This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

Person de-Identification: A Comprehensive Review of Methods, Datasets, Applications, and Ethical Aspects Along-With New Dimensions

Wasiq. Khan, *Senior Member, IEEE,* Luke. Topham, Umar. Khayam, Sandra. Ortega-Martorell, Panter. Heather, Darren Ansell, Dhiya. Al-Jumeily, *Senior Member, IEEE,* and Abir. Hussain, *Senior Member, IEEE*

Abstract—Person de-identification has become a challenging problem that is receiving substantial attention because of the growing demand for privacy protection and related regulations. In this context, computer vision and Deep Learning (DL) algorithms offer automated solutions for Face de-identification (FDeID), commonly used to conceal personal identities in visual data. The existing survey studies addressing the FDeID topic lack comprehensive coverage of modern generative DL-based FDeID methods, limitations of data resources, proposing new applications, and potential technical and ethical research directions, which are covered for the first time in this survey. Throughout the manuscript, we offer critical analysis from various perspectives with a recurring theme of the growing impact that generative deep learning techniques are beginning to have on FDeID and related areas such as gait de-identification. In addition, we suggest 17 novel research dimensions and corresponding research questions in both technical and dataset perspectives, which will advance the research frontiers in this domain. The insights presented in this survey can benefit the research community and diverse stakeholders such as law enforcement, healthcare, industry, etc. It offers valuable insights into the performance analysis of existing methodologies, identifies research gaps, highlights application domains, and suggests precise possible avenues for future contributions.

Index Terms—Biometrics, Face and gesture recognition, Security and Privacy Protection, Posture

1 Introduction

THE individual's or a collective entity's privacy pertains to their right to keep personal information private and the option to reveal such information at their discretion. Whenever identifiable information is collected and retained, issues related to privacy emerge. With its significant prospects for enhancing productivity, Artificial Intelligence (AI) utilisation raises several legitimate concerns related to privacy protection and regulation [1], particularly considering the General Data Protection Regulation (GDPR) [2]. In this context, recent advancements in automated face recognition and face detection, particularly within video surveillance applications and smart tools (e.g., policing, social media, etc.), have given rise to privacy challenges. Regardless of the source of identifiable information (e.g., security cameras), various approaches have been developed to protect the individual's privacy.

Dr. Wasiq Khan (corresponding author) is a Senior Lecturer of Artificial Intelligence (AI) at the School of Computer Science and Mathematics, Liverpool John Moores University (LJMU), UK.
Dr Luke Topham is a Research Associate at the School of Computer Science and Mathematics, Liverpool John Moores University (LJMU), UK.
Umar Khayam is studying for an MSc in Applied AI at Deakin University, Australia.
Sandra. Ortega-Martorell is a professor of data sciences at SCSM, LJMU.
Panter. Heather is a Senior Lecturer at the School of Justice, LJMU.
Darren Ansell is a Professor of Aerospace and autonomous systems at the University of Central Lancashire, UK.
Dhiya. Al-Jumeily (OBE) is professor of AI in SCSM, LJMU.
Abir. Hussain is a professor of AI at Sharjah University, UAE.

Person de-identification (PDeID) refers to hiding identifiable information from source data (e.g., image, video, gait, etc.) such that AI-based tools or humans are unable to identify the person. Because of the vast emerging applications, PDeID is one of the hot topics with its diverse applications, specifically in public privacy, security, and law enforcement domains.

Generally, PDeID has been achieved through full-body obfuscation, face blurring [3] [4], and face synthesis [5] [6] [7]. In addition, appearance change (i.e., clothing) has been proposed in several works for the PDeID [5] [6]. The literature also contains PDeID and re-identification for improved privacy protection [7]. However, Facial de-Identification (FDeID) is the most common type of PDeID, mainly focusing on concealing facial identity, with broad scope and interest along with diverse applications such as state monitoring [8], UAVs [9], security domains (e.g., policing) [10] [11], autonomous systems such as robotics [12] [13], smart city concepts [14], and many more. Such applications lead to a higher demand for privacy protection, particularly visual identification through face capture and video streams.

From a broader perspective, FDeID can be categorised into traditional, technological, and, recently, AI, particularly machine learning (ML), deep learning (DL), and computer vision-based methods. The traditional methods use a cloth or similar material to cover the face of the accused

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

before media reports [15]. Alternatively, technological approaches use computational algorithms such as face blurring [16] [17] [18] [19] [20], pixelation [21] [22] [23], and face synthesis [24], which perform better in certain conditions. However, these methods require human interventions that are very time-consuming, such as manual blurring or pixelation of images [22]. Applying a blurring filter to videos or images [23] is also an alternative which reduces the utility of information in an image or video frame. Some recent methods, including k-same [24], preserve image utility that requires a large dataset while producing low-quality outcomes. However, the literature also recommends blurring as one of the most effective approaches for protecting the privacy of faces [19], regardless of its limitations, such as loss of facial utility.

Alternatively, AI-based approaches provide non-restraining and reliable solutions. More specifically, recent developments in DL and big data provide opportunities to produce generalised and more efficient FDeID. Furthermore, these methods can be fine-tuned for specific applications with limited datasets using transfer learning [25]. The literature concludes that compared to DL-based FDeID, conventional technological methods, including face blurring, pixelation, and block-based approaches, are unreliable [26] [4]. For instance, DL-based face recognition algorithms can easily recognise a blurred face using the original image. As an example, [27] proposed uncovering the privacy of blurred or pixelated images using DL. Likewise, [28] proposed image enhancement to remove blur from images. These methods demonstrated a high identity recognition rate within the faces blurred with conventional methods by utilising DL models.

1.1 Motivation

The development of FDeID methods, particularly with the recent advancements in DL and computer vision, has potential impacts within diverse application domains, including public privacy and security, smart environments, law enforcement such as policing, video games, animal welfare, and many more [8]— [14]. Recently, the UK Police Authority reported [29], [30] substantial time consumption, potentially even days, on pixelating body-worn camera footage due to concerns about privacy and GDPR. This issue has prompted the government authorities to commit to investigating these challenges. Pixelating appears to consume a considerable amount of time, potentially degrading the efficiency of police work. In this context, the police and security services could benefit from non-invasive, unrestricted, and reliable FDeID systems in realistic scenarios, such as body-worn cameras.

Further to time consumption, the Force Management Statement (FMS) for the Metropolitan Police Service (MPS) recently stated [1] an ever-increasing demand for privacy protection and related data protection legislation. The MPS has been reviewing its policies and procedures to improve efficiency, mainly by using technological solutions. The FMS further highlights AI-based solutions as a future strategy, particularly with the emergence of smart environments and increasing video surveillance (e.g., street cameras and body-worn camera devices). They aim to utilise AI tools for social media monitoring and automated analysis of mobile data. Considering the facts reported by FMS, FDeID might be highly useful for handling visual information, which currently requires a large amount of resources for data curation and analysis.

In addition, despite the presence of several review studies in this context, as outlined in Supplementary Material (SuppM) Table S1, existing works emphasise the techniques and methods employed for FDeID and PDeID but need to address several crucial aspects. Firstly, most of these surveys are outdated (e.g., [31] [32] [33]) and do not address advanced topics such as the use of Generative Adversarial Networks (GAN) and Generative Neural Networks (GNNs). Secondly, existing surveys lack the identification and recommendation of clear, concise, and precise solutions (and research directions) in multi-perspectives such as **a)** available datasets (e.g., limitations, strengths, new directions); **b)** potential new interdisciplinary applications; **c)** technical methods (i.e., identification of unresolved challenges). Moreover, most of the current review studies (except [34]) do not adequately address diversity and ethical considerations, which hold the utmost significance in the context of FDeID.

1.2 Contributions

This survey paper focuses on the comprehensive review of FDeID technological approaches, available datasets, new applications, ethical and data privacy aspects, limitations of existing works in various dimensions, and future research directions, along with recommendations. To the best of the authors' knowledge, existing surveys (as shown in Table S1 of SuppM) do not address FDeID in the context of diversity and ethical concerns, future novel research directions (methods and data assets), and new application perspectives. Furthermore, because of the emergence of recent technologies and the rapid proliferation of FDeID with diverse applications, particularly related to public privacy, safety, and security, FDeID has become an exceedingly prominent subject. In this context, the proposed survey will be beneficial, offering a comprehensive overview of FDeID from diverse perspectives, addressing novel aspects of the problem, enabling a clear understanding of the topic, potential applications, and future research gaps and opportunities (with multiple unresolved research challenges) that will be of great importance to related communities.

2 Review Methodology

As mentioned earlier, this survey aims to comprehensively review the existing research in FDeID and aid future work in the field from various perspectives. The following subsections explain the adapted methodology for this review study. The scope of this article is guided by two filters: research dimensions and search strategy.

2.1 Research Dimensions

The research aspects investigated in this survey include:

a) *Datasets availability for FDeID and their limitations, strengths, and major gaps.*

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

- ***b)*** *Assess existing FDeID methods and their strengths and limitations.*
- ***c)*** *Improvements and research directions for the existing FDeID datasets and technological approaches.*
- ***d)*** *Comparative analysis of the conventional, ML-based, and recently, DL-based FDeID approaches.*
- ***e)*** *Potential applications of the FDeID considering the emergence of smart city environments and the increase of video surveillance in various forms.*
- **f)** *Ethical concerns and regulations requiring attention for the research and development of FDeID systems.*

Initially, the survey presents the breadth of FDeID methods, evaluates their performances, and reveals the interrelationship between these methodologies. Subsequently, an overview of existing datasets used for FDeID tasks is presented, which mainly serve as training and evaluation resources for ML-based FDeID approaches. Furthermore, we identify several new dimensions that can serve for further exploration or refinement in future endeavours. Additionally, our review focuses on the ethical dimensions of FDeID, which has become a hot topic within the applied AI domain. Finally, we present a review of existing and potential new FDeID applications that would be highly impactful, specifically for the industrial community and law enforcement authorities.

2.2 Search Strategy

Table 1 includes a list of keywords and permutations used to explore the FDeID literature for this survey. The keywords are categorised into context and objective. Context refers to the FDeID datasets and methods required to achieve the objectives of the FDeID elements. Objective refers to de-identifying a person, mainly FDeID. The database libraries searched include IEEE Xplore, Science Direct, ACM Digital Library, Scopus, and Google Scholar. To filter the vast research and find only relevant studies aligned with the objectives of this survey, we defined a range of selection and quality assessment criteria that consider: **a)** only articles in English; **b)** only articles published in peer-reviewed journals or conferences, ensuring the quality of research; and **c)** non-repeated articles.

TABLE 1
KEYWORDS WE USED TO EXPLORE THE FDEID LITERATURE

Goal	Keywords
Context	face de-identification, face blurring, face masking, facial privacy, AI-based face deidentification, person de-identification, face obfuscation, face perturbations, face anonymisation, face cartooning, visual privacy protection, video surveillance, privacy tools, policing tools
Objective	masking, blurring, obfuscation, detection, identification, de-identification, recognition, estimation, privacy, ethical AI, privacy protection

With this search strategy, we identified 450 articles, which were further filtered to eliminate irrelevant literature. We remained with 172 peer-reviewed works covering face deidentification methods, datasets, applications, and ethical concerns.

Figure 1 shows that 40% of the reviewed papers belong to journal publications, and 37% are conference papers. In comparison, the remaining 23% are book chapters, workshops and reports published by government bodies (e.g., Police) and other sources (e.g., research thesis). Figure 1 also shows that 26% and 19% of studies belong to methods and datasets, respectively; 13% and 14% cover the ethics and applications, respectively; 7% address the future research directives; 17% other dimensions (*i.e.*, broader perspectives), and 4% existing surveys. It can be noticed that the highest proportion of reviewed FDeID approaches are based on face blurring (29%), followed by neural art and conventional approaches (20%), GAN (20%), GAN with k-based (11%), DL (11%), and GNN (9%).

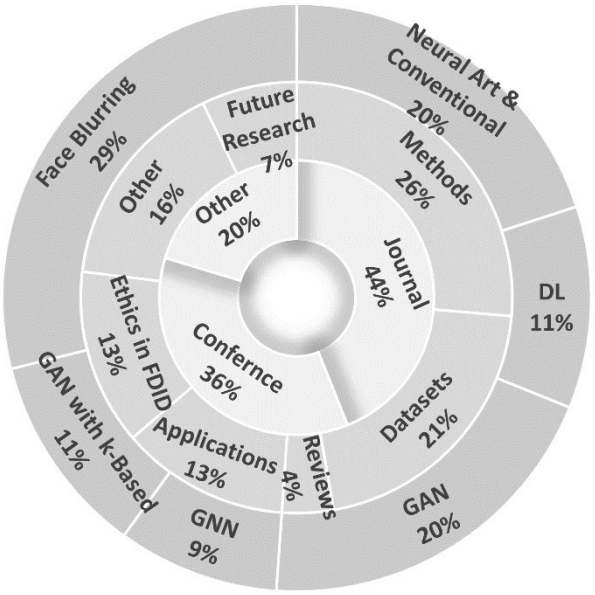


Fig. 1. Distribution of publication types, review dimensions, and FDeID methods explored in this survey.

2.3 Organisation

The remaining manuscript is organised as follows. Section 3 comprises a detailed review of existing works concerning FDeID methods. Section 4 presents the available datasets, corresponding challenges, and limitations. Section 5 entails a comprehensive review of various application domains, while Section 6 addresses the ethical concerns related to the topic. Section 7 summarises the possible future research directions and recommendations in multiple dimensions, such as data assets, methods, and new applications. Finally, concluding remarks are presented in Section 8.

3 FACE DE-IDENTIFICATION APPROACHES

This section summarises various FDeID approaches, strengths, limitations, and uses. Various FDeID methods have been introduced that can generally be categorised into conventional FDeID methods, computational and technological approaches, and ML or DL-based methods, as detailed in the following sections. Table S2 (in SuppM) summarises the literature concerning FDeID methodologies, study objectives, datasets used, performance measures, and associated limitations.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

3.1 Conventional FDeID Approaches

Computational methods concerning FDeID were introduced long ago, whereas early approaches used manual blurring or pixelating of videos and images [19]. Using blur filters on images in [23] is claimed as a better approach for protecting privacy and PDeID; however, gender can easily be recognised in this method. Likewise, different filters may produce varying levels of privacy and situation awareness. Furthermore, [22] highlighted several limitations of face blur approaches, mainly the lack of automation and reliability.

With the growing use of social media applications, there has been a drastic demand for individuals' privacy protection. In [19], the original user (content owner) can restrict the facial identity of a specific person(s) upon request from other users who are tagged. This provides a certain level of privacy on social media platforms, preventing users' identities from being misused by other users (*i.e.*, only the tagged person can see the image). Likewise, [20] proposed a facial privacy protection approach for social media by employing a trained ML model for face detection and recognition. The work proposes a system to prevent unwanted individuals from effectively recognising users in a photo. The work reported 87.4% success in preventing the users from identifying their contacts in restricted photos.

A scrambling approach which hides the face identity is proposed in [21]. The study uses the Colorado State University face identification evaluation system, which provides standard face recognition algorithms, standard statistical methods, and performance evaluation. The face recognition task uses Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA). The final subspace is obtained by multiplying the PCA and LDA basis vectors. The image pixels are modified, so the generated images are unidentifiable. For both PCA and LDA algorithms, the recognition rate is nearly 0% at rank 0 and remains below 10% at rank 50. However, this study uses a limited amount of dataset and diversity.

In the context of multi-object images, the literature contains several works introducing privacy control methods for multiple users. For instance, in scenarios where the first user is granted access to view only a single object, the remaining objects are obscured or blurred for that particular user. This concept is implemented by [35] for crime deterrence and investigation. It refers to an object's privacy policies, which are determined according to the object's closeness to viewers. It also determines abstraction operators to hide the visual information of objects.

Despite the successful use of application-oriented conventional FDeID approaches, these methods are invasive and require substantial human intervention, which is impractical given the massive data available through various means, the increasing demand for surveillance, and simultaneously the regulations and concerns of privacy protection and GDPR. Thus, autonomous, efficient, and generalised methods are required to perform FDeID and handle the challenges of real-time dynamics.

3.2 DL-Based FDeID Approaches

The limitations of conventional image processing-based FDeID have been resolved using DL methods, such as landmark detection and Deep Neural Networks (DNNs).

3.2.1. Autonomous Face detectors-based FDeID

A face-blurring pixel-based approach is proposed in [36] by utilising multiple face detectors where faces and corresponding pixels are detected following the implementation of Dempster's rule to perform the blurring of the identified region. Another face burring approach based on multi-boosting is introduced in [37], which combines face detection with pedestrian detection using the Viola-Jones algorithm. A skin detector is used to eliminate false positives. The model first detects pedestrians and then corresponding faces within the identified region (*i.e.,* pedestrian segment). It blurs all the faces of identified subjects in image or video frames. The study reported an average of two false positive detections per image frame, limiting its use in real-world environments.

The face-blurring approach in [16] is utilised for children's privacy, performing child detection followed by a blurring task before uploading the image to a social network. In case a child under the age of 16 years is detected in an uploaded picture, the system automatically blurs the face region. A pre-trained DL model (VGG-16 trained) is used to identify the age. A similar face-blurring approach is proposed in [17], which first detects the faces with the Viola-Jones detection algorithm [38]. This approach uses a background removal method using image subtraction in the pre-processing stage. In the second step, tracking is performed with a colour space algorithm over the detected faces. The template matching algorithm is then used to reduce the processing time, and a final Gaussian filter is applied to the detected face. The study indicated that in some multi-face experiments, the detection rate was very low, mainly because of the inability to detect all faces in the image.

A face-obfuscating approach for preserving visual privacy in social media platforms is proposed in [39]. It detects a user's face from an input image, applies the adversarial perturbation, and returns the image with a perturbed face. This model indicated reliability for the face detection (*i.e.*, 98% accuracy); however, perturbed images are still recognisable.

A face cartooning approach for privacy protection in video is proposed in [40]. For face detection, the Viola-Jones face detector [38] is utilised. The developed system can perform cartooning for entire images or selective regions of images. In addition to the pre-trained face detector, this work performs image processing, including blurring, Sobel edge detector, and mean shift filter. This strengthens the cartooning effect and makes the image less blurry. However, the performance (70% face recognition accuracy) for processed images is not very satisfactory for the applications.

3.2.2. Deep Neural Networks (DNNs) for FDeID

Considering the limitations of face detector-based methods, [41] proposed a DNN model for facial obfuscation against unauthorised face recognition. The model uses adversarial facial obfuscation to generate images with feature vectors significantly diverging from the original in the

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

embedding space while keeping perceptual similarity. The study conducted a survey regarding face obfuscation against unauthorised face recognition using DNN and concluded that a little perturbation could cause DNN face recognition to produce false predictions.

Face attribute transfer mode is presented in [42] uses DNN to map non-identity-related facial attributes to face images. The model detects faces within the image frame using a pre-trained landmark detection, then synthesises the detected faces and provides re-identification for matching the original image with the generated one. This approach preserves expression, light condition, and head pose. It transfers the facial expressions in the original image to the target faces of a consented subject. While the study reported effective FDeID results, it has limited use for the occluded faces, e.g., where faces overlap.

A similar DL-based FDeID approach is proposed in [43] with applications to digital image information exchange, which utilises block scrambling and DL techniques. With the Arnold random scrambling algorithm, the main parts of the human face, such as the eyes, nose, mouth, etc., are scrambled. The scrambled image is then processed by a Convolutional Neural Network (CNN) model for face recognition. While these works perform satisfactorily from application perspectives, the diversity aspect of the models' training is limited. For example, datasets used contain only frontal images, single instances, and limited diversity.

A face-swapping technique for patient privacy protection in clinics is proposed in [44]. A DNN is used to automatically perform facial swaps, taking input video and generating swapped face video as output. Face detection is achieved through MTCNN and Single Shot Scale-invariant Face Detector (S3FD. Face Alignment Network (FAN) performs extraction and alignment on the face data. Although the recognition rate with original faces is less than 10%, performance further degrades for realistic and diverse datasets. A similar work [45] proposes a deepfake-based approach to generate fake faces to be swapped with the original one. It protects privacy in medical videos containing patients' faces, which could be swapped to a target face and become unrecognisable. Like [44], the dataset contains only frontal face images and limited diversity (e.g., use of frontal pose, static background).

A DL-based approach in [46] for privacy protection within the videos captured in street cameras, public places, banks, etc., uses the responses of a DNN to transfer the style of one image to another. The neural art algorithm is used for de-identification, requiring two images as input: a content image to be transformed and a style image to be used for transforming the content image.

A similar approach is proposed in [47] based on a neural art algorithm utilising the VGG DNN's responses trained on ImageNet. The input image is processed to obtain an initial foreground background estimation using background subtraction based on Gaussian Mixture Models (GMMs). For face detection, the Viola-Jones face detector [38] is employed where the detected face is masked with the altered face. The outcomes show that the resulting image is recognisable explicitly in realistic environments, potentially because of the limited generalisation of the model, for instance, being trained over frontal videos only in controlled settings (e.g., indoor settings).

A subspace decomposition technique to decouple the parameters that control different facial attributes is proposed in [48]. This model learns subspaces from a training set with annotations for gender, age, and race attributes. Multimodal Discriminant Analysis (MMDA) [49] captures the essence of gender, race, or age in a single constant vector parameter. For facial landmark identification, the Adaptive Appearance Model (AAM) [50] is employed. A mask is then applied to remove hair and background from the input image. The utilisation of MMDA helps to synthesise new faces with target attributes. This approach, like [51], uses only frontal faces in training and validation, which is uncommon in realistic cases.

3.3. Differential Privacy (DP) and Diffusion Models for FDeID

Recently, many works, such as [52] [53] [54], have performed de-identification using diffusion models. Diffusion models use an iterative forward diffusion process to destroy structure in a data distribution [55]. It is then possible to restore the data via reverse diffusion. For example, in [52], diffusion models are applied to make small changes to face shapes, providing a level of privacy while remaining identifiable as faces. Similarly, [53] uses a diffusion model to blur images. However, to mitigate the common problem of computational expense associated with the iterative nature of diffusion models, [53] uses the forward and backward process to estimate image quality and to apply the forward process accordingly. Unlike [52] [53], which results in blurred, unnatural images, [54] results in more natural images by using generative methods to add alternative facial features. However, the results of [54] are unlikely to fool a human observer. Due to their iterative nature, diffusion models are relatively computationally expensive, which may have implications for their usage, for example, in real-time video streaming [53].

Study [56] introduces a face anonymization framework composed of a data-driven deep neural network with a differential privacy mechanism. This approach allows for adjustable privacy-utility balance through the privacy budget and generates high-quality, identity-agnostic images suitable for tasks like detection and tracking without requiring pre-annotations. This study also uses CelebA and CelebA-HQ datasets for the training and cross-data validation and is thus limited to frontal faces. For the cross-dataset validation (CelebA), this approach produced a structural similarity index (SSIM) of 0.82, an identity distance of 1.1, and a protection success rate of 0.96.

In recent research [57], the limitations of k-same obfuscation to composition attacks and background knowledge inferences are experimented with, reporting potential violations of its privacy guarantees. The study proposes employing the DP application for facial identity obfuscation using generative ML models. Additionally, a method to enforce DP by directly modifying pixel intensities is proposed, sacrificing some visual quality for versatility in obfuscating any image. Experiments show that DP is more resilient to composition and parrot attacks and offers

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

comparable utility while providing stronger privacy guarantees. The study concludes with recommendations for implementing generative models and pixel-space image obfuscation to achieve better privacy protection.

3.4. Advanced DL-based FDeID Approaches

Recently, the advancement in generative AI and computer vision has accelerated this domain, producing various FDeID methods addressed in the following subsections.

3.4.1. GAN-based FDeID methods

The GAN is an adversarial process where a generator model learns to generate realistic-looking images from the actual data. In contrast, the discriminator learns to distinguish between the generated images and the corresponding actual training data [58]. In relation to FDeID, GAN uses the face synthesis approach to protect face privacy and preserve utility for still images and video data.

The literature contains a variety of GAN-based FDeIDs, mainly for privacy protection. Research in [59] utilizes GAN to generate the deidentified image, which looks different from the original image, while face utility, such as gender, age, and race, is preserved. The model adopts a structural similarity index to quantify the similarity between the original and the generated images. This approach achieves verification accuracy between 94% and 97%; however, it struggles when evaluated over 'faces in the wild' comprising varying head poses, occlusion, and other dynamics.

Another work [60] presents a GAN-based FDeID for privacy preservation during website access. To resist fully reconstructing images, the framework uses a discriminator GAN to directly reconstruct data to a designated target distribution, assuming that the target distribution differs from the data distribution. The generator and re-constructor are implemented using three different structures, including VGG Nets [61] and a CNN model. The framework aims to increase the distance between original data and its reconstruction and to preserve individual privacy while retaining significant information. The model indicated 90% accuracy when evaluated on multiple grey-scale datasets.

Another GAN-based FDeID approach is proposed by [5] to resolve the overfitting problem. The work also enhances the generated image quality using the improved U-Net [62] in the generator. Two discriminators with a seven-layer network architecture are designed to strengthen the feature extraction ability. The design of an adversarial loss function is introduced to reduce the problem of model collapse and overfitting during the training. The study also reported the ability of full-body de-identification; however, it indicates relatively lower performance.

EPD-Net is proposed in [63] utilizing a GAN-based architecture to maximise emotion similarity while minimising person identification. The model generates an output image with minimised identifiable features (compared to the input face image) while preserving the emotion of the input face. While this approach indicates reliable performance, further improvements can be made in several aspects. For example, the dataset is limited to frontal faces and a single instance per image.

FDeID is extended to real-time video in the recent GAN-based work [64]. A face dynamic similarity module is implemented to preserve facial dynamics while transforming facial identities. The dynamic similarity model uses a pre-trained landmark detection module to quantify the discrepancy between landmarks on original images compared to de-identified images focusing on features such as eyebrows, which are heavily related to facial expressions. The work was designed to enable anonymous telemedicine and video-based diagnosis.

A full-body de-identification method using GAN is presented in [6] generates a de-identified image with cloth changing where the face is de-identified through hairstyle and background replacements. The GAN model ensures synthetic images look natural and fit well within the original scene. For face synthesis, this approach uses a pre-trained deep model (DCGAN), while for face detection, the Viola-Jones face detector [38] is utilised. Despite the composition of multiple methods, the outcomes indicate poor face detection performance when evaluated over a larger dataset (Human 3.6M [64] dataset).

Alongside FDeID, a head obfuscating approach is proposed in [65] revealing that a simple blurring approach is insufficient for this task. In contrast, a knowledge transfer approach is used between the encoder and decoder, where the decoder (during training) learns from the encoding component to reduce parameters to facial coordinates. A GAN model generates missing visual contents while conditioning the context. However, both approaches assume appearance and texture similarity between the missing part and the context. This model can generate head inpainting solely from the body and scene context without resorting to any information from the head region.

Secret Face Generative Adversarial Network (SF-GAN) is proposed in [66], claiming FDeID without losing facial attribute information. This approach aims to perform FDeID effectively and generate visually reasonable images while retaining the facial attribute information of the original images. SF-GAN uses shallow-face attribute information and deep-face attribute information and adopts different processing strategies for multi-attribute retention. This method reports reliable performance. However, datasets are limited to frontal view only, limiting their useability in most practical scenarios.

Alternatively, PrivacyNet [67] imparts soft biometric privacy to face images via image perturbation. The image perturbation is performed using a GAN-based semi-adversarial network. PrivacyNet modifies an input face image such that it is effective for face-matching purposes but unreliable for attribute classifiers. This approach further trains a cycle-GAN model without the auxiliary face matcher. The results showed comparatively better performance in perturbing the target attributes without affecting the matching utility of face images. However, a human observer may distinguish between perturbed face images and non-modified ones.

An end-to-end facial privacy protection approach [68] uses pixel-wise face region loss to seamlessly replace a face in an image with a synthesised face. The study uses Multi-task CNN (MTCNN) for face detection and face swapping, replacing the original image's face with an auto-generated

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

one. The generator is built upon U-Net [62], consisting of an encoder and a decoder while preserving the background of the original image. PatchGAN is adopted as a discriminator to identify the generated face images from actual ones. The outcomes reported that the generated images are completely different from the original images, with 97.9% face detection accuracy.

A similar approach for the FDeID that preserves the image's background is proposed in [69]. The model can automatically anonymise faces in images while retaining the original data distribution. Interestingly, this work produces a diverse dataset of human faces, Flickr Diverse Faces (FDF), which includes unconventional poses, occluded faces, and a vast variability in backgrounds. The study reported over 95% accuracy for the face detection for cross-evaluation over the Wider Face dataset. However, non-traditional poses may cause this model to generate corrupted faces.

A framework for FDeID is proposed in [70] based on obfuscating visual appearance while preserving identity features such as race, expression, and age. It comprises two major components: an identity-aware region discovery module and an identity-aware face confusion module. The former adaptively locates the identity-independent attributes on human faces and generates the privacy-preserving faces using original faces and discovered facial attributes. The outcomes reported effective anonymisation of facial appearance; however, humans may easily identify the person in generated images by race, expression, age, and other attributes.

A recent study [71] investigates the effectiveness of state-of-the-art methods for privacy protection, mainly face obfuscation approaches. The authors conducted an online survey (N=110). They found that DeepFake obfuscation is a viable alternative to state-of-the-art obfuscation methods such as blurring, pixelating, and replacement with avatars. The work also investigates how DeepFake obfuscation can enhance privacy protection without negatively impacting the image's aesthetics. The outcomes revealed that the person identification rate for public figures obfuscated significantly varies with respect to the corresponding method. For instance, humans' success rate for DeepFakes (29%) is far lower than blurred faces (95.96%), pixelated faces (85%), avatars (75%), and masked faces (59.18%). This clearly indicates the effectiveness of DL and GAN-based approaches for the FDeID compared to conventional technological approaches.

3.4.2. GAN with Autoencoders and GNN for FDeID

Convolutional autoencoders [72] impart privacy using the transformation of input face images by utilising semi-adversarial networks with CNNs. Convolutional autoencoder is trained in the first step, producing an image that closely resembles the original image from the training set while incorporating gender prototype information. Further training involves incorporating feedback from both auxiliary CNN-based gender classifiers and auxiliary CNN-based face matching into the loss function. This produces regenerated images so that the error rate of the auxiliary gender classifier increases while the auxiliary face matcher is not unduly influenced.

Another GAN-based approach is proposed in [73] to control privacy in images and videos. The system first detects a face using the Viola-Jones face detector [38] and then uses GNNs to transform the detected face into a new form (e.g., a different expression). The face generator is trained over the RAFDB dataset [74] to generate a new face. The GNNs used in this work allow different image generation processes and synthesise faces with different appearances under varying poses and facial expressions. It also preserves non-identity features such as gender, race, etc. Along with its effectiveness for utility preservation and privacy protection, this approach is similar to [72] struggles to handle hazy or occluded scenes.

A controllable FDeID method utilising generative AI and Ml algorithms is proposed in [75] offering a customizable balance between data utility preservation and privacy protection, as well as producing diverse and high-quality images. Based on GAN inversion and the StyleGAN2 model, this method uses a multi-objective loss to optimize image semantics, contextual cues, and specialized loss terms, ensuring identity suppression, utility preservation, diversity, and realism. Experiments are conducted on cross datasets, showing better face verification, data utility, and image quality. Despite its effectiveness, validation is performed on datasets either captured in static background, with less diversity, or with frontal faces as the majority sample.

3.4.3. Autoencoders-based FDeID methods

Fully connected convolutional autoencoders are used in [76] for the FDeID. For model training, finetuning of the encoder is performed to preserve facial attributes. The tuned network then performs FDeID in an end-to-end fashion by forward passing the facial image through the modified encoder, which changes face identity while preserving other attributes. Subsequently, the decoder reconstructs a new face. As the autoencoders tend to produce a blurred reconstruction, the system also uses a deblurring model, which is trained over blurred images to remove Gaussian blur from images. The overall end-to-end system is aimed at embedded systems applications, such as autonomous UAV flight privacy preservation.

A recent study [77] proposes a Quality Maintenance-Variational AutoEncoder that preserves face expressions in FDeID. Firstly, it de-identifies the input image and then reconstructs its utility. The model integrates vector quantisation into the structure of the generative model to generate high-quality face images. OpenCV and CNN are used for face detection and facial expression classification. A similar FDeID approach utilising an adversarial auto-encoder coupled with a trained face-classifier is proposed in [51]. A new variant of perceptual loss is employed to maintain source expression, pose, and lighting conditions while capturing the essence of the target identity. To encode the target image, the model uses a pre-trained face classifier, ResNet-50 [78], trained over the VGGFace2 [79]. The model uses a target image randomly selected from the person's video and maximises the distances between the face descriptors of the output video and the target image. This contributes to the applicability of the method to real-time

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

video streams.

3.4.4. k-Obfuscation FDeID methods

The k-Anonymity and k-Same are the popular approaches used for the FDeID and privacy preservation with the following major categories.

3.4.4.1. k-Same and k-Anonymity models: Research [24] employed the k-Same model to determine the similarity between faces based on a distance metric and to create new faces by averaging image components. The study reported 'k' selection as challenging, partly depending upon the level of protection prohibiting the ability for all individuals to be known.

A hybrid algorithm (k-Same-Select) was recently proposed [26], claiming its usefulness for data utility preservation compared to k-Same and ad-hoc methods. Likewise, k-Same-M is introduced in [80] by combining a model-based image parameterisation and a formal privacy protection model. The algorithm trains a generative model until the difference between the original and reconstructed images is minimal. The parameter vector of the model serves as an encoding for the input image. The study identified pixelation as a particularly ineffective approach because it produced recognisable faces.

A k-Anonymity-based de-identification in video frames has recently been proposed in [81], preserving the pose expression and other utility features. Face pose is determined as a separate model in the preliminary step before the FDeID. This method indicated better performance compared to the k-Same approach. Notably, it works for side poses, which is mostly required in practice. However, face detection would be required to perform the FDeID and other processes.

Another study [118] proposes a similar approach that maintains various facial attributes such as expression, age, and gender. It randomly selects *k*-face images and transfers the face attributes from the test face to the *k*-selected faces using the ELEGANT model [82]. The *k*-selected faces have the same attributes as the test face. The ELEGANT model encodes face images into latent space by using an encoder. A decoder decodes the latent encoding to the corresponding face image. In the latent space, the corresponding parts of the two latent encodings exchange the relevant attributes of the two original face images. Results indicated that this approach outperforms the *k*-Same approach [24].

3.4.4.2. k-Same with GAN and GNNs: Facial identity controllable GAN [83] utilised k-Same anonymity and GAN methods for the FDeID and preservation of other identifiable features such as hair, colour, eyes, and expressions. The conventional manifold k-Same method mixes multiple face images in the latent identity space, risking privacy leakage and poor data utility. Averaging faces leads to blurry images, affecting quality. To address these issues, an autoencoder-based conditional generative model disentangles identity from non-identity attributes, applying manifold k-Same for k-Anonymity. This enhances performance by embedding structural features, head pose, and expression. However, it is limited to frontal faces and may cause de-identified faces to match others, raising privacy concerns.

To tackle the challenges in existing methods, such as [84], FDeID approach known as k-Same-Siamese-GAN is proposed in [85], comprising face recognition, cluster generating, and candidate clustering. Mixed precision training ensures privacy protection on close-form identities for time and space efficiency. This approach also enables the re-identification for which the Siamese network has been modified and incorporated. While this approach produced nearly natural and realistic-looking de-identified face images, it requires large training time and identifiable output faces.

A recent work introduces the k-Same-Net [84], a composite of GNNs and k-Anonymity mechanism, to protect privacy on a closed set of identities. This model produced realistic and natural-looking facial images corresponding to the identities from the training data and artificial non-existing identities. The outcomes comprise various facial expressions while preserving the utility of age, gender, and race. This approach was also able to re-identify from output images. An improved version of [84] proposes synthesised surrogate faces for FDeID [86], mainly for social media and cloud-based services. This approach integrates diversity into the de-identified faces, replacing an original face with a surrogate face synthesised using GNN. While these methods indicate efficient performance (~100%), they are limited to frontal faces and single faces per image. Furthermore, the quality of the generated images lacks a synthetic appearance.

3.4.4.3. k-Same with AAM: An appearance-based approach (k-Same-furthest) has recently been proposed [87], mainly focusing on high reliability and accuracy. Because the conventional k-Same is an appearance-based algorithm, a 'ghosting' artefact tends to appear in the output due to the misalignments of the *'k'* images involved. This happens despite the images being aligned based on a small number of facial landmarks. To prevent ghosting artefacts in the de-identified faces, k-Same-furthest averages the faces in the feature space constructed by an AAM. The FDeID is performed using the faces that are furthest away, hence maximising identity loss and achieving perfect privacy protection regardless of the value of *'k'*. On the other hand, results revealed that using PCA representation of face images, the recognition rates of the de-identified faces are slightly above zero; however, they are comparatively better than the k-Same-M faces.

A framework named GARP-Face, proposed in [88], balances the utility preservation in FDeID in relation to gender, age, and race attributes. Given an input face image, GARP-Face determines its gender, age and race attributes using facial analysis techniques in the first step. It then performs the FDeID by blending with the GAR representative super-face, which is similar to the original face and has consistent attributes. This method builds a utility-specific AAM per category, utility determination, and a diverse face gallery. The parametrisation of a face image is performed to minimise the difference between a utility-specific AAM model and the input image. This approach can be further improved with better attribute classifiers.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

3.5. Summary

This section comprehensively reviews FDeID approaches based on conventional image processing, DL, GAN, GNN, DP, and *k*-Anonymity methods. Table S2 (in SuppM) summarises the literature concerning FDeID methodologies, study objectives, datasets used, performance measures, and associated limitations. The literature uses diverse evaluation metrics w.r.t FDeID methods and appropriateness of the application context. A detailed list of evaluation metrics, along with a brief description and mathematical formulation, is presented in Table S3 of SuppM. It can be noticed in Table S2 and Fig. 2 that generally, GAN and GNN-based approaches such as [59], [66], [70], [68], [69], [84], [86], emerged as the most effective, falli ng to 10% or less post-deidentification rate. For example, [68] reports 98.2% and 98.9% de-ID rates on the VGCFace2 and CelebA datasets, respectively. This indicates a significant reduction in the ability to identify faces, showcasing the robustness of these techniques in preserving anonymity. However, most of these approaches are limited to only frontal camera view and without occluded faces (or conditions), which is not the case in realistic environments (e.g., street surveillance cameras).

Likewise, humans can identify generated faces by corresponding attributes (e.g., race, expression, age, etc.); some of the works use relatively small datasets with limited diversity and realistic dynamics (e.g., occlusions [89]) and particularly, multiple camera perspectives such as profile/rear view, which is common in practice (e.g., smart city cameras). Similarly, in [60], a low-dimensional image has less chance to re-construct.

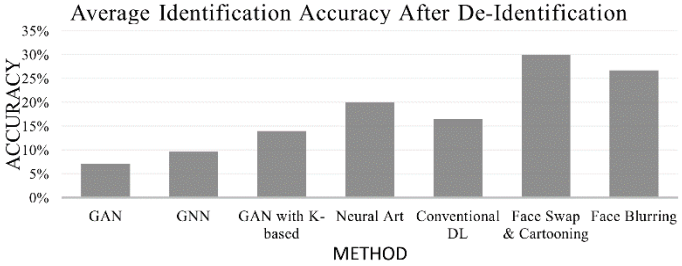


Fig. 2. The average facial identification rate reported after FDeID has been performed using various de-identification methods. The average was calculated from the results reported in the literature surveyed.

In contrast, conventional DL-based approaches such as face swapping, cartooning, and face blurring [7], [42], [41], [43], [77], and [27] were less successful in obscuring identities. These techniques resulted in a higher average identification rate (post deidentification), exceeding 25%, where the generated outcomes are either recognisable by humans (e.g., [42]) or comprise of limited diversity [43]. Finally, the *k*-Same family [84], [85], [83], [5], and [6] integrates GAN with *k*-Anonymity, indicating reliable performance, particularly attribute preservation; however, individuals can be re-identified via other cues besides facial identity.

While GANs offer reliability in FDeID, for example, [83] reports a de-ID rate of 91.09%. However, they require more processing time and computational resources [90], which is also true for Neural art methods. Alternatively, GNNs provide a good balance between processing time and effectiveness, making them suitable for applications where both are important. Other traditional methods, such as face blurring and pixelation, are time-efficient and least resource-intensive; however, they are less effective at ensuring privacy. On the other hand, DP-based FDeiD methods are highly reliable for obtaining privacy, with variable processing times depending on the specific approach.

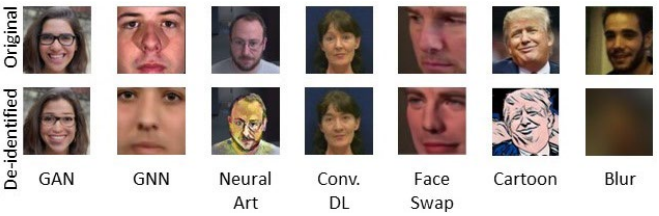


Fig. 3. FDeID output samples generated using various conventional and advanced technological approaches.

4 Person de-Identification Datasets

This section comprehensively reviews available PDeID, FDeID, and full-body de-identification datasets in 2D and 3D settings. Common trends and limitations are also summarised in Table 2 and mainly include **i)** dataset size, **ii)** diversity concerning various factors, e.g., socio-demographic attributes, **iii)** single vs multi-camera view, **iv)** single vs multi-instance images, **v)** dimensionality (e.g., 2D, 3D), **vi)** availability and annotations, **vii)** strengths and limitations, and several other factors.

Figure 4 demonstrates that most of the existing datasets are based on images (87%) compared to video datasets (13%). Likewise, only 5% of datasets are captured from a 3D camera view despite its effectiveness for real-world applications. Some datasets (18%) are available upon request, while 24% of datasets are not annotated, requiring substantial time for experimental analysis. Furthermore, only 18% of the datasets contain full-body poses. The identified datasets and the original source are briefly described in Appendix A (in SuppM).

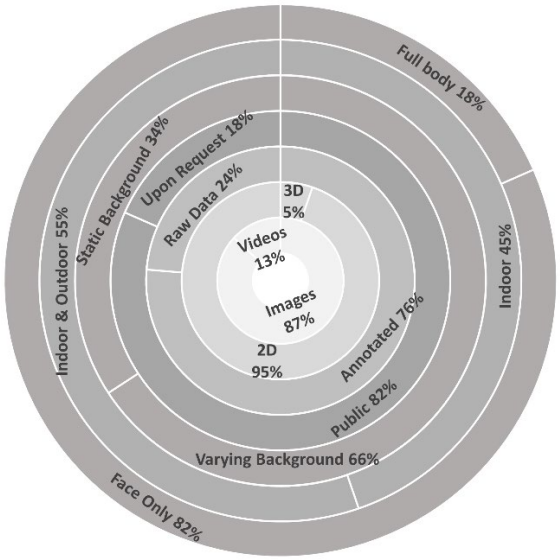


Fig. 4. Distribution of existing PDeID datasets along with diverse aspects, e.g., dataset type, size, availability, camera view, body signature, etc.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

TABLE 2
SUMMARY OF 38 RELATED DATASETS REVIEWED WITH DETAILED STATISTICS, AVAILABILITY, STRENGTHS, AND LIMITATIONS

Dataset reference	Body parts, Data type	Instances	Participants	Indoor (I) OR Outdoor (O)	Available publicly (✔) Or upon request (R)	Annotated	Background variations	Strengths & limitations
[91]	Face images, 2D	202.5k	10,177	I, O	✔	✔	✔	Face identification dataset (CelebA) comprises varying poses and backgrounds, useful for DL model generalisation, 40 binary attribute annotations per image, and 5 landmark locations.
[92]	Face images, 2D	1,724	515	I	R	✔	×	Age estimation dataset (MORPH) comprises age, ethnicity, gender, height, and weight information. Only frontal faces with no background variations. Coarse to fine image quality.
[93]	Face images, 2D	216	67	I	R	✔	×	Facial expressions (RaFD) dataset comprises diversity in terms of varying poses and expressions; however, the dataset is small and only a single background is used.
[74]	Face images, 2D	29,672	-	I, O	✔	✔	✔	Facial expression dataset (RAF-DB) has high diversity in subjects' age, gender, ethnicity, head poses, lighting condition, occlusion, and special effects. Provides 5 accurate & 37 estimated landmarks. No information about the number of subjects. Contains mostly frontal faces.
[89]	Full body Videos	64,204	54	I	✔	×	✔	Person identification dataset (ChokePoint) has diversity, such as occlusion, sharpness, and pose varying. 48 videos in total with a resolution of 800x600. Limited to indoor environments without realistic dynamics, containing gender bias, limited size, and lack of annotations.
[94]	Face images, 2D	3,755	276	I	✔	✔	×	MUCT face database comprises 480x640 image resolution, diversity of lighting, age, and ethnicity; 76 manual landmarks annotations. Static background and frontal camera view in all images.
[95]	Face images, 2D	13,233	5,749	I, O	✔	✔	✔	Face dataset (LFW) has diversity, such as variation in pose, lighting, and quality. However, it mostly comprises frontal face images.
[96]	Face images, 2D	4,000	126	I	✔	×	×	Facial expression dataset (AR Face) contains different genders, facial expressions, illumination conditions, and occlusion; frontal faces only, captured in two controlled sessions.
[97]	Face videos & speech data	2,360	295	I	R	✔	×	Face video dataset (XM2VTS) comprises rotating head videos captured from front side. There is good data for head detection and tracking. However, there is less environmental diversity.
[98]	Face expression videos	593	123	I	R	✔	×	Facial expression dataset (CK+) has diversity, e.g., varying backgrounds and 7 different emotions. It was captured with a static background in a controlled environment from a frontal view.
[99]	Face images, 2D	165	15	I	✔	×	×	Face recognition & expression dataset (Yale) comprises low-quality images in controlled settings and frontal camera perspective.
[100]	Face images, 2D	60,000	2,000	I, O	✔	✔	✔	Person identification dataset (PIPA) with diversity such as age, activities, and face poses; gathered from Flickr, part of the dataset contains multiple face instances per single frame.
[101]	Multi-instance ace images, 2D	393,703	-	I, O	R	✔	✔	Face detection dataset (Wider Face) has diverse backgrounds, scales, poses, occlusion, expressions, makeup, and illumination. In total, 32,203 images with 393,703 labelled face instances. Users must submit final prediction files to evaluate the performance.
[102]	Multi-instance ace images, 2D	11,931	-	I, O	✔	✔	✔	Face detection in the wild dataset (MALF) comprising 5,250 images with 11,931 face instances (captured from public sources such as Flickr) in diverse conditions and activities. There is no information about the number of subjects; dataset contains mostly frontal faces.
[103]	Full body images, 2D	2,098	-	I, O	✔	×	✔	Clothing co-parsing dataset comprises a wide range of styles, accessories, garments, occlusion, backgrounds, and poses. 1,000+ images are annotated at the pixel level. No face-specific annotations are provided; however, they can be annotated.
[104]	Face images, 3D	2,500	100	I	R	×	✔	Facial expression dataset (BU-3DFE) comprises people with diverse ages (18-70 years old) and ethnicities captured in a controlled environment from two angles (45 and -45 degrees).
[105]	Full body images, 2D	53	-	I, O	✔	✔	✔	Motion detection dataset (CDnet) of videos to detect change in environmental dynamics. Total 53 videos (4-6 video sequences in each category) with over 140k frames. Data is not specific for a person; there is no subject information, but it provides annotations for moving objects.
[64]	Full body images	3.6M	11	I	✔	✔	×	Human pose dataset (Human3.6M) is captured with four cameras from different angles. Each subject was captured with 17 scenarios (e.g., discussion, smoking, talking phone, walking, etc.), in an indoor settings and contains multiple poses (e.g., front, side, and back) with annotations.
[106]	Face images, 2D	70,000	-	I, O	✔	✔	✔	Flickr-HQ faces dataset comprising high-quality images with varying age, ethnicity, and image background. No subjective information is provided, mainly from a frontal camera perspective.
[107]	Face images, 2D	58,797	200	-	✔	✔	✔	PubFig face dataset (used for attribute & smile classification, face identification) collected from online sources comprising varying lighting, scene, camera, etc. Only a frontal camera view is available. Multiple images per person are available.
[108]	Face images, 2D	30,000	-	I, O	✔	✔	✔	Face classification dataset (CelebA-HQ) comprises better-quality images with variations such as pose, background, ethnicity, lighting, etc. Mostly, frontal faces are cropped.
[109]	Face images, 2D	49,4414	10575	I, O	✔	✔	✔	CASIAWebFace dataset was collected from IMDb comprising faces with diversity (e.g., age, ethnicity, etc.), multiple poses, camera position, and background. The dataset is not annotated.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

[110]	Face images, 2D	141,130	695	I, O	✔	✔	✔	FaceScrub dataset comprises face images collected from online sources, processed automatically and then manually. The data includes a fair distribution of males and females with other diversities (e.g., pose, background, etc.). Mostly frontal face images.
[79]	Face images, 2D	3.31M	9000	I, O	✔	✔	✔	VGGFace2 is a face recognition dataset collected from online sources, comprising diversity of age, pose, illumination, ethnicity, etc containing ~362 samples per subject from frontal view.
[111]	Face images, 2D greyscale	400	40	I	✔	×	×	Face synthesis dataset (ORL) contains diversity, e.g., capture time, lighting, and facial expressions. There is gender bias, low resolution (92x112, 8-bit grey), and frontal faces only.
[112]	Face images, 2D	20,000	-	I, O	✔	✔	✔	Face detection and age estimation dataset comprising variation in age, pose, facial expression, illumination, occlusion, etc. Frontal faces only with no clear information on subjectivity.
[113]	Face images, 2D	1.8M	-	I, O	✔	✔	✔	FaceForensics++ is a facial forgerie dataset with 1.8m images generated from 1000 videos collected from online sources. It contains only frontal poses without multi-instance images.
[114]	Full body video data, 2D	65	9	I, O	✔	✔	✔	PEVID video dataset for person detection and activity recognition, comprising diversity in gender, capture time, ethnicity, race, and performing different actions with different poses. Each video is 16 sec long with 25fps. Out of 65 videos, only 20 videos are annotated.
[115]	Multi-instance face images, 2D	5,171	-	I, O	✔	✔	✔	FDDB face detection dataset with varying resolution and poses (fontal faces as the majority). In total, 5,171 faces in a set of 2,845 images. No information on the subject count is provided.
[116]	Face images, 2D	14,126	1199	I	✔	×	×	FERET face recognition dataset, comprising duplicate images per subject. The dataset contains only frontal poses with fewer environmental variations.
[117]	Face images, 2D	750K	337	I	R	×	×	Multi-PIE face expression dataset: Participants were captured in multiple sessions with different poses (15 viewpoints including frontal and side), illumination, and facial expression.
[118]	Full body video data, 3D	15,000	8	I	✔	✔	✔	BEHAVE data presents 321 videos recorded with 4 Kinect RGB-D multi-view cameras. One of the large-size persons tracking datasets with subjects interacting with 20 objects in 5 environments. The number of participants is small (8 only) and therefore limited diversity.
[119]	Full body dataset, images	632	-	O	✔	×	✔	VIPeR person tracking dataset captured from varying angles, including side and back, and realistic outdoor environment. Images are scaled to 128x48 pixels. There is no information on the number of subjects and annotated body parts.
[120]	Face images dataset, 2D	40	400	I	✔	✔	×	**AT&T:** Face images captured with varying times, lighting conditions, facial expression. Dataset is captured with static background, poor resolution (92x112 pixels), frontal (upright and facing forward) perspective, with some flexibility allowed for slight sideways adjustments.
[106]	Face images dataset, 2D	70,000	-	I, O	✔	✔	✔	**FFHQ** Face images dataset with many variations in age, ethnicity, and glasses wearers. Faces are cropped automatically from public platforms (Flickr) using a third-party DL model. It comprises frontal faces only with a single instance per image in most cases.
[121]	Face images dataset	240	40	I	✔	✔	×	**IMM** is a small facial expression image dataset with frontal faces only. Points of correspondence are placed per image so the dataset can be readily used for building statistical shape models.
[112]	Face images dataset	20,000	-	I, O	✔	✔	✔	**UTKFace** is the face images containing annotations for age, gender, ethnicity, and landmarks (68 points). It covers various face poses, expressions, resolution, and age span (0-116 years old). However, it has frontal faces without multi-instances and number of subjects (not shown).
[122]	Face images dataset	1.5m	-	I, O	✔	✔	✔	**FDF,** a large face image dataset, has 1.5m faces in the wild, with diversity such as face poses, age, ethnicity, occlusion, and backgrounds. Annotated for 7 facial landmarks, ear, eye, shoulder, nose, and face. Most cases are limited to only one face per image and frontal faces.

5 Domains and Applications

With the ever-increasing growth of big data generation, IoT devices, smart city frameworks, powerful machines, cloud services, and advances in DL, the application aspect of FDeID has also been increasing—particularly applications within law enforcement, healthcare, sports, and entertainment, described as follows.

5.1. Potential Applications in Law Enforcement

Law enforcement agencies use security cameras to deter criminals and collect evidence [123] but these cameras indiscriminately capture data, intruding on the privacy of innocent bystanders. De-identification, especially reversible methods such as in [124], can record spatial areas whilst maintaining the privacy of anyone captured by the camera. If a crime is discovered in the video footage, then it may be possible for the police or approved security personnel to reverse the de-identification (e.g., face mask) using a key, such as in [124].

Developments in the Internet of Things (IoT) have further driven the adoption of security monitoring devices, such as video cameras, in homes [125]. A particular issue that affects such IoT devices is security attacks aimed at gaining unauthorised access to video streams. Despite its limitations, PDeID would present one measure towards maintaining partial privacy in the event of such an attack. Reversible de-identification would present the possibility of ensuring that only authorised people, such as the homeowner or security services, could access the original video (*i.e.*, without de-identification).

Similarly, PDeID is widely used for security purposes at airports, railway stations, and shopping centres [126]. Such applications capture people and pose potential ethical concerns. Reversible de-identification in this context may allow security personnel access to the relevant data while ensuring privacy when the data is de-identified. Such applications are also likely to gather significant footage of people as they walk. Gait, the manner of a person's walking, is a biometric feature that can provide clues to their identity, specifically by utilizing machine learning [126]. Therefore, in addition to de-identifying detected faces, de-identification of body parts, e.g., limbs, would also be required.

A proposed potential security application is Reversible Chaotic Masking [128]. It scans foreground objects to identify faces and windows (on buildings) using DNN. The

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

faces and windows are irreversibly scrambled to improve privacy, where authorised personnel can access the images, and only crime suspects' faces are revealed. However, the generated images are unnatural in appearance and do not protect against gait identification or other non-facial visual clues such as clothing. Moreover, the current system does not implement reversible scrambling of images, resulting in images that cannot be easily unscrambled, potentially hiding criminal evidence. Furthermore, the suspects' faces are not scrambled. This poses potential privacy issues in cases of false identification.

An alternative solution is proposed in [129] with a conditional GAN used to obtain a synthetic face using an encoder to hide the identity of the people and maintain a natural look to the image. Unlike [128], the hiding of faces can be reversed using a decoder by authorised personnel with a valid key. Despite the advantages of reversible face masking in this solution, it does not provide protection against methods such as gait identification or hide additional visual clues such as clothing.

5.2. Potential Applications in Healthcare

Falls can result in serious health problems, particularly for the elderly [130], resulting in approximately 684,000 yearly deaths [131]. Computer vision methods, combined with ML classification, have been suggested as an appropriate fall detection method in assisted living [132], allowing appropriate personnel to be alerted in the event of a fall. Although such a system can potentially improve the safety of the elderly and disabled, it also presents serious ethical concerns, such as an invasion of privacy. PDeID methods provide a potential solution to such privacy concerns [133], but further work may be required to ensure that de-identification methods do not interfere with the safety and accuracy of the fall detection solutions.

Similarly, a related healthcare application that poses privacy issues is emotion detection for suicide prevention [134]. Emotional states have been shown to be identifiable using computer vision and ML [135]. Such solutions could identify people at risk of suicide, e.g., in schools, hospitals, and prisons, and alert relevant professionals. In [136], it is reported that FDeID is possible while preserving emotion and non-biometric facial features. However, other biometric features, such as gait, are not de-identified, and therefore, further work is required to ensure that such solutions can identify those at risk while maintaining privacy.

5.3. Advertisement/ Entertainment Applications

Improvements in eye and gaze tracking have resulted in increasing applications for tracking peoples' attention to advertisements for shopping [137], tourism [138], and more. Such applications involve gathering images of pedestrians in public environments, posing privacy and ethical issues. A potential solution is presented in [139], where faces are de-identified, but facial expressions and gaze are preserved, thus improving privacy without removing the ability to perform gaze detection. However, such methods may provide weaker de-identification as some facial features are not hidden, such as the hairstyle, presenting clues about the person's identity [24].

5.4. Social Media Applications

Face identification is commonly used on social media platforms for profile matching [140], person identification [141], and attributing posts to known people [142]. Several methods are proposed for preserving privacy in social media images, such as [143] and [144]. The solutions achieve natural-looking images with faces altered to change the appearance significantly. By providing a measurable obfuscation method, users can balance the level of privacy required with the desired image quality.

However, [145] suggests that even with faces completely removed from an image, people can routinely identify people based on clues such as body type and clothing. Therefore, it is likely that further de-identification is necessary to achieve significant levels of privacy, for example, via the obfuscation of further identifiable characteristics such as hairstyle, body type, and clothing.

6. Ethical Considerations in Face Identification

The person identification using facial recognition market has grown significantly in recent years, showing around $3.2 billion in 2019. It is expected to grow to $7 billion by 2024, with an estimated growth rate of 16.6%/annum in 2024 [146]. The utilisation of Facial Recognition Technology (FRT) showed promising results in identifying individuals and indicated significance in assisting law enforcement professionals (e.g., in the US and UK) [147]; however, there are other occasions where the use of FRT is considered harmful [148] as well as nonconsensual [149].

As such, increasing use of FRT is concerning due to its inaccuracies, which can exacerbate social inequalities, particularly in identifying communities of colour [150]. In this regard, Bacchini et al. [151] reported that FRTs affect the black community more because they have comparatively more data in law enforcement databases, and FRTs are not well-trained on people of many colours. This leads to frequent misidentifications due to the challenge of differentiating darker complexions using facial features. Klare et al. [152] benchmarked six facial recognition algorithms, which show significant degradation in accuracy for dark complexion compared to other racial communities. It should be noted that most FRTs are trained on Caucasians and East Asians [153], leading to improved recognition of such ethnicities compared to other racial groups.

Another important dimension requiring further investigation is the lack of regulatory measures that enable commercial organisations to work without legal constraints. For instance, FRT provided organisations with details about their customers' behaviour without legal consent. Customers' photographs and personal details can be forwarded to FRT to alert retailers when their customers enter the retail shops for improved customer service. Even though such actions can improve and tailor customer services, it is also regarded as violating privacy and the consumers' trust in their retailers [154].

The FRT is also expected to play an important role in

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

healthcare, such as diagnosing genetic disorders, monitoring patients, and providing details about health, e.g., age and pain experience. Due to these utilisations in health care, informed consent is required for collecting and archiving patients' visual information. However, patients could be unaware that their images are used for diagnoses [155]. As ML systems need updating by training and validation with various patients' images, this could raise the issue that informed consent may not be regarded as necessary. Hence, related industries and healthcare organisations are required to work in collaboration and to inform patients of ethical consent and outcomes. Boczar et al. [156] showed that healthcare clinicians need to be aware of the implications of using face recognition systems in medical settings where patient images collected and used for research need the patients' consent. Study also reported concerns when FRT is developed to replace nursing assessments and clinician diagnoses.

TABLE 3
ETHICAL CONSIDERATION AND RELATED CHALLENGES IN FACIAL RECOGNITION TOOLS AND RESEARCH STUDIES

Study	Year	Ethical aspects covered
[160]	2022	AI and the ethical issues are discussed, such as endogenous, the inability to predict and stability
[161]	2020	Identified ethical issues for face recognition algorithms for people with plastic
[162]	2019	Applications of FRT in health care settings and the ethical concerns
[163]	2019	Provided details about the issues of face recognition and ethical consent with examples
[157]	2020	The role of researchers in eliminating the unethical utilisation of AI for face recognition.
[158]	2022	Privacy and security and public safety
[156]	2021	Healthcare and ethical considerations for FRT
[164]	2022	Ethical considerations for AI are discussed, particularly for face recognition and the effects of the utilised datasets.
[165]	2021	The authors indicated the use of Homomorphic Encryption to preserve the privacy of individuals for face recognition and eliminate ethical issues.
[166]	2020	The paper indicated ongoing research in this domain despite the concerns surrounding ethical issues due to the use of technology for FRT.
[167]	2020	The concern of utilising face recognition by the police.
[168]	2022	Study indicated the balance of utilising face recognition despite its ethical issues in delivering social safety.
[169]	2020	Ethics of face recognition on vulnerable populations.

In [157], a survey study involving 480 researchers in image processing, facial recognition, AI, and computer science. This study reported a disagreement with the lack of ethical consideration of facial recognition works. Considering the wider scope of FRT, [158] three main issues to consider are privacy, security, and public safety. The study also revealed that privacy rights are important due to correspondence with autonomy. National biometric facial recognition database that can be used to combat serious crimes and in relation to suitable accountability mechanisms could be considered tolerable; however, utilising a large number of images from social media databases (such as Clearview AI's technology) to find minor violations is considered unacceptable. The study also concluded that FRT provides a vital influence on security; however, its use in safety is not obvious.

Table 3 shows recent studies addressing the ethical issues in relation to person identification and facial recognition. In summary, there are various potential issues related to the use of FRT, including the incorporation of ethnicity, gender, and sexual preferences in decision making which could lead to discrimination and inequality in society. Another concern involves distributing people's private data due to collecting massive amounts of biomedical information about individuals. As facial data may be collected without the person's consent, such as the collection of facial images from CCTV cameras and mounted cameras in the street that can be used by researchers for image and face recognition, this could be considered forced consent rather than approved consent for the handling of the identifiable information [159].

Finally, in comparison with the EU, USA, and China, the EU is currently playing a major role in the enforcement of personal and identifiable information protection and regulating the utilisation of AI in face recognition. In the USA, certain states started using legislation to collect and process biomedical data in commercialised applications. On the other hand, in China, there are no specific restrictions on the use of FRT; therefore, the system is widely used in various communities, public institutions, government bodies, and businesses.

7. DISCUSSIONS ON KEY INSIGHTS AND ADVANCING RESEARCH FRONTIERS OF PDEID

This survey covers multiple dimensions of PDeID, specifically FDeID, focusing on technical methods, datasets, new applications, and ethical concerns. We address strengths and research gaps within these dimensions, which might be of significant interest to the diverse community. These outcomes are useful for advancing the research frontiers of FDeID towards the fully autonomous, adaptive, non-invasive, and unrestricted approaches while considering the growing interest in this field and big data generated through various means and surveillance technologies.

7.1. FDeID Approaches: Potential Gaps and Recommended Research Questions (RQs)

7.1.1. Divergent Obfuscation: In works such as [136], [51], [59], faces are masked to hide the person's identity; however, if the same obfuscated artificial face is created for the same person each time, there may still be identity clues. For example, the routine of the person (such as daily visiting a place) or co-occurrences of people may provide clues to either or both of their identities (*i.e.*, two or more people who spend substantial time together). Therefore, it may be necessary to ensure that each occurrence of an individual is de-identified uniquely.

RQ1: How can dynamic PDeID methods uniquely obfuscate each occurrence of an individual's face, preventing identity clues from routines or co-occurrences?

7.1.2. Outlook de-identification: Although FDeID is the most common approach to de-identifying still images, [145] suggests that humans can often identify people via

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

the body and clothing. Therefore, only FDeID is unlikely to achieve significant privacy improvements, and de-identification methods should also de-identify other identifiable characteristics such as body type and clothing. It maintains a natural look to an image after such significant de-identification, which is a non-trivial problem.

RQ2: How can PDeID methods be improved to obfuscate identifiable characteristics, e.g., body type and clothing, while maintaining a natural look in visuals?

7.1.3. Reversible de-identifications: Reversible gait de-identification significantly alters body parts to obscure identifiable gait characteristics [170], providing privacy while still allowing police to identify criminals and missing persons.

FDeID methods, like replacing instead of blurring images, aim to maintain a natural appearance [129]. This approach is more challenging for gait de-identification, as changing body appearance alone won't hide identifiable gait characteristics. Future work should explore balancing thorough de-identification with maintaining a natural look.

RQ3: How can reversible gait de-identification effectively obscure identifiable gait patterns while maintaining the natural appearance of images and still allow identification to law enforcement when necessary?

PDeID poses ethical issues by enabling the posting of unsuitable content like hate speech and reducing the chance of offenders being identified and penalized. This issue may be addressed using reversible de-identification, such as in [124] however, challenges exist when offenders use de-identification to be anonymized.

RQ4: How can reversible de-identification prevent offenders from using PDeID to post prohibited content anonymously while allowing authorities to identify them?

7.1.4. Footstep de-identification: Several works have highlighted the potential of footstep sounds for PDeID [171] [172] [173]. Despite this, to the best of the authors' knowledge, no attempts have been made to de-identify footsteps. One solution is removing all audio or just the footstep sounds, which would lead to unnatural recordings. Alternatively, distorting the footstep sounds might help, but even simple distortions could reveal the identity through the rhythm. Thus, sufficiently altering the sounds for PDeID may also result in unnatural audio.

RQ5: How can footstep sounds be effectively de-identified to obscure the walker's identity while maintaining natural-sounding audio in recordings?

Similarly, other identifying factors, such as scars and tattoos, have been shown as clues to a person's identity [133]. However, none of the existing PDeID methods address such identifiable features.

RQ6: How can de-identification methods be improved to obscure identifiable features like scars and tattoos effectively?

7.1.5. Diversity context: EDI (Equality, Diversity, and Inclusion) is crucial in our social lives to build inclusive communities and promote social justice. In AI, it ensures fair and unbiased outcomes, fostering innovation and equity. In FDeID, this can be achieved by considering several factors, e.g., socio-demographic attributes (e.g., ethnicity, gender, age, etc.) and environment (e.g., occluded).

RQ7: How can DL models be employed to explore the impact of socio-demographic attributes and environment on the performance of FDeID approaches?

7.1.6. Multi-perspective multi-instance: Most of the trained DL models use single-view faces (e.g., frontal perspective), which is uncommon in realistic environments. Likewise, with the growing smart city infrastructure, IoT, and video surveillance, the existing FDeID methods are inappropriate for handling multi-person (*i.e.*, multiple faces) scenes. Further investigations are required to explore the utilisation of state-of-the-art computer vision approaches to handle this challenge.

RQ8: How can state-of-the-art DL approaches improve FDeID methods to handle realistic dynamics, e.g., multi-perspective and multi-instance scenarios?

7.1.7. Uncertainty and Real-time dynamics: To the best of the authors' knowledge, existing works are lacking to handle the dynamics of realistic scenarios such as occlusions (in faces or body segments) and make tracking and obfuscation more challenging. Further research is required to investigate the use of dynamic state estimation models (e.g., Kalman filter, probabilistic methods) equipped with spatial-temporal DL methods to perform better in real-time dynamic and uncertain conditions.

RQ9: How can dynamic state estimation and spatial-temporal DL methods be combined to improve tracking and obfuscation under occluded conditions?

7.1.9. Adaptivity: To the best of the authors' knowledge, none of the existing approaches address the 'Adaptive AI' aspects, which may be useful for FDeID performance improvements. For instance, biometrics (e.g., face, gait, etc.) may adapt to several factors such as age, illness, emotions, cognitive condition, and environment. Further investigations are needed to address the utilisation of adaptive AI for the FDeID, particularly to better handle the real-time dynamics and further developments in this area.

RQ10: How do factors such as age, illness, emotions, cognitive condition, and environment impact FDeID performance, and how can adaptive AI address these in real time?

7.1.10. Transparent and trustworthy: Currently, explainable and interpretable AI are the major topics in AI, yet they are not addressed in the reviewed literature. Further investigations will help advance this domain, supporting human-in-loop AI and enabling the transparent and trustworthy AI goals set by the government authorities, such as the national AI strategy published by the UK parliament [174].

RQ11: How can explainable and interpretable AI be utilized in FDeID methods to support human-in-the-loop decision-making and achieve transparent, trustworthy AI?

7.1.11. Non-invasive non-restraining abilities: Whilst few studies, such as [6], [26], [28] address the unrestrictive FDeID; they only cover multiple viewing angles. We highly recommend using multi-modal methods along with a generalised dataset (see dataset Section 4) to set the foundations for a fully non-restraint, non-invasive FDeID approach. For instance, multi-modal DL methods can be used to classify camera perspective, followed by a face segmentation model, for better automation and adaptation to multi-view camera perspectives (like real-world

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

scenarios).

RQ12: How can multi-modal DL methods be utilized to establish an unrestricted, non-invasive FDeID approach, considering 360° camera perspectives of real-world environments?

7.2. Data Assets (Gaps and Recommendations)

The datasets used for PDeID are summarized in Table 2, mainly in terms of potential uses, size, availability, diversity, camera view, availability, the capturing environment, and other aspects (e.g., 2D/3D etc.). Based on our detailed review, we recommend the following new dimensions that might be useful for advancing the existing datasets and better training of DL models for the PDeID tasks.

7.2.1. Non-Restraining, Multiview, Multi-poses: Despite some of the existing datasets, such as LFW [95] and FDDB [115], include non-restrained faces, which predominantly consist of frontal and perspective views. To the best of the authors' knowledge, no existing datasets in the context of FDeID cover 360° perspective, encompassing varying camera views (e.g., bird's-eye, perspective, etc.). The limitation also extends to full body and gait datasets such as PEViD [114] (9 participants only), which we encourage the research community to acknowledge as potential research gaps. For example, a common challenge in human pose estimation is its difficulty in handling unconventional poses, such as individuals being upside down or engaging in dynamic perspectives (e.g., yoga exercises).

RQ13: How can the generation of primary datasets covering 360° perspectives and unconventional body poses improve the performance of FDeID and human pose estimation models?

7.2.2. Multi-instance: Datasets such as PIPA [100], Wider Face [101], MALF [102], and FDDB [115] contain multiple faces per image however, additional datasets addressing this concern are highly required to train large models. In realistic environments, application points of view, and generalised performance, training of the DL models must undergo using multi-instance and realistic datasets.

RQ14: How can additional multi-instance datasets (acquired in realistic conditions) improve the training and performance of DL models for the FDeID in realistic environments?

7.2.3. Occlusion and Uncertainty: Existing FDeID and related privacy protection techniques significantly lack addressing the occlusion problem commonly occurring in real-world environments (e.g., video surveillance) in various forms, such as half faces (covered by other faces), objects hiding the faces, a person passing behind an obstruction (e.g., tree) etc. There are some efforts to address the occlusion in the literature, such as UTKFace [112], RAF-DB [74], ChokePoint [89], Clothing Co-Parsing [103]; however, these datasets are either small, less diverse, or captured in a controlled environment (e.g., indoor, static background).

Furthermore, no existing datasets include images of faces or full bodies captured alongside the shadows, which are common in realistic environments and could potentially affect the performance of FDeID methods.

RQ15: How can the development of larger and diverse datasets addressing the challenges of occlusion and shadowing improve the performance of FDeID methods in realistic conditions?

7.2.4. Sociodemographic diversity: Several datasets, such as MORPH [92], RAF-DB [74], and MUCT [94], aim to encompass diversity in terms of age, gender, and ethnicity. However, the literature of datasets contains a notable scarcity, mainly for human gait and full body poses captured from diverse populations with balanced distribution [175]. Video datasets such as PEViD [114] reported some diversity; however, it was limited to a small sample size (9 participants only) and did not adequately represent the full spectrum of diversity within the population. Furthermore, style (e.g., clothes, shoes), height, and BMI are the attributes significantly influencing the gait and pose datasets [176], which are largely underrepresented or unavailable.

RQ16: How can the development of more diverse and balanced datasets, including attributes such as style, height, gender, ethnicity, and BMI etc., improve the performance of face and gait-based privacy preservation methods?

7.2.5. Full body poses and high dimensional datasets: It can be noted from Table 2 (and Fig.4) that only 18% of the datasets cover the full body dataset. Also, only 5% of the reviewed datasets comprise 3D facial images or full-body poses. This clearly shows a need to acquire a comprehensive dataset of 3D videos and full-body poses along with real-time dynamics mentioned in this section.

This, furthermore, applies to the gait datasets as reported in our recent compilation of a world-class gait dataset [176]. This would undoubtedly enhance the performance, reliability, and generalisation improvements of the DL-based FDeID approaches, specifically in real-world applications where 3D datasets are significant for geometric map generation and various applications.

RQ17: How can the acquisition of comprehensive 3D video datasets with full-body poses enhance the performance, reliability, and generalization of DL-based FDeID?

7.2.6. Environmental factors: Whilst 55% of the datasets in Table 2 were captured in an outdoor environment with varying backgrounds (66%), almost half of the datasets were captured in an indoor environment or static background. This puts limits on the FDeID model's generalisation ability in realistic environments. To advance the research frontiers of PDeID and privacy preservation, there is a drastic need to consider the dynamic factors while composing face or body datasets, such as busy outdoor environments with noisy backgrounds (e.g., urban areas), varying weather conditions (e.g., rainy, foggy, snowy), lightening & illuminations (e.g., sunlight), shadows etc.

RQ18: How can the inclusion of dynamic factors such as noisy and diverse backgrounds and varying weather and lighting conditions in datasets improve the generalization ability of FDeID and PDeID methods in realistic environments?

8. Conclusions and Takeaway From Study

This study comprehensively explores PDeID and, mainly, FDeID using technological methods. The study also extensively reviews available data assets, technical approaches, ethical aspects, and potential applications. Specifically, it provides a detailed examination of FDeID methods and solutions critical for implementing the machine-based PDeID and privacy protection techniques (Section 3 and Table S2 in SuppM). The survey includes a

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

comparative analysis between traditional computer vision methods and the advanced DL-based approaches for the FDeID, emphasising the latter's advantages. From a technical perspective, we have identified several limitations in the existing FDeID methods and, therefore, provided a variety of research directives (Section 7) that will be of significant use to the research community and associated stakeholders. The highlighted recommendations will be useful to advance the research frontiers of PDeID, paving the pathway towards fully autonomous, non-invasive, non-restraining, reliable PDeID methods.

Further, from a technical perspective, this study performs an in-depth review of available datasets (Section 4, Table 2, and Appendix A in SuppM). It provides a comparative analysis for the readers, presenting all-in-one insights into datasets and associated properties. We identify existing datasets' limitations and provide several possible contributions and recommendations (Section 7) to improve them. This mainly includes multi-instance, occluded, multi-pose, and multi-perspective data assets compilation, which has uses in interdisciplinary domains (e.g., healthcare, social sciences, sports, etc.) and possesses high importance for enhancing the generalisation of ML-based FDeID.

The survey also highlights the ethical issues in the related domains and potential applications of FDeID (Section 6), particularly within law enforcement, healthcare, and social media. For instance, we propose potential security applications using reversible chaotic masking to identify people at risk of suicide, e.g., in schools, hospitals, and prisons, and alert relevant professionals. Likewise, other biometrics, such as gait, are not de-identified in most applications, requiring further work to ensure privacy protection. Moreover, this study suggests that even with faces wholly removed from an image, humans can routinely identify people based on clues such as body type and clothing. Therefore, further de-identification is likely necessary to achieve significant levels of privacy, for example, by obfuscating further identifiable characteristics such as hairstyle, body type, and clothing.

Finally, the review results are presented in a readily comprehensible format, such as comparative tables and visualisations, making them accessible to non-technical readers and professionals in relevant fields (e.g., law enforcement, healthcare professionals, etc.). Identifying technical shortcomings within the existing literature across various dimensions and recommending numerous potential research directions holds significant value for the research community and a wide-ranging audience.

REFERENCES

[1] M. Police, "Force Management Statement," Metropolitan Police, 2021.

[2] E. P. Office, "General Data Protection Regulation," *Official Journal of the European Union,* vol. 59, 2016.

[3] A. Prachi and P. J. Narayanan, "Person De-Identification in Videos," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 21, pp. 299-310, 2011.

[4] L. Yifang, V. Nishant, K. B. P., H. Hongxin and C. Kelly, "Blur vs. Block: Investigating the Effectiveness of Privacy-Enhancing Obfuscation for Images," in *2017 IEEE CVPR*, Honolulu, HI, USA, 2017.

[5] J. Lin, Y. Li and G. Yang, "FPGAN: Face de-identification method with generative adversarial networks for social robots," *Neural Networks,* vol. 133, pp. 132-147, 2021.

[6] K. Brkic, I. Sikiric, T. Hrkac and Z. Kalafatic, "I know that person: Generative full body and face de-identification of people in images," in *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, Honolulu, HI, USA, 2017, July.

[7] F. Ivan, K. Zoran and H. Tomislav, "Deep metric learning for person Re-identification and De-identification," in *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia, 2016.

[8] A. Imran, S. Keith and W. Andrew, "Surveillance and the 'Monitoring' of Citizens by the State," in *Terrorism in the Classroom: Security, Surveillance and a Public Duty to Act*, Cham, Springer International Publishing, 2019, pp. 43-59.

[9] S. Hazim, A. H. Sawalmeh, A.-F. Ala, D. Zuochao, A. Eyad, K. Issa, O. N. Shamsiah, K. Abdallah and G. Mohsen, "Unmanned Aerial Vehicles (UAVs): A Survey on Civil Applications and Key Research Challenges," *IEEE Access,* vol. 7, pp. 48572-48634, 2019.

[10] S. Rick and P. Tim, "Policing and security," in *Australian Policing*, 2020, pp. 221-235.

[11] C.-B. Karine, I. Federica and S. Mark, "Border security as practice: An agenda for research," *Security Dialogue,* pp. 195-208, 2014, 06.

[12] K. Juraj, et al, "AMZ driverless: The full autonomous racing system," *Journal of Field Robotics,* vol. 37, no. 7, pp. 1267-1294, 08 2020.

[13] M. Simone, et al, "Robotics and Autonomous Systems," *Robotics and Autonomous Systems,* vol. 74, no. 3, 07 2015.

[14] S. P. Mohanty, U. Choppali and E. Kougianos, "Everything you wanted to know about smart cities: The Internet of things is the backbone," *IEEE Consumer Electronics Magazine,* vol. 5, no. 3, pp. 60-70, 2016.

[15] "Why Police Cover the Face of Accused – Law of Presumption of Innocence," 07 05 2019. [Online]. Available: https://legalversity.com/why-police-cover-the-face-of-accused-law-of-presumption-of-innocence.

[16] V. Mladenovic, S. Djukanovic, N. Stefanovic, A. Kar, M. Jovanovic and S. Makov, "Kids security on social networks by face blur technique," *IOP Conference Series: Materials Science and Engineering,* vol. 1029, p. 012042, jan 2021.

[17] A. R. Ali and B. N. Dhannoon, "Real Time Multi Face Blurring on Uncontrolled Environment based on Color Space algorithm," *Iraqi Jr. of Sci.,* pp. 618-1626, 2019.

[18] F. S. Al-Mukhtar, "Tracking and Blurring the Face in a Video File," *Al-Nahrain Journal of Science,* no. 1, pp. 202-207, 10 2018.

[19] A. Besmer and L. R. Heather, "Tagged photos: concerns, perceptions, and protections," *Extended Abstracts on Human Factors in Comp. Sys,* pp. 4585-4590, April 2009.

[20] P. Ilia, I. Polakis, E. Athanasopoulos, . F. Maggi and . S. Ioannidis, "Face/Off: Preventing Privacy Leakage From Photos in Social Networks," in *Proc. 22nd ACM SIGSAC Conf. Comp. and Comm. Security*, 2015, October.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

[21] D. Frédéric and E. Touradj, "A framework for the validation of privacy protection solutions in video surveillance," in *2010 IEEE Conf. Multimedia and Expo*, Singapore, 2010.

[22] C. . G. Neustaedter, S. Greenberg and . M. J. Boyle, "Blur filtration fails to preserve privacy for home-based video conferencing," *ACM Transactions on Computer-Human Interaction,* vol. 13, no. 1, pp. 1-36, March 2006.

[23] M. J. Boyle, C. Edwards and . S. Greenberg, "The effects of filtered video on awareness and privacy," in *Proceedings of the 2000 ACM conference on Computer supported cooperative work*, New York, 2000, December.

[24] E. M. Newton, L. Sweeney and . B. Malin, "Preserving privacy by de-identifying face images," *IEEE Transactions on Knowledge and Data Engineering,* vol. 17, no. 2, pp. 232-243, 2005.

[25] Z. Fuzhen, Q. Zhiyuan, D. Keyu, X. Dongbo, Z. Yongchun, Z. Hengshu, X. Hui and H. Qing, "A Comprehensive Survey on Transfer Learning," *Proceedings of the IEEE,* vol. 109, pp. 43-76, 2021.

[26] R. Gross, E. Airoldi, B. Malin and L. Sweeney, "Integrating Utility into Face De-identification," in *International Workshop on Privacy Enhancing Technologies PET 2005: Privacy Enhancing Technologies*, Berlin, Heidelberg, 2005.

[27] R. McPherson, R. Shokri and V. Shmatikov, "Defeating image obfuscation with deep learning," *arXiv preprint arXiv:1609.00408,* 2016.

[28] J. Li, Y. Zhou, . J. Ding, C. Chen and X. Yang, "ID preserving face super-resolution generative adversarial networks," *IEEE Access,* vol. 8, pp. 138373-138381, 2020.

[29] C. Hymas, "Police waste hours pixelating body camera footage instead of fighting crime," Yahoo news, 2022.

[30] C. Hymas, "Police waste hours pixelating body camera footage instead of fighting crime," Telegraph, 2022.

[31] S. Ribaric and N. Pavesic, "An overview of face de-identification in still images and videos," in *2015 11th IEEE Conference and Workshops on Automatic Face and Gesture Recognition (FG)*, Slovenia, 2015.

[32] S. Ribaric, A. Ariyaeeinia and N. Pavesic, "De-identification for privacy protection in multimedia content: A survey," *Signal Proc: Image Comm.,* vol. 47, 6 2016.

[33] J. Padilla-López, A. Chaaraoui and F. Flórez-Revuelta, "Visual Privacy Protection Methods: A Survey," *Expert Systems with Applications,* 06 2015.

[34] B. Meden, et al, "Privacy–Enhancing Face Biometrics: A Comprehensive Survey," *IEEE Trans. Information Forensics and Security,* vol. 16, pp. 4147-4183, 2021.

[35] K. Chinomi, N. Nitta, Y. Ito and N. Babaguchi, "PriSurv: Privacy Protected Video Surveillance System Using Adaptive Visual Abstraction," in *Int. Conf. MMM 2008: Advances in Multimedia Modeling*, Heidelberg, 2008.

[36] P. Minary, F. Pichon, D. Mercier, É. Lefèvre and B. Droit, "An Evidential Pixel-Based Face Blurring Approach," in *International Conference on Belief Functions: Theory and Applications*, Cham, 2016, September.

[37] D. Alexandre, P. Nicolas, P. Frederic and C. Bertrand, "Face blurring for privacy in street-level geoviewers combining face, body and skin detectors," in *Proceedings of the 11th IAPR Conference on Machine Vision Applications, MVA 2009*, 2009, Jan.

[38] P. A. Viola and M. J. Jeffrey, "Robust real-time face detection," *International journal of computer vision,* vol. 57, no. 2, p. 37–154, 2004.

[39] C. Varun, G. Chuhan, T. Brian, F. Kassem, J. Somesh and B. Suman, "Face-off: Adversarial face obfuscation," in *Proceedings on Privacy Enhancing Technologies.*, 2020.

[40] E. Ádám, B. Tibor, V. Patrick, W. Thomas and R. Bernhard, "Adaptive cartooning for privacy protection in camera networks," in *2014 11th IEEE Conf. AVSS*, Seoul, Korea (South), 2014.

[41] J. Hao and Y. Tao, "Adversarial facial obfuscation against unauthorized face recognition," *Journal of Physics: Conference Series,* vol. 1903, p. 012026, April 2021.

[42] Y. Li and S. Lyu, "De-identification without losing faces," in *Proceedings of the ACM Workshop on Information Hiding and Multimedia Security*, 2019, July.

[43] W. Shen, Z. Wu and J. Zhang, "A face privacy protection algorithm based on block scrambling and deep learning," in *Cloud Computing and Security*, vol. 11065, S. Xingming, P. Zhaoqing and B. Elisa, Eds., Springer International Publishing, 2018, pp. 359-369.

[44] W. Ethan, S. Frederick, S. Jenny and J. Eakta, "Practical Digital Disguises: Leveraging Face Swaps to Protect Patient Privacy," 2022.

[45] B. Zhu, H. Fang, Y. Sui and L. Li, "Deepfakes for medical video de-identification: Privacy protection and diagnostic information preservation," in *Proc. AAAI/ACM Conf. AI, Ethics, and Society*, NY, US, 2020, February.

[46] K. Brkić, T. Hrkać and Z. Kalafatić, "Protecting the privacy of humans in video sequences using a computer vision-based de-identification pipeline," *Expert Systems with Applications,* vol. 87, pp. 41-55, 2017.

[47] B. Karla, H. Tomislav, S. Ivan and K. Zoran, "Towards neural art-based face de-identification in video data," in *2016 1st Int Workshop on Sensing, Proc. and Learning for Int. Machines (SPLINE)*, Aalborg, Denmark, 2016.

[48] S. Terence and Z. Li, "Controllable Face Privacy," in *2015 11th IEEE Conference and Workshops on Automatic Face and Gesture Recognition*, Ljubljana, Slovenia, 2015.

[49] T. Sim, S. Zhang, J. Li and Y. Chen, "Simultaneous and orthogonal decomposition of data using Multimodal Discriminant Analysis," in *2009 IEEE 12th International Conference on Computer Vision*, Kyoto, 2009.

[50] T. Cootes, G. Edwards and . C. Taylor, "Active appearance models," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 23, no. 6, pp. 681-685, 2001.

[51] O. Gafni, L. Wolf and Y. Taigman, "Live face de-identification in video," in *2019 IEEE/CVF Int. Conf. on Comp/ Vision (ICCV)*, Seoul, Korea (South), 2019.

[52] H. Uchida, N. Abe and S. Yamada, "DeDiM: De-identification using a diffusion model," in *2022 IEEE BIOSIG*, Germany, 2022.

[53] Y. Xingyi, X. Zhao, Y. Wang and W. Sun, "Generation of Face Privacy-Protected Images Based on the Diffusion Model," *Entropy,* vol. 26, no. 6, 2024.

[54] Ž. Babnik, P. Peer and V. Štruc, "eDifFIQA: Towards Efficient Face Image Quality Assessment Based On Denoising Diffusion Probabilistic Models," *IEEE Transactions BIOD,* 2024.

[55] J. Sohl-Dickstein, E. Weiss, N. Maheswaranathan and S. Ganguli, "Deep Unsupervised Learning using

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

Nonequilibrium Thermodynamics," in *International Conference on Machine Learning*, 2015.

[56] W. Yunqian, L. Bo, D. Ming, R. Xie and S. Li, "IdentityDP: Differential private identification protection for face images," *Neurocomputing,* vol. 501, 2022.

[57] W. L. Croft, J.-R. Sack and W. Shi, "Obfuscation of images via differential privacy: From facial images to general images," *Peer-to-Peer Networking and Applications,* vol. 14, p. 1705–1733, 2021.

[58] G. Ian, et al., "Generative Adversarial Networks," *Advances in Neural Inf. Processing Sys,* vol. 3, no. 11, 06 2014.

[59] Y. Wu, F. Yang, Y. Xu and H. Ling, "Privacy-protective-GAN for privacy preserving face de-identification," *Journal of Comp. Sci and Tech,* vol. 34, pp. 47-60, 2019.

[60] H. Nguyen, . D. Zhuang, . P.-Y. Wu and . M. Chang, "Autogan-based dimension reduction for privacy preservation," *Neurocomputing,* vol. 384, pp. 94-103, 2020.

[61] S. Karen and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," in *ICLR*, 2014.

[62] R. Olaf, F. Philipp and B. Thomas, "U-Net: Convolutional Networks for Biomedical Image Segmentation," in *MICCAI 2015*, Cham, 2015.

[63] A. Aggarwal, R. Rathore, P. Chattopadhyay and L. Wang, "Epd-net: a gan-based architecture for face de-identification from images," in *2020 IEEE Conference (IEMTRONICS)*, Vancouver, BC, Canada, 2020, September.

[64] C. Ionescu, D. Papava, V. Olaru and C. Sminchisescu, "Human3.6M: Large Scale Datasets and Predictive Methods for 3D Human Sensing in Natural Environments," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 36, no. 7, pp. 1325-1339, July 2014.

[65] S. Qianru, M. Liqian, S. J. Oh, L. V. Gool, B. Schiele and M. Fritz, "Natural and Effective Obfuscation by Head Inpainting," in *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, UT, USA, 2018.

[66] Y. Li, Q. Lu, Q. Tao, X. Zhao and Y. Yu, "SF-GAN: face de-identification method without losing facial attribute information," *EEE Sig. Proc. Lett,* vol. 28, 2021.

[67] V. Mirjalili, S. Raschka and A. Ross, "PrivacyNet: Semi-Adversarial Networks for Multi-Attribute Face Privacy," *IEEE Tran. on Img. Proc,* vol. 29, pp. 9400-9412, 2020.

[68] Z. Kuang, Z. Guo, J. Fang, J. Yu, N. Babaguchi and J. Fan, "Unnoticeable synthetic face replacement for image privacy protection," *Neurocomputing,* vol. 457, pp. 322-333, 2021.

[69] H. Hukkelås, R. Mester and F. Lindseth, "DeepPrivacy: A Generative Adversarial Network for Face Anonymization," in *Advances in Visual Computing*, Cham, 2019.

[70] J. Li, L. Han, R. Chen, H. Zhang, B. Han, L. Wang and X. Cao, "Identity-preserving face anonymization via adaptively facial attributes obfuscation," in *Proceedings of the 29th ACM Conference on Multimedia*, 2021, October.

[71] M. Khamis, . H. Farzand, . M. Mumm and K. Marky, "DeepFakes for Privacy: Investigating the Effectiveness of State-of-the-Art Privacy-Enhancing Face Obfuscation Methods," in *Proceedings of the 2022 International Conference on Advanced Visual Interfaces*, 2022, June.

[72] V. Mirjalili, S. Raschka, A. Namboodiri and A. Ross, "Semi-adversarial networks: Convolutional autoencoders for imparting privacy to face images," in *In 2018 International Conference on Biometrics (ICB)*, Cold Coast, QLD, Austrailia, 2018.

[73] B. Meden, R. C. Mallı, S. Fabijan, H. K. Ekenel, V. Štruc and P. Peer, "Face deidentification with generative deep neural networks," *IET Signal Processing,* vol. 11, no. 9, pp. 1046-1054, 2017.

[74] S. Shan, W. Deng and J. Du, "Reliable Crowdsourcing and Deep Locality-Preserving Learning for Expression Recognition in the Wild," in *2017 IEEE Conf. on Comp. Vision and Pattern Recog*, Honolulu, USA, 2017.

[75] B. Meden, M. Gonzalez-Hernandez, P. Peer and V. Štruc, "Face deidentification with controllable privacy protection," *Image and Vision Computing,* vol. 134, 2023.

[76] P. Nousi, S. Papadopoulos, A. Tefas and I. Pitas, "Deep autoencoders for attribute preserving face de-identification," *Signal Processing: Image Communication,* vol. 81, p. 115699, 2020.

[77] Z. N. B. S. T. M. A. A.-D. M. A.-D. Qiu Yuying, "A Novel Generative Model for Face Privacy Protection in Video Surveillance with Utility Maintenance," *Applied Sciences,* vol. 12, no. 14, 2022.

[78] K. He, X. Zhang, S. Ren and J. Sun, "Deep Residual Learning for Image Recognition," in *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Las Vegas, NV, USA, 2016.

[79] Q. Cao, L. Shen, W. Xie, O. M. Parkhi and A. Zisserman, "VGGFace2: A Dataset for Recognizing Face across Pose and Age," in *International Conference on Automatic Face and Gesture Recognition*, 2018.

[80] R. Gross, L. Sweeney, F. d. la Torre and S. Baker, "Model-Based Face De-Identification," in *2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06)*, York, NY, USA, 2006, June.

[81] B. Samarzija and S. Ribaric, "An approach to the de-identification of faces in different poses," in *37th Int. Convention on Inf. and Comm Tech., Electronics and Microelectronics (MIPRO)*, Opatija, Croatia, 2014.

[82] T. Xiao, J. Hong and J. Ma, "ELEGANT: Exchanging Latent Encodings with GAN for Transferring Multiple Face Attributes," in *Proc. European Conference on Computer Vision (ECCV)*, Muinch, Germany, 2018, September.

[83] Y. Jeong, J. Choi, S. Kim, Y. Ro, T.-H. Oh, D. Kim, H. Ha and S. Yoon, "FICGAN: facial identity controllable GAN for de-identification," 2021.

[84] B. Meden, Ž. Emeršič, V. Štruc and P. Peer, "k-Same-Net: k-Anonymity with generative deep neural networks for face deidentification," *Entropy,* vol. 20, no. 1, p. 60, 2018.

[85] Y.-L. Pan, M.-J. Haung, K.-T. Ding, J.-L. Wu and J.-S. Jang, "K-Same-Siamese-GAN: K-same algorithm with generative adversarial network for facial image De-identification with hyperparameter tuning and mixed precision training," *16th IEEE Int. Conf. AVSS*, Taipei, Taiwan, 2019, September.

[86] S. Guo, S. Feng, Y. Li, S. An and H. Dong, "Integrating diversity into neural-network-based face deidentification," in *37th Chinese Cont. Conf*, Wuhan, China, 2018, July.

[87] L. Meng and Z. Sun, "Face De-identification with perfect privacy protection," in *37th Int.l Convention on Inf. and Comm Tech, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia, 2014.

[88] D. Liang, Y. Meng, B. Erik and L. Haibin, "GARP-face: Balancing privacy protection and utility preservation in face de-identification," in *IEEE International Joint Conference on Biometrics*, Clearwater, FL, USA, 2014.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

[89] Y. Wong, S. Chen, S. Mau, C. Sanderson and B. C. Lovell, "Patch-based Probabilistic Image Quality Assessment for Face Selection and Improved Video-based Face Recognition," in *IEEE Biometrics Workshop, CVPR,* Colorado Springs, CO, USA, 2011, June.

[90] U. Garciarena, A. Mendiburu and R. Santana, "Analysis of the transferability and robustness of GANs evolved for Pareto set approximations," *Neural Networks,* vol. 132, pp. 281-296, 2020.

[91] L. Ziwei, L. Ping, W. Xiaogang and T. Xiaoou, "Deep Learning Face Attributes in the Wild," in *2015 IEEE International Conference on Computer Vision (ICCV)*, Santiago, Chile, 2015.

[92] K. Ricanek and T. Tesafaye, "MORPH: a longitudinal image database of normal adult age-progression," in *7th International Conference on Automatic Face and Gesture Recognition (FGR06)*, Southampton, UK, 2006.

[93] O. Langner, R. Dotsch, G. Bijlstra, D. H. J. Wigboldus, S. T. Hawk and A. v. Knippenberg, "Presentation and validation of the Radboud Faces Database," *Cognition and Emotion,* vol. 24, no. 8, pp. 1377-1388, 22 Nov 2010.

[94] S. Milborrow, J. Morkel and F. Nicolls, "The MUCT Landmarked Face Database," *Pattern Recognition Association of South Africa,* 2010.

[95] G. B. Huang, M. Mattar, T. Berg and E. Learned-Miller, "Labeled faces in the wild: A database forstudying face recognition in unconstrained environments," in *Workshop on faces in'Real-Life'Images: detection, alignment, and recognition*, Marseille, France, 2008.

[96] A. Martinez and R. Benavente, "The ar face database: Cvc technical report, 24," 1998.

[97] K. Messer, J. Matas, J. Kittler, K. Jonsson, J. Luettin and G. Maître, "Xm2vtsdb: The extended m2vts database," *Proc. of Audio- and Video-Based Person Authentication,* 04 2000.

[98] P. Lucey, J. F. Cohn, T. Kanade, J. Saragih, Z. Ambadar and I. Matthews, "The Extended Cohn-Kanade Dataset (CK+): A complete dataset for action unit and emotion-specified expression," *IEEE Comp. Soc. Conf. (CVPR) Workshops*, San Francisco, CA, USA, 2010.

[99] A. Georghiades, P. Belhumeur and D. Kriegman, "From few to many: illumination cone models for face recognition under variable lighting and pose," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 23, no. 6, pp. 643-660, June 2001.

[100] N. Zhang, M. Paluri, Y. Taigman, R. Fergus and L. D. Bourdev, "Beyond frontal faces: Improving Person Recognition using multiple cues," *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR),* pp. 4804-4813, 2015.

[101] S. Yang, P. Luo, C. C. Loy and X. Tang, "WIDER FACE: A Face Detection Benchmark," in *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Las Vegas, NV, USA, 2016.

[102] B. Yang, J. Yan, Z. Lei and S. Z. Li, "Fine-grained Evaluation on Face Detection in the Wild," in *1th IEEE International Conference on Automatic Face and Gesture Recognition Conference and Workshops*, 2015.

[103] W. Yang, P. Luo and L. Lin, "Clothing Co-parsing by Joint Image Segmentation and Labeling," in *2014 IEEE Conference on Computer Vision and Pattern Recognition*, Columbus, OH, USA, 2014.

[104] L. Yin, X. Wei, Y. Sun, J. Wang and M. Rosato, "A 3D facial expression database for facial behavior research," in *7th International Conference on Automatic Face and Gesture Recognition (FGR06)*, Southampton, 2006.

[105] Y. Wang, P.-M. Jodoin, F. Porikli, J. Konrad, Y. Benezeth and P. Ishwar, "CDnet 2014: An Expanded Change Detection Benchmark Dataset," in *IEEE Conf. on Comp. Vision and Pattern Recog.* Columbus, USA, 2014.

[106] T. Karras, S. Laine and T. Aila, "A Style-Based Generator Architecture for Generative Adversarial Networks," in *IEEE/CVF, CVPR*, Long Beach, CA, USA, 2019.

[107] N. Kumar, A. C. Berg, P. N. Belhumeur and S. K. Nayar, "Attribute and Simile Classifiers for Face Verification," in *International Conf. on Comp. Vision (ICCV)*, 2009.

[108] T. Karras, T. Aila, S. Laine and J. Lehtinen, "Progressive Growing of GANs for Improved Quality, Stability, and Variation," *arXiv preprint arXiv:1710.10196,* 2017.

[109] D. Yi, Z. Lei, S. Liao and S. Z. Li, "Learning Face Representation from Scratch," 2014.

[110] H.-W. Ng and S. Winkler, "A data-driven approach to cleaning large face datasets," in *2014 IEEE International Conference on Image Processing*, Paris, France, 2014.

[111] F. Samaria and A. Harter, "Parameterisation of a stochastic model for human face identification," in *Proc. 1994 IEEE Workshop on App. of Comp. Vis,* Sarasota, USA, 1994.

[112] Z. Zhifei, S. Yang and Q. Hairong, "Age Progression/Regression by Conditional Adversarial Autoencoder," in *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2017.

[113] A. Rössler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies and M. Niessner, "FaceForensics++: Learning to Detect Manipulated Facial Images," in *IEEE/CVF, ICCV*, Seoul, Korea (South), 2019.

[114] P. Korshunov and T. Ebrahimi, "PEViD: Privacy evaluation video dataset," in *Proceedings of SPIE - The International Society for Optical Engineering*, Switzerland, 2013, 08.

[115] V. Jain and E. Learned-Miller, "FDDB: A Benchmark for Face Detection in Unconstrained Settings," 2010.

[116] H. Moon, S. Rizvi and P. Rauss, "The FERET evaluation methodology for face-recognition algorithms," *IEEE Trans. on Pattern Analysis and Machine Intelligence.,* vol. 22, no. 10, pp. 1090-1104, 2000.

[117] R. Gross, I. Matthews, J. Cohn, T. Kanade and S. Baker, "Multi-PIE," in *8th IEEE Int. Conf. on Automatic Face & Gesture Recognition*, Amsterdam, Netherlands, 2008.

[118] B. Bhatnagar and e. al, "BEHAVE: Dataset and Method for Tracking Human Object Interactions," in *IEEE/CVF CVPR*, 2022.

[119] D. Gray, S. Brennan and H. Tao, "Evaluating Appearance Models for Recognition, Reacquisition, and Tracking," in *IEEE international workshop on performance evaluation for tracking and surveillance (PETS)*, 2007.

[120] A. L. Cambridge, "The database of faces," 1994.

[121] M. M. Nordstrøm, M. Larsen, J. Sierakowski and M. B. Stegmann, "The {IMM} Face Database - An Annotated Dataset of 240 Face Images," Richard Petersens Plads, Building 321, {DK-}2800 Kgs. Lyngby, 2004, May.

[122] H. Hukkelås, R. Mester and F. Lindseth, "DeepPrivacy: A Generative Adversarial Network for Face Anonymization," in *Advances in Visual Computing*, 2019.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

[123] N. Pavesic and S. Ribaric, "An overview of face de-identification in still images and videos," in *11th IEEE Int.Conf. on Auto FG*, Ljubljana, Slovenia, 2015.

[124] Y. Wen, B. Liu, J. Cao, R. Xie, L. Song and Z. Li, "IdentityMask: Deep Motion Flow Guided Reversible Face Video De-Identification," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 32, no. 12, pp. 8353-8367}, 2022.

[125] H. Touqeer, S. Zaman , R. Amin, M. Hussain, F. Al-Turjman and M. Bilal, "Smart home security: challenges, issues and solutions at different IoT layers," *The Journal of Supercomputing,* vol. 77, p. 14053–14089, 2021.

[126] M. Kumar, N. Singh, R. Kumar, S. Goel and K. Kumar, "Gait recognition based on vision systems: A systematic survey," *Journal of Visual Communication and Image Representation,* vol. 75, p. 103052, 2021.

[127] L. Topham, W. Khan, D. Al-Jumeily, A. Waraich and A. Hussain, "Gait identification using limb joint movement and deep machine learning," *IEEE Access,* vol. 10, pp. 100113-100127, 2022.

[128] A. Fitwi, Y. Chen, S. Zhu, E. Blasch and G. Chen, "Privacy-preserving surveillance as an edge service based on lightweight video protection schemes using face de-identification and window masking," *Electronics: Recent Advances in Computer Science & Engineering,* vol. 10, no. 3, pp. 1–36,, 2021.

[129] H. Proença , "The UU-Net: Reversible Face De-Identification for Visual Surveillance Video Footage," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 32, no. 2, pp. 496-509, 2022.

[130] L. Ren and Y. Peng, "Research of Fall Detection and Fall Prevention Technologies: A Systematic Review," *IEEE Access,* vol. 7, pp. 77702-77722, 2019.

[131] "World Health Organisation, "Falls," Fact Sheets," 2022. [Online]. Available: https://www.who.int/news-room/fact-sheets/detail/falls . [Accessed 20 Oct 2022].

[132] N. Thakur and C. Y. Han, "A Study of Fall Detection in Assisted Living: Identifying and Improving the Optimal Machine Learning Method," *Wireless Sensors Networks and Artificial Intelligence for Intelligent Health Monitoring,* vol. 10, no. 3, p. 39, 2021.

[133] M. Shopon, S. N. Tumpa, Y. Bhatia, K. N. P. Kumar and M. L. Gavrilova, "Biometric Systems De-Identification: Current Advancements and Future Directions," *Privacy,* vol. 1, no. 3, pp. 470-495, 2021.

[134] R. A. Bernert, A. M. Hilberg, R. Melia, J. P. Kim, N. H. Shah and F. Abnousi, "Artificial intelligence and suicide prevention: A systematic review of machine learning investigations," *Suicidal Behavior as a Complex Dynamical System,* vol. 17, no. 16, p. 1–25, 2020.

[135] W. Sheng and X. Li, "Multi-task learning for gait-based identity recognition and emotion recognition using attention enhanced temporal graph convolutional network," *Pattern Recognit,* vol. 114, 2021.

[136] A. Agarwal, P. Chattopadhyay and L. Wang, "Privacy preservation through facial de-identification with simultaneous emotion preservation," *Signal, Image Video Process,* vol. 15, no. 5, p. 951–958, 2020.

[137] M. Meißner, J. Pfeiffer, T. Pfeiffer and H. Oppewal, "Combining virtual reality and mobile eye tracking to provide a naturalistic experimental environment for shopper research," *Journal of Business Research,* vol. 100, p. 445–458, March 2017.

[138] N. Scott, C. Green and S. Fairley, "Investigation of the use of eye tracking to examine tourism advertising effectiveness," *Current Issues in Tourism,* vol. 19, no. 7, p. 634–642, 2016,.

[139] G. Letournel, A. Bugeau, V.-T. Ta and J.-P. Domenger, "Face de-identification with expressions preservation," in *2015 IEEE Int. Conf. Img. Proc*, QC, Canada, 2015.

[140] T. Sokhin, N. Butakov and D. Nasonov, "User Profiles Matching for Different Social Networks Based on Faces Identification," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*, 2019.

[141] B. C. Becker and E. G. Ortiz, "Evaluating open-universe face identification on the web," *IEEE Conf. Computer Vision and Pattern Recognition Workshops*, 2013.

[142] R. S. Bhowmick, I. Ganguli, J. Paul and J. Sil, "A Multimodal Deep Framework for Derogatory Social Media Post Identification of a Recognized Person," *ACM Trans. Asian Low-Resource Lang. Inf. Process,* vol. 21, 2022.

[143] H. Chi and Y. H. Hu, "Face de-identification using facial identity preserving features," in *2015 IEEE Global Conference on Signal and Information Processing*, 2016.

[144] T. Li and L. Lin, "AnonymousNet: Natural face de-identification with measurable privacy," *IEEE Comp. Soc. Conf. on CVPRW,* p. 56–65, 2019, June.

[145] A. Rice, P. J. Phillips, V. Natu, X. An and A. J. O'Toole, "Unaware Person Recognition From the Body When Face Identification Fails," *Psychol Sci,* vol. 24, no. 11, pp. 2235-2243, 1 Nov 2013.

[146] Methot, "Facial Recognition Market by Component (Software Tools (2D Recognition, 3D Recognition, and Facial Analytics) and Services), Application Area (Emotion Recognition, Access Control, and Law Enforcement), Vertical, and Region - Global Forecast to 2024," Market and Markets, 2019.

[147] J. H. B. D. Jr, "Cell Phones, Social Media, and the Capitol Insurrection," *The Judges' Journal,* vol. 60, no. 02, 2021.

[148] H. Kelly and R. Lerman, "America is awash in cameras, a double-edged sword for protesters and police," The Washington Post, 2020.

[149] E. Selinger and W. Hartzog, "The Inconsentability of Facial Surveillance," Boston University, 2019.

[150] R. A. Kendall, "Ethics and Facial Recognition Technology: An Integrative Review," in *3rd World Symposium on Artificial Intelligence (WSAI)*, 2021.

[151] F. Bacchini and L. Lorusso, "Race, again: how face recognition technology reinforces racial discrimination," *Journal of Inf. Comm. Ethics in Soc,* vol. 17, no. 3, 2019.

[152] K. B. F and et.al, "Face Recognition Performance: Role of Demographic Information," *IEEE Transactions on Information Forensics and Security,* vol. 7, no. 6, 2012.

[153] P. J. Phillips and et.al, "An other-race effect for face recognition algorithms," *ACM Trans. Appl. Percept,* vol. 8, no. 2, 2011.

[154] J. Sarabdeen, "Protection of the rights of the individual when using facial recognition technology," *Heliyon,* vol. 8, no. 3, 2022.

[155] P. Balthazar, P. Harri, A. Prater and N. M. Safdar, "Protecting Your Patients' Interests in the Era of Big Data,

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

Artificial Intelligence, and Predictive Analytics," *J Am Coll Radiol,* vol. 15, 2018.

[156] D. Boczar and et.al, "Using Facial Recognition Tools for Health Assessment," *Plast Surg Nurs,* vol. 41, no. 02, pp. 112-116, 2021.

[157] "Facial-recognition research needs an ethical reckoning," *NATURE,* vol. 587, 2020.

[158] M. Smith and S. Miller, "The ethical application of biometric facial recognition technology," *AI & Soc,* vol. 37, 2022.

[159] W. Chen and M. Wang, "Regulating the use of facial recognition technology across borders: A comparative case analysis of the European Union, the United States, and China," *Telecommunications Policy,* vol. 47, no. 02, 2023.

[160] L. Xue and Z. Pang, "Ethical governance of artificial intelligence: An integrated analytical framework," *Journal of Digital Economy,* vol. 1, no. 1, 2022.

[161] J. Bouguila and H. Khochtali, "Facial Plastic Surgery and Face Recognition Algorithms: interaction and challenges. A scoping review and future directions," *J Stomatol Oral Maxillofac Surg,* vol. 121, no. 06, 2020.

[162] N. Martinez-Martin, "What Are Important Ethical Implications of Using Facial Recognition Technology in Health Care?," *AMA Journal of Ethics,* 2019.

[163] H. Margetts and C. Dorobantu, "Rethink government with AI," *Nature,* 2019.

[164] A. Birhane, "The unseen Black faces of AI algorithms," *Nature,* vol. 610, 2022.

[165] D. Franco and et.al, "Toward Learning Trustworthily from Data Combining Privacy, Fairness, and Explainability: An Application to Face Recognition.," *Entropy (Basel),* vol. 23, no. 08, 2021.

[166] B. Thompson and R. V. Noorden., "The troubling rise of facial recognition technology.," *Nature,* 2020.

[167] D. Castelvecchi, "Is facial recognition too biased to be let loose?," *Nature,* vol. 587, no. 7834, pp. 347-349, 2020.

[168] D. Almeida, K. Shmarko and E. Lomas, "The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks," *AI Ethics,* vol. 2, no. 3, pp. 377-387, 2022.

[169] R. V. Noorden, "What scientists really think about the ethics of facial recognition research," *Nature,* 2020.

[170] L. K. Topham, W. Khan, D. Al-Jumeily, A. Waraich and A. J. Hussain, "Gait Identification Using Limb Joint Movement and Deep Machine Learning," *IEEE Access,* vol. 10, p. 100113–100127, 2022.

[171] P. Connor and A. Ross, "Biometric recognition by gait: A survey of modalities and features," *Computer Vision and Image Understanding,* vol. 167, 2018.

[172] J. T. Geiger, M. Kneißl, B. Schuller and G. Rigoll, "Acoustic Gait-based Person Identification using Hidden Markov Models," in *Proceedings of the 2014 Workshop on Mapping Personality Traits Challenge and Workshop*, 2014.

[173] L. Fuxiang and J. Qi, "Research on Recognition of Criminal Suspects Based on Foot Sounds," in *ITNEC Conference* , 2019.

[174] H. Government, "National AI Strategy," Office for Artificial Intelligence, UK, 2021.

[175] L. Topham, W. Khan, D. Al-Jumeily and A. Hussain, "Human body pose estimation for gait identification: A comprehensive survey of datasets and models," *ACM Computing Surveys,* vol. 55, no. 6, pp. 1-42, 2022.

[176] L. K. Topham, W. Khan, D. Al-Jumeily, A. Waraich and A. J. Hussain, "A diverse and multi-modal gait dataset of indoor and outdoor walks acquired using multiple cameras and sensors," *NATURE Sci. Data,* vol. 10, no. 320, 2023.

[177] S. Ravi, P. Climent-Pérez and F. Florez-Revuelta, "A Review on Visual Privacy Preservation Techniques for Active and Assisted Living," *Multimedia Tools and Applications,* pp. 1-41, 07 2023.

[178] M. R. Hasan, R. Guest and F. Deravi, "Presentation-Level Privacy Protection Techniques for Automated Face Recognition - A Survey," *ACM Computing Surveys,* vol. 55, 02 2023.

[179] H. Wang, Y. Wang, Z. Zhou, X. Ji, D. Gong, J. Zhou, Z. Li and W. Liu, "CosFace: Large Margin Cosine Loss for Deep Face Recognition," in *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, Salt Lake City, UT, USA, 2018.

[180] J. Deng, J. Guo, N. Xue and S. Zafeiriou, "ArcFace: Additive Angular Margin Loss for Deep Face Recognition," in *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Long Beach, CA, USA, 2019.

[181] R. Rothe, R. Timofte and L. V. Gool, "Deep expectation of real and apparent age from a single image without facial landmarks," *International Journal of Computer Vision,* vol. 126, pp. 144--157, 2018.

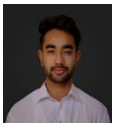
[182] N. V. P. K. B. H. H. K. C. Yifang Li, "Effectiveness and Users' Experience of Obfuscation as a Privacy-Enhancing Technology for Sharing Photos," in *Proceedings of the ACM on Human-Computer Interaction*, NA, 2017.



Wasiq Khan (Senior Member, IEEE) received a Ph.D. in speech analysis and intelligent reasoning from the University of Bradford, U.K. Currently, he is a Senior Academic in AI with the Department of Computer Science, Liverpool John Moores University, U.K. He is also a Visiting Professor of AI with the University of Anbar, Iraq. He has been publishing the research outcomes in high-impact journals and is editorial board member for prestigious Journals and international conferences.



Luke K. Topham received a B.Sc. degree in computer science from the University of Chester in 2014, an M.Sc. degree in computer science from LJMU in 2015, an M.Phil. degree in engineering from the University of Liverpool in 2020, and a Ph.D from LJMU in 2024. His current research interests include gait identification using computer vision and machine learning.



Umar Khayam is an MSc graduate in Applied AI with Deakin University, Australia. He has also been working as RA at DevNation, Pakistan. His research interests include machine/deep learning, pattern matching, and face analysis.



Dr. Sandra Ortega-Martorell received a Ph.D. in Computer Science from the Autonomous University of Barcelona, Spain. She is currently a Reader (Associate Professor) in Data Science at Liverpool John Moores University. Her expertise is in the development of AI/ML solutions, with an increasing emphasis on translation to healthcare. She is the Principal Investigator of a €10M EU project (TARGET, GA n. 101136244) for the development of digital twin technology for the

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2024.3485990

early diagnosis and personalised management and rehabilitation of patients suffering from stroke related to atrial fibrillation.



Dr. Heather Panter is a retired American police detective with 13+ years of law enforcement experience with local and federal police agencies. In 2016, she earned her PhD in Criminology from Cardiff University (UK). As a senior lecturer, she is the programme leader of LJMU's MSc Policing and Criminal Investigations.



Prof. Darren Ansell, received the B.Sc. degree in electrical and electronic engineering from the Institute of Science and Technology, The University of Manchester, and the Ph.D. degree in antenna optimization using evolutionary algorithms from Cranfield University. He is an Engineering Lead for Space and Aerospace and a Professor in aerospace engineering. Previously, he worked in industry at BAE Systems in management roles, specializing in mission systems and autonomy.



Prof. Dhiya. Al-Jumeily OBE is a professor of Artificial Intelligence and the president of eSystems Engineering Society. He has extensive research interests covering a wide variety of interdisciplinary perspectives concerning the theory and practice of Applied Artificial Intelligence in medicine, human biology, environment, intelligent community and healthcare. He has published well over 300 peer reviewed scientific international publications, 17 books and 17 book chapters, in multidisciplinary research areas.



Abir J. Hussain (Senior Member, IEEE) received a Ph.D. degree from The University of Manchester, U.K. She is currently a professor in machine learning with the University of Sharjah, UAE. She is one of the initiators and chairs of the Development in e-Systems Engineering (DeSE) series, most notably illustrated by the IEEE technically sponsored DeSE International Conference SeriesAbir Hussain is a professor of AI working within the College of Engineering at University of Sharjah, UAE. She also holds IEEE Senior Membership (email: abir.Hussain@sharjah.ac.ae).

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/