IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

ADVANCEMENTS IN MULTIMODAL BIOMETRIC SYSTEMS

Gurpreet Kaur[1]
[1]Associate Professor
[1]P G Department of Computer Science,
[1]SGGS College, affiliated to Panjab University, Chandigarh, India

Abstract: Biometric systems have become integral in providing secure and reliable methods for identity verification. As technology progresses, there is a paradigm shift towards the adoption of multimodal biometric systems, which leverage multiple physiological and behavioral characteristics for enhanced accuracy and robustness. This paper delves into the intricate details of multimodal biometric systems, examining the underlying technologies, theoretical frameworks, challenges, and future directions.

Keywords: Unimodal, Multimodal, Biometric, Authentication, Security

I INTRODUCTION

In Multimodal Biometric Technologies , each major biometric modality is dissected, examining the state-of-the-art technologies utilized in multimodal systems. The evolution of biometric systems establishes the need for multimodal approaches in overcoming the limitations of unimodal systems. The multimodal biometric systems are scrutinized, including enhanced accuracy, improved robustness, and increased security. There are diverse applications of multimodal biometric systems across various industries, including government and law enforcement, financial services, healthcare, and enterprise security. The limitations and challenges, addressing issues related to integration complexity, privacy concerns, and the necessity for standardized protocols [1]. The unimodal uses only one biometric data such as fingerprint or face or palm print or iris. Multimodal biometric is the convention of combining and correlating multiple biometrics[2]. Multimodal authentication endow with more than one level of authentication than the unimodal biometrics.

II SECURITY BIOMETRIC SYSTEM APPLICATIONS

Security implications of multimodal biometric systems, focus on their effectiveness in thwarting spoofing attacks and enhancing overall system security. The ethical considerations related to user privacy, data protection, and potential misuse of biometric information is a continuous process . Exploring new perspectives and advancements in the security implications of multimodal biometric systems can lead to innovative solutions and improvements in authentication technologies [3].

Behavioral Biometrics for Continuous Authentication investigates the integration of continuous authentication using behavioral biometrics, such as keystroke dynamics, mouse dynamics, or gait analysis. The continuous authentication mechanisms can enhance the overall security of multimodal systems by dynamically adapting to users' behavioral patterns.

Blockchain Secure Biometric Data Handling leverages blockchain technology to enhance the security of storing and handling biometric data in multimodal systems. The decentralized and tamper-resistant ledger can contribute to securing sensitive biometric information and maintaining user privacy.

Post-Quantum Cryptography in Biometric Systems is a multimodal biometric systems. This ensure the long-term security and resilience of biometric data against potential quantum computing threats.

Artificial Intelligence in Multimodal Systems is develops models to provide accurate results but also offer transparent explanations for decision-making, addressing concerns related to system interpretability and user trust.

Cross-Modal Transfer Learning uses the knowledge gained from one biometric modality and transfers it to enhance the enhance the performance of another, improving overall system accuracy.

Biometric Template Protection Using Homomorphic Encryption is used during transmission and storage without compromising the accuracy of multimodal biometric systems.

Differential Privacy for Biometric Data protects the individual privacy in multimodal biometric systems. It explore how the mechanism of adding noise to the data during processing achieves a balance between accuracy and privacy, especially in large-scale deployments.

Secure Hardware Enclaves such as Trusted Execution Environments (TEEs), in multimodal biometric systems. This hardware-based security can protect sensitive computations and biometric data from potential attacks.

Adversarial Attacks on Multimodal Systems works on the generative adversarial networks (GANs) or other techniques might be employed to manipulate or spoof multiple biometric modalities and propose robust defense mechanisms.

Human-Centric Security Metrics form a human-centric perspective with factors such as user acceptance, usability, and the psychological impact of security measures on individuals.

III UNIMODAL BIOMETRICS

Unimodal biometrics refers to the use of a single physiological or behavioral characteristic for identification or verification purposes. It relies on one distinct trait to recognize and authenticate individuals. It is Simple in implementation and usage, non-intrusive and user-friendly. here are challenges associated by being susceptible to environmental factors of illumination and noise, time bound variable traits, with limited accuracy.

3.1 Facial Recognition

Facial recognition is a mechanism for identification using the face. This is further extended to photos inputs, continuous videos and real time authentication modes[4]. Identifying individuals and in other cases comparing if both the inputs are refereeing to the same person is a challenge. Facial recognition algorithms leverage mathematical representations of facial features to identify individuals. There are several algorithms in literature with advantages and limitation. A fundamental techniques used is Principal Component Analysis (PCA). This is expressed below by the equation as

[X = bar{X} + sum_{i=1}^{n} a_i cdot e_i] *(3.1)*

Here, X represents the facial image, bar{X} is the mean face, a_i denotes the weights for each principal component e_i, and n is the number of principal components

3.2 Fingerprint Recognition

This is the method to verify the identity of a person. The fingerprints need to be captured, stored and compared as required [5]. These impressions consisting of a series of ridges and grooves. These are located with minutiae points with beginning points and terminates. These minutiae points are mapped with lines. The mathematical computations, with the minutiae points serving as key identifiers. The Euclidean distance formula is often applied

[D = sqrt{sum_{i=1}^{n} (P_i - Q_i)^2}] *(3.2)*

where, D represents the Euclidean distance between two fingerprint minutiae sets P and Q

3.3 Iris Recognition

This is an automated biometric. It uses pattern recognition. Either one or both iris are are scanned. The patterns are unique and stable[6]. The mathematical representation of the iris involves encoding its unique patterns. The Daugman's Integro-Differential Operator captures the distinctive features, expressed as:

[M(x, y) = G(rho, phi) left|frac{d}{dr} left(frac{I(x, y)}{dr}right)right| dr d(phi)] *(3.3)*

Here, M(x, y) is the iris pattern, G(rho, phi) is a 2D Gaussian function, and (I(x, y) is the iris intensity.

3.4 Voice recognition

This systems allows the users to communicate with technology. Simple conversation creates a comfort zone [6]. It capably performs trivial tasks. This employs mathematical models to analyze speech signals. The Hidden Markov Model (HMM), with the probability density function expressed as:

[P(O|lambda) = prod_{t=1}^{T} sum_{i=1}^{N} c_i cdot b_i(O_t) cdot alpha_{t,i} \] *(3.4)*

This equation represents the probability of observing the acoustic vector sequence (O) given the model parameters lambda.

3.5 Gait Recognition

Gait recognition involves analyzing the spatiotemporal parameters of an individual's walking pattern [7]. The Dynamic Time Warping (DTW) algorithm calculates the similarity between two gait sequences using the following formula:

[D(i, j) = d(i, j) + min left(D(i-1, j), D(i, j-1), D(i-1, j-1)right)] *(3.5)*

Here, (D(i, j)) is the cumulative distance, (d(i, j)) represents the local distance between two gait feature vectors, and (i) and (j) index the feature vectors.

These mathematical representations showcase the complexity and sophistication involved in modeling the distinct characteristics of each biometric modality within multimodal biometric systems. The fusion of these diverse mathematical frameworks contributes to the system's ability to provide robust and accurate identity verification across multiple dimensions.

International Research Journal
IJNRD
Research Through Innovation

IV Multimodal Biometric

Multimodal biometrics involves the integration of two or more unimodal biometric systems to enhance the overall accuracy and reliability of identification or verification[8][9]. By combining different modalities, the system aims to compensate for the limitations of individual methods. It extends higher accuracy and reliability, with enhanced security as it provides multiple layers of verification. There is a increased - complexity in system design with higher cost and potential privacy concerns due to the collection of diverse biometric data.

4.1 Behavioral biometrics

Biometric of behaviour encompassing keystroke dynamics, mouse dynamics, gait analysis, and more, offers a unique perspective in user authentication [10]. This paper provides a comprehensive review of behavioral biometrics, presents a novel methodology for behavioral data collection, and analyzes the potential applications and challenges in this evolving field. Behavioral biometrics leverage unique user traits, providing an additional layer of security beyond traditional methods[11].

Behavioral biometrics involve the analysis of unique patterns in human behavior. This includes keystroke dynamics, mouse dynamics, gait analysis, and other behavioral traits. Keystroke dynamics involve the analysis of typing patterns, including key press duration and intervals. Numerous studies have demonstrated the effectiveness of keystroke dynamics in user authentication. Mouse dynamics focus on the unique patterns in mouse movements, clicks, and scrolls. This modality adds an additional layer of security, particularly in web-based environments[13]. Gait analysis studies the distinct walking patterns of individuals. Although primarily used in surveillance, gait analysis has potential applications in user authentication. Behavioral biometrics face challenges related to variability, user acceptance, and environmental factors. Ensuring robustness in real-world scenarios remains a significant concern.

V Discussion

Accuracy vs. Complexity : Unimodal systems, while simpler, may have limitations in accuracy. Multimodal systems strive to achieve higher accuracy but come with increased complexity.

Application Specificity: Unimodal systems may be suitable for specific applications with moderate security requirements. Multimodal systems are often deployed in high-security environments where accuracy is paramount[14].

Continuous Advancements: Both unimodal and multimodal biometrics benefit from continuous advancements in technology, including the incorporation of machine learning and deep learning techniques.

Ethical Considerations: As biometric systems become more prevalent, ethical considerations surrounding privacy, data security, and user consent are of growing importance for both unimodal and multimodal approaches [15].

The goal of multimodal systems is to enhance accuracy, reliability, and security by combining information from diverse sources. The choice between unimodal and multimodal biometrics depends on the specific requirements of the application, considering factors such as accuracy, security level, and the operational environment. Advances in technology continue to shape the landscape of biometrics, offering innovative solutions to address various challenges.

VI Conclusion

It underscores the significance of multimodal biometric systems in shaping the future of secure identity verification by addressing both technical and user-related aspects of this emerging field. Behavioral biometrics offer a unique and promising avenue for user authentication. This study contributes to the understanding of keystroke dynamics, mouse dynamics, and gait analysis, highlighting their potential applications and challenges. As technology evolves, behavioral biometrics are poised to play a vital role in enhancing security measures. The paper concludes with a call to action for continued research and development in this dynamic field. By exploring these innovative areas, contributions to the ongoing evolution of multimodal biometric systems, addressing current challenges and shaping the future of secure and privacy-aware identity verification technologies.

VII Competing interests

The authors have no Competing interests at stake and there is No Conflict of Interest.

References

[1] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20.

[2] Rattani, A., Derakhshani, R., & Ross, A. (2016). A survey of biometric systems in large-scale databases. ACM Computing Surveys (CSUR), 49(1), 7.

[3] Radoglou-Grammatikis, P., Sarigiannidis, P., & Moscholios, I. (2017). Security for the internet of things: A survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials, 20(3), 2727-2756.

[4] M. A. Turk and A. P. Pentland, "Face recognition using eigenfaces," *Proceedings. 1991 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, Maui, HI, USA, 1991, pp. 586-591, doi: 10.1109/CVPR.1991.139758. keywords: {Face recognition;Face detection;Humans;Character recognition;Computer vision;Head;Eyes;Nose;Computational modeling;Image recognition}

[5] Prabhakar, Salil. (2001). Fingerprint Classification and Matching Using a Filterbank.

[6] J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1148-1161, Nov. 1993, doi: 10.1109/34.244676. keywords:

{Testing;Iris;Biometrics;Humans;Decision theory;Error analysis;Image texture analysis;Pattern recognition;Fingerprint recognition;Face},

[7] Rabiner, Lawrence R.. “A tutorial on hidden Markov models and selected applications in speech recognition.” *Proc. IEEE* 77 (1989): 257-286.

[8] Stylios, Ioannis & Thanou, Olga & Androulidakis, Iosif & Zaitseva, Elena. (2016). A Review of Continuous Authentication Using Behavioral Biometrics. 10.1145/2984393.2984403.

[9] Li, S.Z., Schouten, B., Tistarelli, M. (2009). Biometrics at a Distance: Issues, Challenges, and Prospects. In: Tistarelli, M., Li, S.Z., Chellappa, R. (eds) Handbook of Remote Biometrics. Advances in Pattern Recognition. Springer, London. https://doi.org/10.1007/978-1-84882-385-3_1

[10] Ross, Arun & Poh, Norman. (2009). Multibiometric Systems: Overview, Case Studies, and Open Issues. 10.1007/978-1-84882-385-3_11.

[11] Al-zanganawi, Anfal & Kurnaz, Sefer. (2020). Human Biometrics Detection And Recognition System Using SVM And Genetic Algorithm Iris As An Example. 1-4. 10.1109/ISMSIT50672.2020.9255095.

[12] Sanjekar, Priti & Patil, Jayantrao. (2013). An Overview of Multimodal Biometrics. Signal & Image Processing: An International Journal (SIPIJ) Vol. 4. 57-64. 10.5121/sipij.2013.4105.

[13] Snelick, Robert & Indovina, Mike & Yen, James & Mink, Alan. (2003). Multimodal biometrics. 68. 10.1145/958444.958447.

[14] Aruna, Boda & Joseph, Dr. (2023). Multimodal Biometrics for Human Identification usingArtificial Intelligence. International Journal of Emerging Science and Engineering. 12. 1-6. 10.35940/ijese.A4278.1212123.

[15] Adjoudj, Reda & Belhia, Souaad & Allal, Anis & Bahram, Tayeb. (2023). Intelligent Integration and Fusion of Multimodal Biometric Systems. The Eurasia Proceedings of Science Technology Engineering and Mathematics. 26. 287-294. 10.55549/epstem.1409583.

International Research Journal
IJNRD
Research Through Innovation