

A Survey on Biometrics Authentication: Modalities, Multimodal Fusion, and Template Security

Ονοματεπώνυμο: Μάνος Παναγιώτης-Νικόλαος

Αριθμός Μητρώου: ba22669170

Μάθημα: Ασφάλεια Πληροφοριακών Συστημάτων (2025-2026)

Abstract

In an increasingly digitized world, establishing the identity of individuals with high accuracy and reliability is a critical requirement for securing physical and logical access. Traditional authentication methods, relying on knowledge (passwords) or possession (tokens), are highly vulnerable to loss, theft, and social engineering attacks. Biometric authentication has emerged as a robust alternative, identifying individuals based on their unique physiological or behavioral traits. This survey provides a comprehensive overview of the current state of biometric authentication. We systematically analyze prominent physiological modalities (e.g., fingerprint, facial, and iris recognition) and behavioral modalities (e.g., voice and keystroke dynamics), evaluating their respective strengths and limitations. Furthermore, this paper explores the paradigm of multimodal biometric systems, which fuse multiple traits to overcome the inherent vulnerabilities of unimodal systems, such as spoofing and noisy sensor data. Finally, a significant portion of this survey is dedicated to the critical issue of biometric template security. Since biometric traits are permanently associated with a user and cannot be revoked if compromised, we thoroughly investigate advanced protection mechanisms, focusing on steganography, watermarking, and cryptographic approaches for secure biometric data transmission and storage.

1. Introduction

The exponential growth of online transactions, cloud computing, and ubiquitous digital services has mandated the development of resilient security architectures. At the core of these architectures lies the process of user authentication—the mechanism by which a system verifies the identity of a user. Historically, authentication has been dominated by surrogate representations of identity, namely token-based systems (e.g., smart cards, magnetic stripe cards) and knowledge-based systems (e.g., passwords, Personal Identification Numbers - PINs) [1]. However, these traditional approaches suffer from fundamental security flaws: passwords can be easily forgotten, shared, or cracked through brute-force or phishing attacks, while physical tokens can be lost, duplicated, or stolen [2].

To address these vulnerabilities, biometric authentication has gained unprecedented traction [3]. Biometrics refers to the automatic recognition of individuals based on their distinct physiological characteristics (such as fingerprints, face geometry, iris patterns, and DNA) or behavioral traits (such as gait, voice, and typing rhythm) [4]. Unlike passwords or tokens, biometric identifiers are intrinsically linked to the individual, meaning they are "what you are" rather than "what you know" or "what you have." This paradigm shift not only enhances security by making identity theft significantly more difficult but also improves user convenience by eliminating the need to memorize complex alphanumeric strings [5].

Despite its undeniable advantages, biometric authentication is not without challenges. Unimodal biometric systems—those relying on a single trait—often struggle with issues such as noisy data, intra-class variations, non-universality (e.g., users with worn-out fingerprints), and vulnerability to presentation attacks (spoofing) [6]. Consequently, the scientific community has increasingly focused on multimodal biometric systems, which combine evidence from multiple biometric sources to enhance recognition accuracy and system resilience. Furthermore, the storage and transmission of biometric templates raise severe privacy and security concerns. A compromised password can be reset, but a compromised fingerprint is lost forever. Therefore, securing biometric templates against unauthorized access and tampering is currently one of the most critical research areas in information security.

The remainder of this survey is organized as follows: Section 2 introduces the fundamental concepts and performance metrics of biometric systems. Sections 3 and 4 review the major physiological and behavioral modalities, respectively. Section 5 discusses multimodal biometrics and fusion strategies. Section 6 focuses on biometric template security, highlighting steganographic and cryptographic countermeasures. Finally, Section 7 concludes the paper and outlines future research directions.

2. Fundamentals of Biometrics

To thoroughly understand biometric authentication, it is essential to outline the core characteristics that qualify a biological or behavioral trait as a valid biometric identifier, as well as the standard architecture and evaluation metrics of these systems.

According to seminal research in the field [7], any human trait can serve as a biometric identifier provided it satisfies several critical prerequisites:

- **Universality:** Every individual in the target population should possess the trait.
- **Distinctiveness (Uniqueness):** The trait should be sufficiently different across individuals to distinguish them from one another.
- **Permanence:** The biometric characteristic should remain invariant over a significant period of time, resisting aging or environmental factors.

- **Collectability:** The trait must be measurable quantitatively with reasonable sensing devices.

Beyond these biological prerequisites, practical deployment requires considering Performance (achievable recognition accuracy and speed), Acceptability (the extent to which users are willing to accept the biometric capture process), and Circumvention (how easily the system can be fooled using fraudulent methods) [8].

A standard biometric authentication system operates in two primary phases: the *enrolment phase* and the *authentication (or verification) phase* [7]. During enrolment, a sensor captures the biometric data, which is then processed by a feature extraction module to create a compact, mathematical representation known as a "template." This template is securely stored in a database. During authentication, the user provides a new sample, and the resulting query template is compared against the stored template using a matching algorithm.

The security and reliability of a biometric system are quantitatively evaluated using specific error metrics [9]:

- **False Acceptance Rate (FAR):** The probability that the system incorrectly authorizes an unauthorized user. This is a critical metric for high-security environments.
- **False Rejection Rate (FRR):** The probability that the system incorrectly rejects a legitimate, enrolled user, directly impacting user convenience.
- **Equal Error Rate (EER):** The specific operational threshold where FAR equals FRR. The lower the EER, the more accurate the biometric system is considered to be [9].

3. Physiological Biometric Modalities

Physiological biometrics rely on the physical, structural characteristics of the human body. Because these traits are fundamentally hardwired into human biology, they generally offer high distinctiveness and permanence.

3.1. Fingerprint Recognition Fingerprint recognition is arguably the oldest and most widely deployed biometric modality [10]. It analyzes the pattern of friction ridges and valleys on the surface of the fingertip. Modern automated fingerprint identification systems (AFIS) primarily rely on minutiae-based matching, which extracts localized features such as ridge endings and bifurcations [10]. While highly accurate and cost-effective due to the proliferation of compact capacitive sensors, fingerprint systems face challenges. Specifically, they can be degraded by skin conditions (e.g., cuts, moisture, wear from manual labor) and are vulnerable to presentation attacks (spoofing) using artificial materials like silicone or gelatine [11].

3.2. Facial Recognition Facial recognition captures the spatial geometry of distinguishing features of the face, such as the distance between the eyes, the shape of the jawline, and the depth of the eye sockets. While early systems relied on principal component analysis (e.g., Eigenfaces), the state-of-the-art is currently dominated by Deep Convolutional Neural Networks (CNNs) [12]. These deep learning models have drastically improved accuracy, even in unconstrained environments. However, facial recognition is highly sensitive to variations in illumination, facial expressions, and occlusions (e.g., masks or sunglasses) [12]. Furthermore, the rise of high-resolution digital imagery has necessitated advanced anti-spoofing techniques to distinguish a live 3D face from a 2D photograph or a sophisticated video playback [13].

3.3. Iris Recognition The iris—the coloured ring of tissue surrounding the pupil—exhibits a highly complex, random, and unique pattern formed during fetal development. Iris recognition systems illuminate the eye with near-infrared (NIR) light to capture these intricate patterns without causing discomfort. Using algorithms such as Daugman's Integro-differential operator, the acquired image is transformed into an "IrisCode," a highly compact mathematical template [14]. Iris recognition offers exceptionally low False Acceptance Rates (FAR) and remains stable throughout a person's lifetime. However, user acceptability can be lower due to the perceived intrusiveness of the scanning process, and performance can degrade if users wear certain types of contact lenses or glasses [14].

3.4. Palm and Finger Vein Pattern Recognition Vein pattern recognition is an advanced modality that captures the vascular network beneath the skin's surface. Hemoglobin in the blood absorbs near-infrared light, allowing sensors to image the dark vein patterns against the lighter surrounding tissue [15]. A significant advantage of vein recognition is its inherent liveness detection: the system naturally verifies the presence of flowing blood, making it exceptionally resistant to spoofing [15]. Furthermore, because the trait is internal, it is not susceptible to the physical wear and tear that degrades fingerprints, making it ideal for high-security applications like banking and healthcare.

4. Behavioural Biometric Modalities

While physiological traits are mostly static, behavioral biometrics measure the patterns in which individuals perform specific actions. These modalities are often heavily influenced by both psychological and physical factors. Their primary advantage lies in their potential for continuous, unobtrusive authentication during a user's normal interaction with a system [16].

4.1. Speaker and Voice Recognition Voice recognition identifies an individual based on their vocal characteristics, which are determined by the physical shape of the vocal tract (physiological) and the learned speaking style (behavioral). Voice systems can be

classified into text-dependent (where the user speaks a predetermined passphrase) and text-independent (where the system verifies identity regardless of the words spoken) [17]. Advanced systems utilize Mel-Frequency Cepstral Coefficients (MFCCs) and Gaussian Mixture Models (GMMs) or Deep Neural Networks to model the speaker's voice [18]. While convenient, particularly for telephonic and smart-home applications, voice recognition is highly susceptible to background noise, illness (which alters the vocal tract), and sophisticated replay attacks or AI-generated voice cloning [19].

4.2. Keystroke Dynamics Keystroke dynamics analyze the rhythmic patterns of a user typing on a keyboard. This modality does not require any specialized hardware, making it highly cost-effective for securing computer workstations. The system evaluates features such as "dwell time" (how long a key is pressed) and "flight time" (the time interval between releasing one key and pressing the next) [20]. Although keystroke dynamics offer excellent potential for continuous, background authentication without interrupting the user, the accuracy can be adversely affected by fatigue, injury, or changes in the typing environment (e.g., switching from a mechanical keyboard to a laptop membrane keyboard) [21].

4.3. Gait Analysis Gait analysis is the systematic study of human locomotion. It aims to identify individuals by the unique way they walk. This is one of the few biometric modalities that can be captured at a distance without the subject's explicit cooperation or awareness, making it highly valuable for surveillance and border security applications [22]. However, gait can be obscured by loose clothing, varying footwear, or changes in walking surface, which complicate the feature extraction process [23].

5. Multimodal Biometric Systems

Despite the advancements in sensor technology and machine learning algorithms, unimodal biometric systems (relying on a single trait) face inherent limitations. These include non-universality (e.g., approximately 2% of the population has unreadable fingerprints), high susceptibility to noisy sensor data, and vulnerability to presentation attacks (spoofing) [24].

To mitigate these shortcomings, multimodal biometric systems have been developed. These systems fuse information from two or more biometric sources (e.g., face and fingerprint, or face and voice) to establish a more reliable and robust identity verification framework [25]. Information fusion in biometrics can occur at several levels:

- **Sensor Level:** Raw data from multiple sensors are combined before processing.
- **Feature Level:** Extracted feature sets from different modalities are concatenated into a single, high-dimensional vector.

- **Score Level:** Match scores from independent biometric matchers are combined using normalization techniques (e.g., Min-Max, Z-score) and fusion rules (e.g., Sum Rule, Product Rule) [26]. This is the most widely adopted approach due to its balance of simplicity and performance improvement.
- **Decision Level:** The final boolean outcomes (Accept/Reject) of individual systems are combined using voting schemes (e.g., majority vote, AND/OR logic) [24].

By leveraging multiple traits, multimodal systems significantly reduce False Acceptance Rates (FAR) and False Rejection Rates (FRR), while exponentially increasing the difficulty for an adversary to successfully spoof the system.

6. Biometric Template Security and Privacy

The most critical vulnerability in any biometric system is the permanent nature of the biometric trait. Unlike a password, which can be instantly revoked and reissued if compromised, a stolen fingerprint or iris pattern is compromised for life [27]. Therefore, the secure transmission and storage of the extracted biometric templates are of paramount importance. Storing raw biometric data or unprotected templates in a centralized database creates a lucrative target for cybercriminals.

To address these vulnerabilities, researchers have proposed various template protection schemes, broadly categorized into cancellable biometrics and biometric cryptosystems. Cancellable biometrics intentionally distort the original biometric signal using a non-invertible mathematical transformation; if the transformed template is stolen, the transformation key is changed, effectively "revoking" the biometric [28]. Biometric cryptosystems, such as the Fuzzy Vault or Fuzzy Extractors, securely bind a cryptographic key with the biometric template, ensuring that neither the key nor the template can be retrieved without the presentation of a matching biometric sample.

Beyond standard cryptographic approaches, steganography and watermarking have proven highly effective for securing biometric data, particularly during transmission over insecure networks. Robust methodologies have been proposed for embedding biometric features into multimedia objects to conceal their existence. For instance, Ntalianis and Tsapatsoulis [29] developed a robust video-object steganographic mechanism that facilitates remote authentication via biometrics over wireless networks, demonstrating high resilience against transmission errors. This aligns with earlier work by Ntalianis et al. [30], which utilized video-object oriented biometrics hiding to ensure reliable user authentication even under error-prone network conditions.

Furthermore, digital watermarking provides an essential layer of security for verifying the integrity and authenticity of biometric templates. Tzouveli, Ntalianis, and Kollias

have contributed significantly to this domain by introducing moment-based watermarking techniques. Their research on video object watermarking based on general moments [31] and human face watermarking utilizing Zernike moments [32] provides mathematically robust frameworks for embedding covert authentication data within visual biometrics. In scenarios requiring even stricter security, the incorporation of chaos-based feedback cryptographic schemes into human video objects has been demonstrated to drastically enhance the security of visual biometric data against unauthorized tampering and extraction [33].

7. Future Trends and Challenges

The biometric landscape is undergoing a rapid transformation, driven by advancements in artificial intelligence, ubiquitous computing, and the proliferation of Internet of Things (IoT) devices [34]. While traditional systems operate on a discrete authentication paradigm (logging in once per session), future frameworks and sophisticated threat vectors demand more dynamic approaches [35].

7.1. Continuous and Implicit Authentication One of the most prominent future trends is the shift from point-of-entry verification to continuous authentication [36]. Instead of relying on a single biometric scan, these systems continuously monitor behavioral traits—such as mouse movements, swiping patterns on touchscreens, and background voice variations—to ensure that the authenticated user remains the legitimate owner of the active session [37]. This zero-trust approach significantly mitigates the risk of session hijacking [38]. However, implementing continuous authentication requires highly efficient algorithms to minimize battery consumption on mobile devices and reduce the computational overhead on edge networks [39].

7.2. Deepfakes and Advanced Presentation Attacks As deep learning models have evolved, so too have the mechanisms used to defeat biometric systems. The emergence of Generative Adversarial Networks (GANs) has led to the creation of "Deepfakes"—highly realistic, AI-generated synthetic media capable of mimicking a person's face, voice, or even gait [40]. Deepfakes pose a critical threat to remote identity verification systems, particularly in financial services and secure remote onboarding [41]. Consequently, the development of advanced Presentation Attack Detection (PAD) and Deepfake detection mechanisms has become a primary research focus [42]. Current state-of-the-art defences employ spatio-temporal analysis and physiological liveness cues (e.g., micro-expressions, remote photoplethysmography to detect a heartbeat) to differentiate between genuine biological samples and synthetic replicas [43].

7.3. Privacy-Preserving Biometrics: Federated Learning and Encryption With the increasing regulatory scrutiny surrounding biometric data privacy (e.g., GDPR), centralized storage of biometric templates is becoming legally and functionally

problematic [44]. To address this, the industry is moving towards decentralized and privacy-preserving frameworks [45]. Federated Learning represents a paradigm shift where biometric models are trained locally on edge devices (like smartphones), and only the updated model weights—rather than the raw biometric data—are shared with the central server [46]. Furthermore, advancements in Fully Homomorphic Encryption (FHE) allow for biometric matching to be performed directly on encrypted templates in the cloud, ensuring that the server never accesses the biometric data in its plain-text form [47].

8. Conclusion

Biometric authentication has undeniably revolutionized the paradigm of identity management, offering a compelling balance of security and user convenience over traditional token- or knowledge-based systems [48]. As explored in this survey, physiological modalities like fingerprints, iris, and facial recognition provide high distinctiveness and permanence, while behavioural traits such as voice and keystroke dynamics offer innovative pathways for seamless, continuous verification [49]. The inherent vulnerabilities of unimodal systems have driven the widespread adoption of multimodal biometric architectures, which leverage information fusion at various levels to achieve superior accuracy and resilience against spoofing attacks [50].

However, the permanent and irrevocable nature of biometric traits dictates that security and privacy cannot be afterthoughts [51]. The catastrophic consequences of a compromised biometric template necessitate the rigorous implementation of advanced protection schemes, including cancellable biometrics, biometric cryptosystems, and robust steganographic/watermarking mechanisms for secure transmission. Looking ahead, the arms race between biometric security and adversarial AI (such as Deepfakes) will intensify [52]. The future of reliable authentication lies not only in capturing biological traits with greater fidelity but in establishing comprehensive, decentralized, and privacy-preserving architectures that protect the fundamental digital identity of the user.

References

- [1] 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, Jan. 2004, doi: 10.1109/TCSVT.2003.818349
- [2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer Science & Business Media, 2009, doi: 10.1007/978-1-84882-254-2
- [3] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and Accuracy of Fingerprint-Based Biometrics: A Review," *Symmetry*, vol. 11, no. 2, p. 141, 2019, doi: 10.3390/sym11020141
- [4] A. K. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognition Letters*, vol. 79, pp. 80-105, 2016, doi: 10.1016/j.patrec.2015.12.013
- [5] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: security and privacy concerns," *IEEE Security & Privacy*, vol. 1, no. 2, pp. 33-42, March-April 2003, doi: 10.1109/MSECP.2003.1193209
- [6] A. Ross and A. K. Jain, "Information fusion in biometrics," *Pattern Recognition Letters*, vol. 24, no. 13, pp. 2115-2125, 2003, doi: 10.1016/S0167-8655(03)00079-5
- [7] 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, Jan. 2004, doi: 10.1109/TCSVT.2003.818349
- [8] J. L. Wayman, "Technical testing and evaluation of biometric identification devices," in *Biometrics*, pp. 345-368, Springer, Boston, MA, 1999, doi: 10.1007/0-306-47044-6_16
- [9] N. L. Clarke and S. M. Furnell, "Authentication of users on mobile telephones—A survey of attitudes and practices," *Computers & Security*, vol. 24, no. 7, pp. 519-527, 2005, doi: 10.1016/j.cose.2005.08.003
- [10] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer Science & Business Media, 2009, doi: 10.1007/978-1-84882-254-2
- [11] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial gummy fingers on fingerprint systems," in *Optical Security and Counterfeit Deterrence Techniques IV*, vol. 4677, pp. 275-289, SPIE, 2002, doi: 10.1117/12.462719
- [12] M. Wang and W. Deng, "Deep face recognition: A survey," *Neurocomputing*, vol. 429, pp. 215-244, 2021, doi: 10.1016/j.neucom.2020.10.081

- [13] J. Galbally, S. Marcel, and J. Fierrez, "Biometric antispoofing methods: A survey in face recognition," *IEEE Access*, vol. 2, pp. 1530-1552, 2014, doi: 10.1109/ACCESS.2014.2381273
- [14] J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1148-1161, Nov. 1993, doi: 10.1109/34.244676
- [15] J. G. Wang, W. Y. Yau, A. Suwandy, and E. Sung, "Person recognition by integrating palmprint and palm vein," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 21-33, March 2008, doi: 10.1109/TIFS.2007.916281
- [16] A. Ross and A. K. Jain, "Multimodal biometrics: An overview," in *Proceedings of the 12th European Signal Processing Conference*, pp. 1221-1224, 2004, doi: 10.5281/zenodo.41434
- [17] D. A. Reynolds, "An overview of automatic speaker recognition technology," *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, vol. 4, pp. 4072-4075, 2002, doi: 10.1109/ICASSP.2002.1005735
- [18] T. Kinnunen and H. Li, "An overview of text-independent speaker recognition: From features to supervectors," *Speech Communication*, vol. 52, no. 1, pp. 12-40, 2010, doi: 10.1016/j.specom.2009.08.009
- [19] P. L. De Leon, M. Pucher, J. Yamagishi, I. Hernaez, and I. Saratxaga, "Evaluation of speaker verification security and detection of HMM-based synthetic speech," *IEEE Transactions on Audio, Speech, and Language Processing*, vol. 20, no. 8, pp. 2280-2290, 2012, doi: 10.1109/TASL.2012.2201472
- [20] F. Monroe and A. D. Rubin, "Keystroke dynamics as a biometric for authentication," *Future Generation Computer Systems*, vol. 16, no. 4, pp. 351-359, 2000, doi: 10.1016/S0167-739X(99)00059-X
- [21] S. P. Banerjee and D. L. Woodard, "Biometric authentication and identification using keystroke dynamics: A survey," *Journal of Pattern Recognition Research*, vol. 7, no. 1, pp. 116-139, 2012, doi: 10.13176/11.427
- [22] M. S. Nixon, T. Tan, and R. Chellappa, *Human identification based on gait*, Springer Science & Business Media, 2010, doi: 10.1007/978-0-387-29488-9
- [23] Y. Makiyara, H. Mannami, A. Tsuji, W. A. Hossain, K. Sugiura, A. Mori, and Y. Yagi, "The OU-ISIR gait database comprising the treadmill dataset," *IPSI Transactions on Computer Vision and Applications*, vol. 4, pp. 53-62, 2012, doi: 10.2197/ipsjtcva.4.53

- [24] A. K. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," *Pattern Recognition*, vol. 38, no. 12, pp. 2270-2285, 2005, doi: 10.1016/j.patcog.2005.01.012
- [25] R. Snelick, U. Uludag, A. Mink, M. Indovina, and A. Jain, "Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 27, no. 3, pp. 450-455, 2005, doi: 10.1109/TPAMI.2005.57
- [26] J. Fierrez-Aguilar, J. Ortega-Garcia, D. Garcia-Romero, and J. Gonzalez-Rodriguez, "Audio-visual document authentication with score fusion," *Speech Communication*, vol. 44, no. 1-4, pp. 161-174, 2004, doi: 10.1016/j.specom.2004.10.007
- [27] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614-634, 2001, doi: 10.1147/sj.403.0614
- [28] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948-960, 2004, doi: 10.1109/JPROC.2004.827372
- [29] K. Ntalianis and N. Tsapatsoulis, "Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks," in *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 1, pp. 156-174, Jan.-March 2016, doi: 10.1109/TETC.2015.2400135
- [30] K. Ntalianis, N. Tsapatsoulis, and A. Drigas, "Video-object oriented biometrics hiding for user authentication under error-prone transmissions," *EURASIP Journal on Information Security*, vol. 2011, pp. 1-17, 2011, doi: 10.1155/2011/174945
- [31] P. K. Tzouveli, K. S. Ntalianis, and S. D. Kollias, "Video object watermarking based on moments," in *Lecture Notes in Computer Science*, vol. 4306, pp. 574-585, 2006, doi: 10.1007/11738695_10
- [32] P. Tzouveli, K. Ntalianis, and S. Kollias, "Human face watermarking based on Zernike moments," in *Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology*, pp. 884-889, 2005, doi: 10.1109/ISSPIT.2005.1577130
- [33] P. K. Tzouveli, K. Ntalianis, and S. Kollias, "Security of human video objects by incorporating a chaos-based feedback cryptographic scheme," in *Proceedings of the 12th ACM International Conference on Multimedia*, pp. 315-318, 2004, doi: 10.1145/1027527.1027609

- [34] A. K. Jain, S. Prabhakar, and A. Ross, "Biometrics: A grand challenge," *International Conference on Pattern Recognition*, vol. 2, pp. 935-942, 2004, doi: 10.1109/ICPR.2004.1334458
- [35] M. S. Hossain, "Cloud-supported cyber-physical localization framework for patients monitoring," *IEEE Systems Journal*, vol. 11, no. 1, pp. 118-127, 2015, doi: 10.1109/JSYST.2015.2470644
- [36] H. Feng, K. Fawaz, and K. G. Shin, "Continuous authentication for voice assistants," *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, pp. 343-355, 2017, doi: 10.1145/3117811.3117823
- [37] N. L. Clarke and S. M. Furnell, "Advanced user authentication for mobile devices," *Computers & Security*, vol. 26, no. 2, pp. 109-119, 2007, doi: 10.1016/j.cose.2006.08.008
- [38] T. Feng, Z. Liu, K. A. Kwon, W. Shi, V. Carbunar, Y. Jiang, and N. Nguyen, "Continuous mobile authentication using touchscreen gestures," *IEEE Conference on Homeland Security*, pp. 1-6, 2012, doi: 10.1109/THS.2012.6459351
- [39] E. Maioranca, C. Campolo, A. Molinaro, and A. Iera, "Continuous Authentication in the Internet of Things: A Survey," *IEEE Access*, vol. 9, pp. 165686-165706, 2021, doi: 10.1109/ACCESS.2021.3134954
- [40] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, "Deepfakes and beyond: A Survey of face manipulation and fake detection," *Information Fusion*, vol. 64, pp. 131-148, 2020, doi: 10.1016/j.inffus.2020.06.014
- [41] T. T. Nguyen, C. M. Nguyen, D. T. Nguyen, D. T. Nguyen, and S. Nahavandi, "Deep learning for deepfakes creation and detection: A survey," *Computer Vision and Image Understanding*, vol. 223, p. 103525, 2022, doi: 10.1016/j.cviu.2022.103525
- [42] S. Marcel, M. S. Nixon, J. Fierrez, and N. Evans, *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection*, Springer, 2019, doi: 10.1007/978-3-319-92627-8
- [43] Y. Li, M. C. Chang, and S. Lyu, "In Ictu Oculi: Exposing AI created fake videos by detecting eye blinking," *IEEE International Workshop on Information Forensics and Security (WIFS)*, pp. 1-7, 2018, doi: 10.1109/WIFS.2018.8630787
- [44] P. Campisi, *Security and Privacy in Biometrics*, Springer Science & Business Media, 2013, doi: 10.1007/978-1-4471-5230-9
- [45] A. Natarajan and S. C. Tai, "A Survey on Privacy-Preserving Biometric Authentication Systems," *IEEE Access*, vol. 9, pp. 147814-147833, 2021, doi: 10.1109/ACCESS.2021.3123862

- [46] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Processing Magazine*, vol. 37, no. 3, pp. 50-60, 2020, doi: 10.1109/MSP.2020.2975749
- [47] J. R. Troncoso-Pastoriza and F. Pérez-González, "Secure signal processing in the cloud: enabling technologies for privacy-preserving multimedia cloud processing," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 29-41, 2013, doi: 10.1109/MSP.2012.2230225
- [48] C. Roberts, "Biometrics," *IEEE Security & Privacy*, vol. 5, no. 3, pp. 46-49, 2007, doi: 10.1109/MSP.2007.69
- [49] A. K. Jain, P. Flynn, and A. A. Ross, *Handbook of Biometrics*, Springer Science & Business Media, 2007, doi: 10.1007/978-0-387-71041-9
- [50] R. Singh, M. Vatsa, and A. Noore, "Multimodal biometric systems: A review," *Biometrics: Theory, Applications, and Systems*, pp. 1-6, 2007, doi: 10.1109/BTAS.2007.4401918
- [51] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 54-65, 2015, doi: 10.1109/MSP.2015.2434151
- [52] K. W. Bowyer, "Biometric recognition: An evolving landscape," *Pattern Recognition Letters*, vol. 33, no. 14, pp. 1827-1830, 2012, doi: 10.1016/j.patrec.2012.06.011

