Biometric Systems De-Identification

Subjects: Computer Science, Cybernetics

Contributor: Md Shopon, Sanjida Tumpa, Marina Gavrilova

Biometric de-identification is an emerging topic of research within the information security domain that integrates privacy considerations with biometric system development. A comprehensive overview of research in the context of authentication applications spanning physiological, behavioral, and social-behavioral biometric systems and their privacy considerations is discussed. Three categories of biometric de-identification are introduced, namely complete de-identification, auxiliary biometric preserving de-identification, and traditional biometric preserving de-identification. An overview of biometric de-identification in emerging domains such as sensor-based biometrics, social behavioral biometrics, psychological user profile identification, and aesthetic-based biometrics is presented. The article provides a rich avenue for subsequent explorations of biometric de-identification in the context of information privacy.

Keywords: human identity ; privacy preservation ; biometric security

1. Emerging Types of Biometric De-Identification

We now introduce additional types of de-identification related to emerging biometric research domains. These include sensor-based de-identification, social behavioral biometrics, emotion-based biometrics, and personality traits de-identification.

1.1. Sensor-Based Biometric De-Identification

Sensor-based Biometric De-identification: Sensor-based biometric de-identification can be defined as the introduction of perturbation in sensor-based biometric data to obfuscate either traditional or auxiliary biometric traits or both of them.

Some of the common sensor-based biometrics involve gait sequences and brain signals. Motions of a subject's body joints, while they are walking, represent their gait sequence, and they can be captured using RGB cameras or wearable sensors such as an accelerometer and a gyroscope or a marker-based sensor such as Vicon or a marker-less sensor such as Kinect or a combination thereof [1][2]. Brain signals are captured using an Electroencephalogram (EEG). EEG measures electrical impulses from several electrodes that are attached to the subject's scalp. The device can directly measure neuronal activity and is the most effective method for measuring neurons [3]. In the gait recognition domain, a biometric de-identification system can be designed by considering the gait as a primary behavioral biometric and the estimations of age, gender, emotion, or activity as auxiliary biometrics [2][4][5]. Furthermore, spatial and temporal features extracted over the gait sequence can act as the distinguishing characteristics for the identification of primary and auxiliary biometrics. For brain signal de-identification, a person's identity can remain recognizable while the information about their underlying emotions can be obfuscated.

Widespread deployment of sensors in both indoor and outdoor settings resulted in the application development based on biometric characteristics in domains such as kinesiology, physical rehabilitation, smart-home design, and search-and-rescue operations [6][7][8]. The appropriate architectural design of the biometric system can enable primary biometric identification and auxiliary biometric estimation. Therefore, perturbations need to be introduced in the data in order to obfuscate either the primary biometric trait or auxiliary biometric traits or both to ensure biometric de-identification. Prior research conceals auxiliary biometric traits while preserving primary biometric traits within the data by introducing a deep learning-based neural style transfer [9]. Obscuring auxiliary biometric traits such as age, gender, activity, and emotion, while retaining the ability to identify a person using their gait can be a topic of future work in sensor-based biometric de-identification. Additionally, perturbing gait sequences to prevent gait-based identification while preserving the auxiliary biometric traits can be another future direction of research. The performance of the de-identification methods of each of the future works can be evaluated by using the established primary and auxiliary biometric identification and estimation methodologies.

The methods for identifying the primary biometric or for estimating the auxiliary biometric traits are available in the literature [10]. A deep learning-based approach, such as Generative Adversarial Network (GAN) [11], can be utilized to obtain the optimal perturbation scheme for sensor-based biometric data. In this method, the generator architecture of the network would be responsible for the perturbation and the discriminator architecture would handle the estimation of the primary and auxiliary biometric traits. The architecture of a gait-based behavioral biometric de-identification system is shown in **Figure 2**. The GAN is trained for the person identification task using either the primary biometric traits or auxiliary biometric traits depending on the desired de-identification mode. The random gait sequences which are perturbed using the generator network are passed into two discriminators, which are distinctly responsible for primary biometric de-identification and auxiliary biometric de-identification. The two discriminators are responsible for different tasks: one is to determine the person's Identity based on gait sequence and another is to estimate age, gender, or emotion from the gait. In the current system, both discriminators are executed. However, there could be a different system envisioned where only one of the discriminators is invoked.

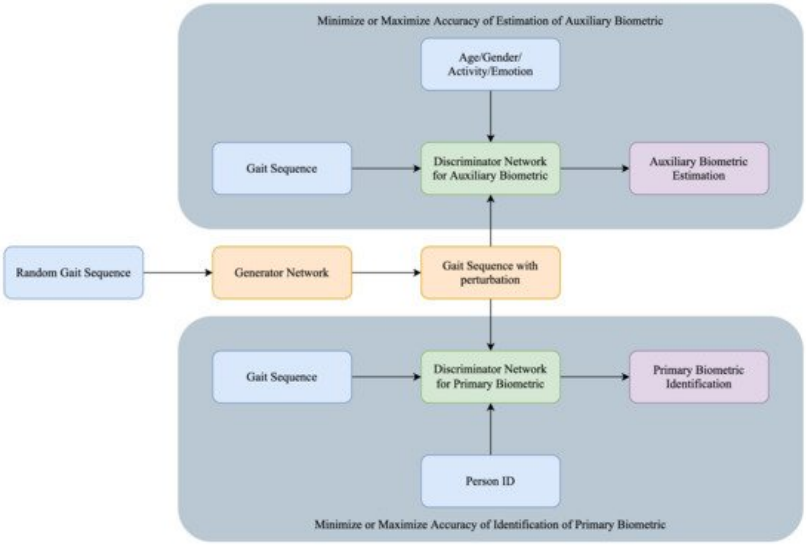

Figure 2. Architecture of gait-based biometric system that can identify both primary gait and auxiliary biometric traits.

In [12], the researchers proposed a method for person identification through gait videos. They found that wearing accessories introduce variations in an individual's gait patterns. Hence, they designed the identification system to handle gait sequences of a person wearing a jacket, holding a bag, or having a specific type of footwear. Hence, another approach to de-identify gait sequences can be used to alter the appearance of the subject by adding artificial accessories using GNNs. This might preserve the original gait information for emotion recognition while perturbing the soft biometric traits. **Table 1** summarizes the above mentioned sensor-based identification and de-identification research studies.

Table 1. Summary of sensor-based identification and de-dentification methods.

Authors	Year	Biometrics	De-Identified Biometrics	Unchanged Biometrics	Accuracy of Recognition
Ahad et al. [2]	2012	Gait	None	All biometrics	24.23% prediction error for gender estimation and 5.39 mean absolute error for age estimation
Iwashita et al. [12]	2013	Gait	None	All biometrics	94.0% on gait recognition
Brkić et al. [9]	2016	Full body	All traditional and soft biometrics	None	Qualitative evaluation
Xu et al. [13]	2017	Gait	None	All biometrics	8.92% mean absolute error on age estimation
Bari et al. [4]	2019	Gait	None	All biometrics	98.08% on person identification
Ahmed et al. [5]	2019	Gait	None	All biometrics	86.67% on emotion recognition

1.2. Emotion-Based De-Identification

Emotion-based de-idetification: Emotion-based biometric de-identification can be defined as the introduction of perturbation in emotion to obfuscate either traditional or auxiliary biometric traits or both of them.

Emotions are one of the most common auxiliary data that are frequently extracted from a human face; however, they can also be deduced from gait and speech [14]. For instance, the authors of [15] proposed a novel method to de-identify faces and the soft biometrics while retaining emotions. They highlighted the difference between their proposed method and naive approaches, such as blurring, pixelization, blindfolding, and inversion of the face images. Their adaptive filtering algorithm smoothed the facial details until the software-based authentication rate fell to approximately half of the original and the human recognition rate.

Thus, the authors of [16] masked original faces with donor-faces to de-identify an image of the original subject. The results show that emotions such as disgust, surprise, and neutrality are preserved 100% of the time, while anger and sadness are preserved more than 98% of the time. Lastly, fear and happiness are preserved only 79% of the time. Similarly, other works used Generative Neural Networks (GNNs) to mask original faces by using donor faces while preserving emotion [17].

The above research studies aimed to preserve emotion while concealing identities. A dual problem of concealing emotion while preserving identity is also possible for consideration. The authors of [18] used Cycle Generative Adversarial Networks (Cycle GANs) to transform a person's voice to hide emotions while retaining the ability for personal identification and speech recognition. Another less common parameter that can be estimated from a face is the body mass of a person [19].

Biometrics such as gait, Electroencephalogram (EEG), and Electrocardiography (ECG) are also gaining popularity for the emotion recognition problem and being researched for personal identification [3][12][20]. Since recognition methods involving these biometric traits are not studied as extensively as facial biometrics, experiments aimed at de-identification of these biometric traits have rarely been conducted. The particular biometric features that play a vital role in person identification are still uncertain; hence, not many have attempted to leverage those features. In [21], features responsible for human activity recognition were compared by using different machine learning methods. In [5], novel techniques for identifying the most significant gait features for emotion recognition were proposed. Such works can be extended to learn important features required for gait-based person identification. Therefore, the features exclusively important for identification can be suppressed to achieve de-identification. Recently, many works attempt to identify person age from their biometrics. Notably, a recent attempt based on gait is presented in [13]. De-identifying age while preserving gait can be a new direction of research. **Table 2** demonstrates the works that were performed on emotion-based identification and de-identification.

Table 2. Summary of emotion-based identification and de-identification methods.

Authors	Year	Biometrics	De-Identified Biometrics	Unchanged Biometrics	Accuracy of Recognition
Letournel et al. [15]	2015	Face	Face	Expression	56.4% on re-identification
Jyotishi et al. [20]	2016	ECG Signal	None	All biometrics	97.3% on person identification
Meden et al. [17]	2018	Face	Face	Emotion	0.016% on re-identification
Li et al. [16]	2019	Face	Face	Emotion	16.5% on re-identification
Aloufi et al. [18]	2019	Voice	Emotion	All remaining biometrics	4.00% on re-identification
Ahmed et al. [5]	2019	Gait	None	All biometrics	86.67% on emotion recognition

Future work in the domain of emotion-based de-identification can include investigations of other biometrics such as voice, signature, or a communication style in the presence of emotion-revealing traits.

1.3. Social Behavioral Biometrics-Based De-Identification

Social Behavioral Biometrics-based De-identification: Social behavioral biometrics-based de-identification can be defined as obscuring either traditional or auxiliary social behavioral biometric traits or both of them to hide the identity of the users.

As social beings, people communicate and interact with each other. Online social networking (OSN) platforms have evolved to become important extensions of the social fabric. Platforms such as Facebook, Instagram, Snapchat, LinkedIn, and Twitter, etc., emulate various facets of everyday social interactions within the personal, professional, and public

realms of our society. According to the definition of Social Behavioral Biometrics (SBB), these social interactions possess many unique features that can be used as the person's biometric signature [22]. Social behavioral patterns provide important biometric cues and hold discriminating capabilities with regards to an individual's identity [22]. The area of social behavioral biometrics aims to model distinguishing characteristics that manifest within a subject's soft-biometric traits such as the patterns in their behaviors, social interactions, and communications. Over recent years, increased adoption and usage of online social platforms has meant that its users leave an ever-increasing trail of digital footprints in the form of the content they share or the patterns in their interactions with other users and the platform. Therefore, privacy preservation of these identifiable digital footprints is required in order to protect users' privacy. SBB-based de-identification refer to the original SBB traits and prevent person-identification.

The concept of Social Behavioral Biometrics (SBB) was introduced by Sultana et al. in 2015 [22]. The weighted networks are generated from the shared URLs, hashtags, retweeted, replied acquaintances, and the tweeting pattern of the users. Li et al. proposed a user identification method across social networks based on the k-hop ($k > 1$) friendship networks by considering the uniqueness of friendship networks [23]. Brocardo et al. proposed a method using the Gaussian–Bernoulli deep belief network to capture the writing style of the users obtained from the lexical, syntactic, and application-specific features for continuous user authentication of Twitter [24]. More recently, Tumpa et al. proposed an SBB system for user identification using users' linguistic profiles by applying score and rank level fusion [25].

Social Behavioral Biometrics de-identification is a new research avenue. For complete de-identification, all traditional and auxiliary SBB features must be obscured or masked. For example, one of the traditional SBB features is linguistic profiles. The linguistic profile of a user can be masked by hiding the writing style of a user, which also changes the sentiment and emotion of the written contents [26]. Thus, both traditional and auxiliary features are obscured. In the case of auxiliary biometrics preserving de-identification, the sentiments of a user's tweets can be preserved while changing the vocabularies of the tweets. The identity of the user cannot be identified by using the traditional biometric, namely linguistic profile as this profile depends on the user's vocabulary for identification. However, the tweets deliver the same messages with the exact sentiments as the auxiliary biometrics are preserved. If the tweets of a user can be changed in such a way that a machine is able to retrieve the original tweets but a human cannot, then this de-identification is considered to be an auxiliary biometrics preserving utility retained de-identification. For the traditional biometric preserving de-identification, the sentiment from a tweet can be removed so that others will obtain the information expressed in the tweet but will not understand the sentiment of the user from that tweet. The examples are discussed considering linguistic profile as traditional biometric and sentiment as auxiliary biometric. A similar idea can be applied by considering the reply, retweet, URL, or hashtag network as traditional and tweeting behavior or emotion as auxiliary biometrics. The de-identification of SBB systems will help to preserve the privacy of the users without interrupting the legal use of information. **Table 3** summarizes the works that were performed on social behavioral biometrics identification.

Table 3. Summary of social behavioral biometrics-based identification methods.

Authors	Year	Biometrics	De-Identified Biometrics	Unchanged Biometrics	Accuracy of Recognition
Wu et al. [26]	2006	Writing style	None	All	72.43% on person identification
Brocardo et al. [24]	2019	Writing style	None	All	23.49% on user verification
Tumpa et al. [25]	2020	Linguistic profile	None	All	99.45% on person identification
Li et al. [23]	2020	Twitter friendship networks	None	All	94.83% on user identification

2. Application Domains

This section summarizes the above discussion by providing a gamut of applications of emerging de-identification research.

Cybersecurity: Gathering intelligence by surveilling suspects in cyberspace is necessary to maintain a secure internet [27]. Government-authorized agents have been known to survey the social networks, disguising themselves among malicious users. Social behavioral biometrics-based de-identification can aid security agents in the covert observation and anonymous moderation of cyberspaces.

Continuous Authentication: Continuous authentication refers to a technology that verifies users on an ongoing basis to provide identity confirmation and cybersecurity protection [28]. Social behavioral biometrics (SBB) authenticates users on social networking sites continuously without any active participation of the users. The templates of users' writing patterns and acquaintance networks information must be stored in the database for SBB authentication. Instead of storing the identifying templates directly, SBB-based de-identification techniques can be applied to the templates to ensure account security and user privacy.

Protecting Anonymity: Authorized officials often publish case studies and written content of cybercrime victims to create public awareness [29]. In such cases, social networking portals and blogs are used as convenient media to disseminate information. Typically, the identities of the victims are kept anonymous. However, the content written by the victim and their social behavioral patterns may still contain identifying information. Therefore, de-identification of these published materials helps protect user anonymity when their identity must be kept confidential.

Multi-Factor Authentication: Leveraging the discriminative ability of an individual's social data and psychological information, a multi-factor authentication system can be implemented [30]. As a remote and accessible biometric, aesthetic identification can also provide additional security if the primary modality is suspected to be compromised. De-identification in this context would preserve the security of the system when storing a user's preference template.

Video Surveillance: Anonymization of primary or auxiliary biometric data protects the privacy of the subjects. If the original biometric is perturbed such that primary biometric identification is successful while the auxiliary biometric traits are not easily recognizable, or vice versa, this solution can be integrated with surveillance methods [31]. In such a situation, the de-identification of primary biometric can ensure the data privacy of individuals who appear in the footage but are not persons-of-interest.

Risk Analysis: The ability to estimate a person's emotional state using the facial biometric or gait analysis finds potential applications in threat-assessment and risk analysis [32]. Analysis of emotional state can be applied in the surveillance of public places in order to estimate the threat posed by an individual based on continuous monitoring of their emotional state. Based on the necessity of data protection, primary biometrics can be obscured while preserving the auxiliary information about emotions.

Health Care: Individuals can exhibit postural problems which could be diagnosed through static posture and gait analysis [33]. In such a case, primary gait biometric can be readily de-identified while preserving auxiliary biometric traits, such as age, gender, activity, and emotion.

Mental illness: Many applications predict and identify mental and/or physical illnesses by monitoring user emotions [5]. De-identifying any sensitive patient biometric data using the methods in the applications discussed above would ensure patient privacy, which could increase their willingness to opt-in for such services.

Adaptive Caregiving: The ability of an intelligent system to analyze user emotion information and exhibit realistic interactions has high potential [5]. De-identification of identity while still recognizing client emotions can preserve client privacy.

Advertisement: One reason why many social media companies mine their users' data is to identify customer interests and gain insights that can drive sales [34]. Naturally, this raises concerns with regards to user data ownership and privacy. De-identifying the corresponding sensitive data while still understanding user's preferences towards certain products can supplement data mining.

Entertainment: Another possible usage of social behavioral information is adaptive entertainment experiences [35]. For instance, movies and/or video games that change the narrative based on the user's emotional responses can be created. However, such applications require the storage and analysis of user information. Users might be more willing to participate when user data are protected and anonymized.

Psychology: Personality traits can be revealed from the digital footprints of the users [6]. A personality trait de-identification system can be used to protect sensitive user information and implement privacy-preserving user identification systems. Furthermore, this concept can be applied in user behavior modeling problems such as predicting the likeliness to take a particular action, for example, clicking on a particular ad. Moreover, personality traits-based de-identification can be used in conjunction with other privacy-preserving measures such as data anonymization to further ensure user privacy protection within OSNs.

Consumer Services: Replacement of traditional identification cards by biometrics is the future of many establishments, such as driver license offices or financial services. De-identification of some real-time information obtained by security cameras for identity verification would ensure additional protection relative to sensitive user data [36].

3. Open Problems

The domain of biometric de-identification remains largely unexplored and has many promising avenues for further research. The impact of the perturbation in the original data on the identification of primary biometric and the estimation of auxiliary biometric can be further investigated. Moreover, the design of innovative deep learning architectures for sensor-based biometric de-identification can result in the development of a practical solutions for privacy preserving video surveillance systems. The acceptable obscureness of biometric data while preserving other biometric is open to discussion. Since certain behavioral biometrics may change over time, the procedure to adapt with the updated behavioral biometric in biometric de-identification requires further analysis in the future.

De-identification approaches for gait and gesture rely heavily on the blurring technique. In this scenario, retaining the naturalness of the de-identified video after the individual's characteristic walking patterns are obscured is one of the main challenges in gait and gesture de-identification. This represents one of the interesting open problems in the domains of gait and gesture de-identification.

Research in emotion-preserving de-identification has been more prevalent with faces than with any other biometric. For gait, EEG, and ECG, which are the most significant features for person identification, are unknown. Hence, the first step with these biometrics will be to identify the biometric features that are crucial for personal identification. Consequently, methods must be developed to obscure any personally identifiable information while retaining the features that represent the subject's emotion in the data. Additionally, face emotion-based de-identification research has produced some promising results. Hence, increasing person identification error is a likely future research direction for emotion preservation-based facial emotion recognition systems.

In the domain of social behavioral biometrics, de-identifying friendship and acquaintance networks is an open problem. The technique of changing the linguistic patterns of social media tweets while preserving emotions and information, and vice versa, has not been explored previously. The reversibility to the original SBB traits after de-identification and subsequent measures to increase the difficulty of reverse-engineering those traits are other interesting problems to explore.

There are many open problems in applying the concept of psychological trait-based de-identification within the domain of privacy-preserving social behavioral biometrics. While clinical research indicates the permanence of psychological traits among adults, they change over time due to significant life events and circumstances. Considering time dependencies and their effect on data preservation is another interesting open problem.

Psychological traits factorize a wide range of human behaviors into a fixed number of labels. Therefore, any de-identification of psychological traits may result in the loss of a nuanced representation of user-generated content. This loss of information may reduce the accuracy of the downstream prediction task. Mitigating this unwanted effect is one of the open problems. Secondly, the degree to which a dataset is de-identified may not be directly measurable. As humans may not be capable of inferring psychological traits from user content, it is difficult to ascertain if the information regarding psychological traits is truly obfuscated from automated systems. This is another interesting problem that should be investigated further.

Finally, multi-modal biometric de-identification has not been explored before. Common multi-modal biometric authentication systems involve combining traditional biometric traits with emerging biometric traits using information fusion. One potential open problem is to design a multi-modal de-identification system that conceals soft biometric traits. As there can be several fusion methods for combining biometric modalities, experiments aimed at finding the most suitable architecture in the context of an applied problem are needed. For multi-modal de-identification, some applications may require all the biometric traits to be obscured, while some may need only particular traits to be modified. Formalizing the underlying principles for the optimal design of multi-modal biometric systems offers a rich avenue for future investigations.

References

1. Tao, W.; Liu, T.; Zheng, R.; Feng, H. Gait analysis using wearable sensors. Sensors 2012, 12, 2255–2283.
2. Ahad, M.A.R.; Ngo, T.T.; Antar, A.D.; Ahmed, M.; Hossain, T.; Muramatsu, D.; Makihara, Y.; Inoue, S.; Yagi, Y. Wearable sensor-based gait analysis for age and gender estimation. Sensors 2020, 20, 2424.
3. Ismail, W.W.; Hanif, M.; Mohamed, S.; Hamzah, N.; Rizman, Z.I. Human emotion detection via brain waves study by using electroencephalogram (EEG). Int. J. Adv. Sci. Eng. Inf. Technol. 2016, 6, 1005–1011.
4. Bari, A.H.; Gavrilova, M.L. Artificial neural network based gait recognition using kinect sensor. IEEE Access 2019, 7, 162708–162722.
5. Ahmed, F.; Bari, A.H.; Gavrilova, M.L. Emotion recognition from body movement. IEEE Access 2019, 8, 11761–11781.
6. Tumpa, S.N.; Kumar, K.P.; Sultana, M.; Hsu, G.S.J.; Yadid-Pecht, O.; Yanushkevich, S.; Gavrilova, M.L. Social Behavioral Biometrics in Smart Societies. In Advancements in Computer Vision Applications in Intelligent Systems and Multimedia Technologies; IGI Global: Hershey, PA, USA, 2020; pp. 1–24.
7. Tang, Y.; Teng, Q.; Zhang, L.; Min, F.; He, J. Layer-wise training convolutional neural networks with smaller filters for human activity recognition using wearable sensors. IEEE Sens. J. 2020, 21, 581–592.
8. Ahmed, F.; Polash Paul, P.; Gavrilova, M.L. Kinect-based gait recognition using sequences of the most relevant joint relative angles. J. WSCG 2015, 23, 147–156.
9. Brkić, K.; Sikirić, I.; Hrkać, T.; Kalafatić, Z. De-identifying people in videos using neural art. In Proceedings of the 2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA), Oulu, Finland, 12–15 December 2016; pp. 1–6.
10. Ribaric, S.; Ariyaeeinia, A.; Pavesic, N. De-identification for privacy protection in multimedia content: A survey. Signal Process. Image Commun. 2016, 47, 131–151.
11. Goodfellow, I.; Pouget-Abadie, J.; Mirza, M.; Xu, B.; Warde-Farley, D.; Ozair, S.; Courville, A.; Bengio, Y. Generative adversarial nets. Adv. Neural Inf. Process. Syst. 2014, 27. Available online: https://papers.nips.cc/paper/2014/file/5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf (accessed on 15 August 2021).
12. Iwashita, Y.; Uchino, K.; Kurazume, R. Gait-based person identification robust to changes in appearance. Sensors 2013, 13, 7884–7901.
13. Xu, C.; Makihara, Y.; Ogi, G.; Li, X.; Yagi, Y.; Lu, J. The OU-ISIR gait database comprising the large population dataset with age and performance evaluation of age estimation. IPSJ Trans. Comput. Vis. Appl. 2017, 9, 1–14.
14. El Ayadi, M.; Kamel, M.S.; Karray, F. Survey on speech emotion recognition: Features, classification schemes, and databases. Pattern Recognit. 2011, 44, 572–587.
15. Letournel, G.; Bugeau, A.; Ta, V.T.; Domenger, J.P. Face de-identification with expressions preservation. In Proceedings of the 2015 IEEE International Conference on Image Processing (ICIP), Quebec City, QC, Canada, 27 September–1 October 2015; pp. 4366–4370.
16. Li, Y.; Lyu, S. De-identification without losing faces. In Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, Paris, France, 3–5 July 2019; pp. 83–88.
17. Meden, B.; Emeršič, Ž.; Štruc, V.; Peer, P. k-Same-Net: k-Anonymity with generative deep neural networks for face deidentification. Entropy 2018, 20, 60.
18. Aloufi, R.; Haddadi, H.; Boyle, D. Emotionless: Privacy-preserving speech analysis for voice assistants. arXiv 2019, arXiv:1908.03632.
19. Wen, L.; Guo, G. A computational approach to body mass index prediction from face images. Image Vis. Comput. 2013, 31, 392–400.
20. Jyotishi, D.; Dandapat, S. An LSTM-Based Model for Person Identification Using ECG Signal. IEEE Sens. Lett. 2020, 4, 1–4.
21. Li, F.; Shirahama, K.; Nisar, M.A.; Köping, L.; Grzegorzek, M. Comparison of Feature Learning Methods for Human Activity Recognition Using Wearable Sensors. Sensors 2018, 18, 679.
22. Sultana, M.; Paul, P.P.; Gavrilova, M. Social behavioral biometrics: An emerging trend. Int. J. Pattern Recognit. Artif. Intell. 2015, 29, 1556013.
23. Li, Y.; Su, Z.; Yang, J.; Gao, C. Exploiting similarities of user friendship networks across social networks for user identification. Inf. Sci. 2020, 506, 78–98.

24. Brocardo, M.L.; Traore, I.; Woungang, I. Continuous authentication using writing style. In Biometric-Based Physical and Cybersecurity Systems; Springer: Berlin, Germany, 2019; pp. 211–232.
25. Tumpa, S.N.; Gavrilova, M.L. Score and Rank Level Fusion Algorithms for Social Behavioral Biometrics. IEEE Access 2020, 8, 157663–157675.
26. Wu, C.H.; Chuang, Z.J.; Lin, Y.C. Emotion recognition from text using semantic labels and separable mixture models. ACM Trans. Asian Lang. Inf. Process. (Talip) 2006, 5, 165–183.
27. Sarker, I.H.; Kayes, A.; Badsha, S.; Alqahtani, H.; Watters, P.; Ng, A. Cybersecurity data science: An overview from machine learning perspective. J. Big Data 2020, 7, 1–29.
28. Deutschmann, I.; Nordström, P.; Nilsson, L. Continuous authentication using behavioral biometrics. IT Prof. 2013, 15, 12–15.
29. Jones, L.M.; Finkelhor, D.; Beckwith, J. Protecting victims' identities in press coverage of child victimization. Journalism 2010, 11, 347–367.
30. Dasgupta, D.; Roy, A.; Nag, A. Multi-factor authentication. In Advances in User Authentication; Springer: Berlin, Germany, 2017; pp. 185–233.
31. Sreenu, G.; Durai, M.S. Intelligent video surveillance: A review through deep learning techniques for crowd analysis. J. Big Data 2019, 6, 1–27.
32. Mason, J.E.; Traoré, I.; Woungang, I. Applications of gait biometrics. In Machine Learning Techniques for Gait Biometric Recognition; Springer: Berlin, Germany, 2016; pp. 203–208.
33. Ahmed, F.; Bari, A.H.; Sieu, B.; Sadeghi, J.; Scholten, J.; Gavrilova, M.L. Kalman filter-based noise reduction framework for posture estimation using depth sensor. In Proceedings of the 2019 IEEE 18th International Conference on Cognitive Informatics & Cognitive Computing (ICCI* CC), Milan, Italy, 23–25 July 2019; pp. 150–158.
34. Bhowmik, A.; Gafur, S.R.; Rafid, A.; Azad, S.; Mahmud, M.; Kaiser, M.S. User Awareness for Securing Social Networks. In Securing Social Networks in Cyberspace; CRC Press: Boca Raton, FL, USA, 2021; pp. 3–15.
35. Wong, K.K.W. Player adaptive entertainment computing. In Proceedings of the 2nd International Conference on Digital Interactive Media in Entertainment and Arts, Perth, Australia, 19–21 September 2007; p. 13.
36. Mrityunjay, M.; Narayanan, P. The de-identification camera. In Proceedings of the 2011 Third National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG), Hubli, India, 15–17 December 2011; pp. 192–195.
