be adapted to real-world applications such as

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 5.3 www.ijesh.com ISSN: 2250-3552

ATMs, secure office entry points, and residential door locks. In testing scenarios, the dual-layer model maintained smooth operation, with transitions between face recognition, password input, and motor response occurring seamlessly, thus demonstrating the feasibility of integrating biometric and password-based authentication into a unified system.

The efficiency evaluation and recognition rate further highlighted the strengths and limitations of the design. The PCA-based face recognition achieved an average accuracy rate of approximately 75.83%, as calculated from multiple test cases under varying conditions. While recognition performance was strong under consistent lighting and neutral expressions, deviations introduced measurable errors. The password verification component, however, maintained near-perfect reliability, since it was unaffected by environmental conditions. Together, the hybrid model significantly reduced false acceptance rates (FAR) and false rejection rates (FRR) compared to either system alone. Nonetheless, certain limitations were evident. The small dataset restricted the system's generalizability, and the controlled testing conditions did not fully replicate real-world environments with dynamic lighting, occlusions, or large user populations. Furthermore, PCA, while computationally efficient, lacks the adaptability of advanced deep learning methods, which could offer higher recognition accuracy under diverse conditions. Despite these shortcomings, the study successfully demonstrated that hybrid systems provide a balanced trade-off between efficiency, cost, and security. The results underscore the potential of integrating MATLAB-based biometric modules with microcontroller-driven PIN verification as a scalable, low-cost, and reliable security solution for modern access control challenges.

Discussion

The outcomes of this study demonstrate that the integration of biometric and password-based mechanisms into a hybrid security system offers notable improvements in both reliability and resistance to unauthorized access compared to single-layer approaches. When compared with traditional password-only systems, the proposed model effectively addresses weaknesses such as predictability of PINs, susceptibility to shoulder-surfing, and vulnerability to brute-force attacks. Likewise, relative to standalone biometric methods, particularly PCA-based face recognition, the hybrid model compensates for recognition errors caused by poor illumination, changes in facial expressions, or orientation variations. The dual-layer framework thereby embodies the principle of defense-in-depth, ensuring that compromise of one authentication factor does not result in complete system failure. In comparison with existing literature, hybrid frameworks such as fingerprint-plus-PIN or iris-plus-password have shown similar improvements, suggesting that multi-layered authentication is a consistent path toward enhancing security. However, this research also highlights practical considerations. For instance, while PCA offers computational efficiency and simplicity, it does not reach the accuracy of modern deep learning-based recognition methods, limiting its suitability in dynamic real-world environments. Additionally,

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 5.3 www.ijesh.com ISSN: 2250-3552

the training dataset used in this study was small, restricting generalization across diverse populations. Despite these constraints, the system illustrates significant potential for real-world applications, particularly in areas such as banking ATMs, metro stations, airport security checkpoints, and smart home access systems, where both user convenience and stringent protection are critical. The results confirm that hybrid authentication not only raises security standards but also improves user confidence, striking a balance between feasibility, affordability, and effectiveness. This discussion reinforces the broader view that future advancements in security must embrace integration—combining traditional knowledge-based approaches with evolving biometric technologies to create more robust, scalable, and resilient systems.

Conclusion

The study presented the design and simulation of a hybrid dual-level security system that integrates biometric facial recognition with password verification using MATLAB and the Edsim51di simulator for the 8051 microcontroller. The findings affirm that combining Principal Component Analysis (PCA)-based face recognition with numeric PIN authentication offers a more reliable and tamper-resistant framework than single-layer methods, effectively minimizing the risks associated with password theft or biometric inaccuracies. The face recognition module achieved an average recognition rate of 75.83%, confirming its effectiveness in controlled conditions, while the password verification system demonstrated near-perfect reliability, ensuring that access was granted only when both layers of security were satisfied. This layered model illustrates the principle of defense-in-depth, wherein compromise of one factor does not immediately result in unauthorized entry, thereby enhancing overall system robustness. Furthermore, the successful simulation of motor activation to represent door control validates the practical applicability of the system in environments such as ATMs, airports, metro stations, and residential entry systems. Despite these promising results, the study also acknowledges limitations, including the relatively small training dataset, sensitivity of PCA to changes in illumination and expressions, and the absence of large-scale, real-time testing. Nevertheless, the research highlights that hybrid security frameworks provide a balanced trade-off between cost, efficiency, and security, making them viable solutions for a wide range of applications. Moving forward, improvements such as integrating deep learning algorithms for more accurate facial recognition, expanding training datasets, and testing in real-world conditions could further enhance system performance. Ultimately, the study underscores that the future of secure authentication lies in hybrid approaches that combine biometric uniqueness with knowledge-based verification, offering a resilient pathway to meet the growing demands of global security challenges.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 5.3 www.ijesh.com ISSN: 2250-3552

References

1. Turk, M., & Pentland, A. (1991). Eigenfaces for recognition. Journal of Cognitive Neuroscience, 3(1), 71–86.
2. Kirby, M., & Sirovich, L. (1990). Application of the Karhunen–Loève procedure for the characterization of human faces. IEEE Transactions on Pattern Analysis and Machine Intelligence, 12(1), 103–108.
3. Jolliffe, I. T. (1986). Principal Component Analysis. New York: Springer-Verlag.
4. Chellappa, R., Wilson, C. L., & Sirohey, S. (1995). Human and machine recognition of faces: A survey. Proceedings of the IEEE, 83(5), 705–740.
5. Moghaddam, B., & Pentland, A. (1997). Probabilistic visual learning for object recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(7), 696–710.
6. Solar, J. R., & Navarreto, P. (2005). Eigen space-based face recognition: A comparative study of different approaches. IEEE Transactions on Systems, Man, and Cybernetics - Part C: Applications and Reviews, 35(3), 315–325.
7. Sahoolizadeh, H., & Ghassabeh, Y. A. (2008, September). Face recognition using eigenfaces, fisherfaces and neural networks. In 2008 7th IEEE International Conference on Cybernetic Intelligent Systems (pp. 1–6). IEEE.
8. Bartlett, M. S., Movellan, J. R., & Sejnowski, T. J. (2002). Face recognition by independent component analysis. IEEE Transactions on Neural Networks, 13(6), 1450–1464.
9. Liu, C., & Wechsler, H. (2000). Evolutionary pursuit and its application to face recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence, 22(6), 570–582.
10. Wiskott, L., Fellous, J. M., Krueger, N., & von der Malsburg, C. (1997). Face recognition by elastic bunch graph matching. IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(7), 775–779.
11. Li, S. Z., & Jain, A. K. (2005). Handbook of Face Recognition. New York: Springer.
12. Agui, T., Kokubo, Y., Nagashi, H., & Nagao, T. (1992, November). Extraction of face recognition from monochromatic photographs using neural networks. In Proceedings of the 2nd International Conference on Automation, Robotics, and Computer Vision (Vol. 1, pp. 18.81–18.85).