Discover Artificial Intelligence

Review

Exploring deep convolutional generative adversarial networks (DCGAN) in biometric systems: a survey study

John Jenkins[1] · **Kaushik Roy**[1]

Received: 20 November 2023 / Accepted: 13 May 2024
Published online: 28 May 2024

Abstract
Over the past few years, there has been a proliferation of research in the area of generative adversarial networks (GANs). GANs present a novel approach to producing synthetic data in varying fields including medicine, traffic control, text transferring, image generation, and cybersecurity. To improve the quality of synthetic generation, specifically for images, the GAN technique was paired with convolutional neural networks (CNNs) to build deep convolutional generative adversarial networks (DCGAN). The DCGAN framework is a simple yet stable framework shown to generate quality photorealistic images. There are a number of studies reviewing GANs, providing a comparative analysis of performance, stabilization, and training methods. With respects to the DCGAN architecture, there are literature reviews reporting its usage in forensic sketch to face transformation and fuzzy face recognition. Here, we provide a review detailing the use of the DCGAN framework with biometrics samples for advancements in biometric authentication systems and cybersecurity. As GANs have shown to be a primary tool in generating deepfakes, we explore the use of DCGANs to generating synthetic biometrics that can deceive security systems and serve as quality training data for other machine learning models. The goal of this review is to contribute a concise consolidated review of techniques involving the DCGAN framework and biometric samples for the improvement of biometric recognition systems and to be used as a reference point for future work in cybersecurity.

Keywords Deep learning · DCGAN · Biometrics · Cybersecurity · Neural networks · Survey

1 Introduction

The use of biometric authentication systems is replacing traditional knowledge-based and token-based systems. With proliferation of inexpensive cameras and scanners, along with improved recognition algorithms and protocols, the distinctiveness of biometrics ensures the efficacy of authentication systems. Although the use of biometrics is making systems more efficient, there are still security vulnerabilities that can be exploited. Biometric spoofing attacks are the act of presenting an illegal sample of similar characteristics to gain unauthorized access to a system. The higher quality and alike the illegal sample, the more likely the sample would successfully bypassed recognition algorithms and protocols and gain unauthorized access.

Most recently deepfakes have been the popular source of quality spoofing attacks. Deepfakes are synthetic media, image or video, where the likeness of someone is mimicked. While the exploitation of forgeries is not novel, deepfakes leverages dynamic techniques from machine learning and artificial intelligence to manipulate and/or generate audio,

✉ Kaushik Roy, kroy@ncat.edu; John Jenkins, jmjenki1@aggies.ncat.edu | [1]Computer Science, North Carolina A&T State University, East Market Street, Greensboro, NC 27411, USA.

images, and videos with a greater ability to deceive. There are a number of notable tools used to create deepfakes, such as faceswapping [1] and autoencoders [2]. Faceswap is a software tool used to blend two images using artificial intelligence. As the face of one image is swapped and fused with the head and body of another, the software aims to blend the face displacement and complexion of the combined image to look natural and genuine [1]. An autoencoder is a specified artificial neural network used to discover efficient representation (feature learning) for a set of data. The autoencoder functions in two parts, an encoding function that transforms the data and a decoding function that attempts to recreate the data from its encoded representation [2]. Deepfakes utilize autoencoders by encoding a person's representation in to a latent space. The encoded latent representation contains significant features detailing facial features and body posture. The latent representation is then decoded using a model trained especially for the target. Those decoded features are overlaid on the core features of the original data. Generative Adversarial Networks (GANs) are also a primary tool and used as a basis in multiple techniques for creating deepfakes. GANs are comprised of two competing neural networks, trained in a zero-sum game, to produce synthetic data from noise [3]. GANs are the deepfake tool under review in this work, for its uses with biometric systems.

Over the past few years, GANs have been used in to advance research a number of experiments in varying fields.

Previous studies on GANs present a comparative analysis on variant-architectures and their performance [4, 5]. The early versions of GANs used supervised learning methods and multilayer perceptrons for the network architecture. The later versions use unsupervised learning techniques and are more robust, increasing in the number application capabilities. There are surveys exploring in-depth challenges with GANs, as well. GANs have shown to unstable in training due to issues with convergence, vanishing or exploding gradients, and mode collapse [6, 7]. In these work, stabilize techniques along with variant-architectures are addressed as steps towards improvements. There are also surveys detailing GANs vast usage in theory and applications [8]. In computer vision, GANs have shown its value in a number of fields including medicine, traffic control, text transferring, image generation and detection, and cybersecurity [9, 10]. In these in-depth studies, many revised GAN architectures are embraced through supervised, unsupervised, and reinforcement learning to solve worldly challenges.

As there are a multitude of variant-architectures, this paper reviews the use of the Deep Convolutional Generative Adversarial Network (DCGAN) architecture [11] with biometrics samples for advancements in biometric authentication systems and cybersecurity; generating synthetic data that can deceive security systems and function as quality training data for other machine learning models. The DCGAN architecture has known applications in generating image datasets, image-to-image and text-to-image translation, face aging, video prediction, and 3D object generation. With respects to the DCGAN architecture, there are reviews detailing its usage in forensic sketch to face transformation (STF) and fuzzy face recognition (FFR) [12, 13]. Based on the STF survey, different facial recognition methods using the DCGAN architecture are used to generate synthetic photo realistic images from drawn forensic sketches [12]. In the FFR review, multiple facial recognition methods using the DCGAN are presented. Each method's implementation and performance are evaluated and compared to other popular models such as VGG-19, RESNET-50, RESNET-18, and faster R-CNN [13].

In this review, we strive to provide a review of the DCGAN architecture usage in biometric recognition systems and cybersecurity. Due to the recent proliferation of deepfakes, synthetic media has shown to become a basis for spoofing attacks. Moreover, the DCGAN framework is known to be one of the primary GAN architectures for quality synthetic image generation. The DCGAN framework's simplistic implementation and ease of access has made it foundational to generating photorealistic images and the focus of this work. With biometric recognition systems becoming a stable in access controls, quality synthetic biometric generation is a major concern to cybersecurity. We intend to contribute a concise consolidated review of techniques involving the DCGAN framework and biometric samples for the improvement of biometric recognition systems. The goal of this review is to become a landmark for the DCGAN framework with biometrics, and to be used as a reference point for future work in cybersecurity. Research papers that focus on improving biometric recognition models were chosen in this review to illuminate the power of the DCGAN framework in adversarial training. The contribution of this literature survey can be summarized in the following:

- Describing the DCGAN architecture: we provide a detailed analysis of the DCGAN architecture, both the generator model and the discriminator model. We express the mathematical operation employed by the model. We also address the challenges in training the GAN model for successful image generation and the steps towards stabilizing the model.
- Techniques used to Generate Biometrics: we provide a consolidation of techniques, over the years, for the use of the DCGAN framework in generating synthetic biometrics. In these work, the DCGAN framework and its variants are

detailed along with the quality of the generated biometrics. We also address the metrics used to evaluate the quality of the generated biometrics.

- Techniques to Improve Biometric Systems: we provide a consolidation of techniques, over the years, for the use of the DCGAN framework to improve biometric recognition models. In these works, the DCGAN framework and its variants are detailed in steps to test and improve recognition models. In some cases, the frameworks are used a data augmentation technique to increase samples for training. In other cases, the DCGAN framework and its variants are used as adversarial training, as a spoofing attack to improve training for existing or developing newer models.

Biometrics such as face, iris, palmprints, and fingerprints provide a unique characteristic to identifying individuals and are a pillar in securing data in modern systems. Figure 1 below shows the typical use of biometrics in modern biometric systems. In a typical biometric system, samples are captured by a camera or sensor for evaluation to grant or deny access to the secure system. The captured samples are used as input to a recognition model for analysis. In that recognition model, some algorithmic feature extraction is used to compare the captured data among a database of previous captured and authenticated data. If a successful match is found, the user is accepted and granted access to the secure system. If a match is unsuccessful, the user is rejected and denied access to the secure system.

In the following section, Sect. 2, we present a detailed background of the Generative Adversarial Networks (GANs) structure and the improved Deep Convolutional Generative Adversarial Network (DCGAN) framework. In Sect. 3, we present a compilation of referenced work using the DCGAN framework with biometrics. In Sect. 4, we provide a discussion of the reference work summarized in Sect. 3 and its impact. In Sect. 5, we concisely present our conclusions on the DCGAN framework use in biometric systems.

2 Background

As the popularity of deepfakes have grown on the years, Generative Adversarial Networks (GANs) and its variants are a primary tool used in produces photorealistic synthetic images. Since its inception in 2014, the proposed concept of GANs, by Goodfellow et al. [3], has quickly become a research hotbed.

2.1 GAN structure

The fundamental idea of GANs is a competitive minimax game between the generator model, G, and the discriminator model, D. As seen in Fig. 2, the two networks are to be trained in tandem until a Nash equilibrium is reach for the objective of generating quality synthetic data; the data generated by G is significantly alike to the training data that D cannot differentiate the synthetic data from the genuine data.

The generator model, G, is passed a uniform random noise distribution (z), and manipulates it during training, G(z), to mirror the target distribution. The generator model is trained to maximize the projected log-probability with which the discriminator model distinguishes G(z) as a real sample. The discriminator model, D, is passed an array of unlabeled samples from G(z) and the real data distribution, p_r. The discriminator is trained to distinguish between the generated, synthetic samples, and real samples [3–7]. This match between G and D forms a minimax game where the loss function is mutually maximized by the discriminator and minimized by the generator, as seen in Eq. 1 below.

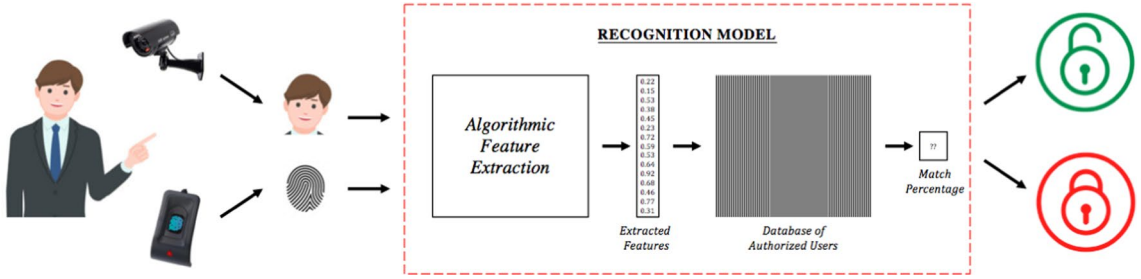

Fig. 1 Illustration of a typical biometric system securing data

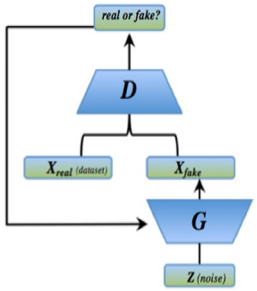

Fig. 2 Visual of the two competing neural networks, the generator model G and the discriminator model D, in the Generative Adversarial Networks (GAN) technique

$$L(D, G) = \min_G \max_D Ex \sim pr\left[\log(D(x))\right] + Ez \sim pz\left[\log(1 - D(G(z)))\right] \quad (1)$$

2.2 DCGAN architecture

To improve the quality of synthetic generation, specifically for images, the GAN technique was paired with Convolutional Neural Networks (CNNs). CNNs are know for is successes in computer vision techniques involving images recognition. This combination led to the proposing of the Deep Convolutional Generative Adversarial Network (DCGAN) technique [11]. The DCGAN technique utilizes a sequence of convolutional operations incorporating spatial up-sampling operations to improve generation. The DCGANs architecture was pioneered to diminish the mode collapse dilemma in GANs. Mode collapse arises when the generator develops bias towards a few outputs and fails to produce unique outputs of each variation from the dataset. The DCGAN architecture is proven to be stable in training for image generation and is a foundational pillar for other GAN architectures. The architectural guidelines for stable training replaces the pooling layers, in an archetypal CNN, with strided convolutions and fractionally-strided convolutions in the discriminator and generator models respectively [11]. Strided convolutions are a deep learning technique that reduces the size of your data. Fractionally–strided convolutions are a deep learning technique that increases the size of the data.

2.2.1 Generator

The first layer of the DCGAN is passed a 100 dimensional uniform noise distribution. The DCGAN architecture starts with a sequence of four fractionally-strided convolutions in the generator to upsample the 100 dimensional input, generating feature maps with increasing spatial dimensions and decreasing depth. Each convolution doubles in size while reducing the number of output channels. After the first convolution operation, the number of output channels is reshaped from 1024 to 512. All of the following convolutional layers have a stride of 2. Batch normalization is used to normalize the activations in each layer, helping to stabilize the training process. Batch normalization also addresses problems with poor initialization and issues in gradient flow. A rectified linear unit (ReLU) activation function is applied in each layer of the generator, except for the last layer. The final layer utilizes a hyperbolic tangent (tanh) activation function to normalize the pixel values, between -1 and 1, and generate the final synthetic image. The final output of the generator has dimensions of 64×64 with 3 output channels (RGB) (Fig. 3).

2.2.2 Discriminator

The discriminator takes in the generators output as input and is followed by four strided convolutions. The discriminator layers processes the synthetic image and downsample it to create feature maps with reduced spatial dimensions and increased depth. Batch normalization is used to normalize the activations in each layer, except the input layer. After batch normalization, a leaky rectified linear unit (Leaky ReLU) activation function is used in all convolutional layers. A Leaky ReLU is a nonlinear function that assigns a non-zero output value for a negative input, with the goal of resolving the "dying ReLU" problem and helping the gradients flow easier throughout the architecture. The use of a Leaky ReLU helps to avoid discarding potentially important information**,** and thus performs better than ReLU in scenarios where the data has a lot of noise or outliers. The output layer of the discriminator is a single neuron with a sigmoid activation function. The output value of the function produces a probability score, between 0 and 1, that signifies if the input image is genuine or not (Fig. 4).

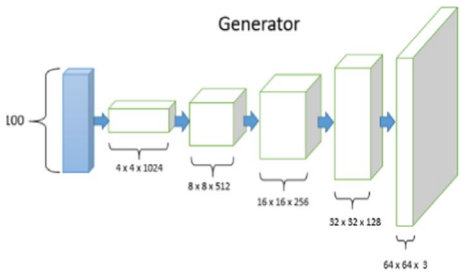

Fig. 3 Illustration of DCGAN's Generator model of four fractionally-strided convolutions. The first layer of the model is passed a 100 dimensional uniform noise distribution and the final layer of the model outputs a synthetic image of 64 × 64 pixels.

2.2.3 Training & stability

The generator receives the feedback from the discriminator as both models are trained together in an adversarial manner. The goal is for the generator model to produce images that are ultimately indistinguishable from the genuine training images. The loss function employed by both models is the binary cross-entropy with the Adaptive Moment Estimation (Adam) optimizer to assist in minimizing the loss. Binary cross-entropy is a frequently used loss function in machine learning and deep learning to measure the differences between predicted binary outcomes and their actual labels. Binary cross-entropy is the negative average of the log of the correctly predicted probabilities. The Adam optimizer is a combination of Root Mean Square Propagation (RMSprop) and Stochastic Gradient Descent (SGD) with momentum. Adam is an optimization algorithm that uses a square gradient to scale the learning rate, adapting to the different parameters based on momentum [6, 7]. The generator uses the feedback from the loss function to continue generating newer images, refining its process, until the discriminator cannot accurately discern the generated images from the genuine training images.

The DCGAN's architecture is simplistic but effective, as it enables the generation of photorealistic images by the use of convolutional layers and adversarial training. The quality synthetic images generated by the DCGAN architecture can be valuable for data augmentation and/or training machine learning models in conditions where that is a shortage of real data. The DCGAN technique gained popularity from its much success with the Large-scale Scene Understanding (LSUN) datasets; generating synthetic images of random background scenes [11]. Evolving its use to the generation of random facial images, the research questions proposed in this work is focuses on the use of the DCGAN technique with biometrics samples.

3 Literature survey

There are a multitude of approaches to using the DCGAN framework with biometric images. Some research papers used the DCGAN framework solely for generating spoofing data or as a spoof detection model. A few used the DCGAN framework in combination with other recognition models as a data augmentation tool. The data generated has been used to expand data mass or as adversarial training to improve recognition models. In this survey we separate those approaches into two categories: (1) Generating Quality Biometrics and (2) Improving Biometric Systems.

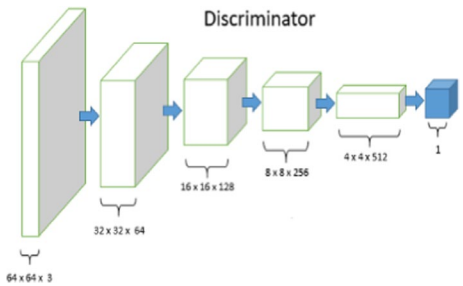

Fig. 4 Illustration of DCGAN's Discriminator model of four strided convolutions. The first layer of the model takes the synthetic image as the input and the final layer outputs a single neuron as the probability score of the input image being genuine.

3.1 Generating quality biometrics

The first category, Generating Quality Biometrics, involves using the DCGAN framework and its variants to generate photorealistic synthetic biometric samples. In the referenced work, real biometric samples are used as input into the DCGAN framework with the intent to produce quality fake biometrics. To evaluate the quality of the fabricated biometrics, a number of metrics are use. The most common metrics for comparing images quality include the Structure Similarity Index Metric (SSIM) and Fréchet Inception Distance (FID). SSIM is a perceptual metric that quantifies image quality degradation. SSIM is a weighted combination of structural differences, luminance masking, and contrast masking. The calculated SSIM index results in a decimal value between − 1 and 1. The value of 1.00 indicates perfect similarity, where 0 indicates no similarity, and − 1.00 indicates a perfect anti-correlation. FID is a metric that quantifies the realism and diversity of images generated by GANs. FID compares the distribution of the generated synthetic images with the distribution of the genuine ones. Since 2020, FID has become one of the standard metric for evaluating the quality of generative models and its data. Below we review those referenced work that used the DCGAN framework for the generation of quality synthetic biometric samples, as seen below in Fig. 5. From a 100 dimenional noise distribution, the generator creates a synthetic image. The discriminator compares the generated image to a real image and feeds that information back to the generator. The generator works to continues to produce a evolved image until the discriminator cannot discern the synthetic image from the genuine image. The referenced work from this section is also shown and summarized in Table 1.

In Choi et al. [14], a verification method is proposed to evaluate the quality of fake fingerprints generated by DCGAN. The synthetic generated fingerprints are compared to non-generated fake fingerprints through four similarity measures. The first metric presents the distributions of the mean and standard deviation of the generated synthetic fingerprints are compared to that of the non-generated fake fingerprints. In the second metric, the Pearson correlation of the histograms is calculated between histograms of the generated synthetic fingerprints and the non-generated fake fingerprints. The third metric calculated is the mean Hamming distance (MHD). MHD, a metric of assessing the similarity of images, is used to compare the generated synthetic fingerprints and non-generated fake fingerprints. The fourth metric, intersection of union (IOU), is used to assess the shape similarity of the generated synthetic fingerprints and non-generated fake fingerprints. From the immense experiments, in terms of the four similarity measures, it was concluded that the DCGAN generated synthetic fingerprints could be used to enhance the fake fingerprint data [14].

Liu et al. [15] proposed applying the DCGAN framework to face data. Using a Tensorflow implementation, the DCGAN framework is applied the CelebA dataset for fake face image generation. The discriminator for the generated data predicted a loss distribution ranging mainly from 0.35 to 0.50, with the genuine data predominantly around 0.5. In relation to the inclusive loss values and the predictive distribution analysis of the discriminator, it was resolute that the DCGAN model was creditable for virtual human face modeling. The data produced from training the DCGAN model produced synthetic faces similar to the genuine faces and can be used to build a synthetic face model database, resolving the issues

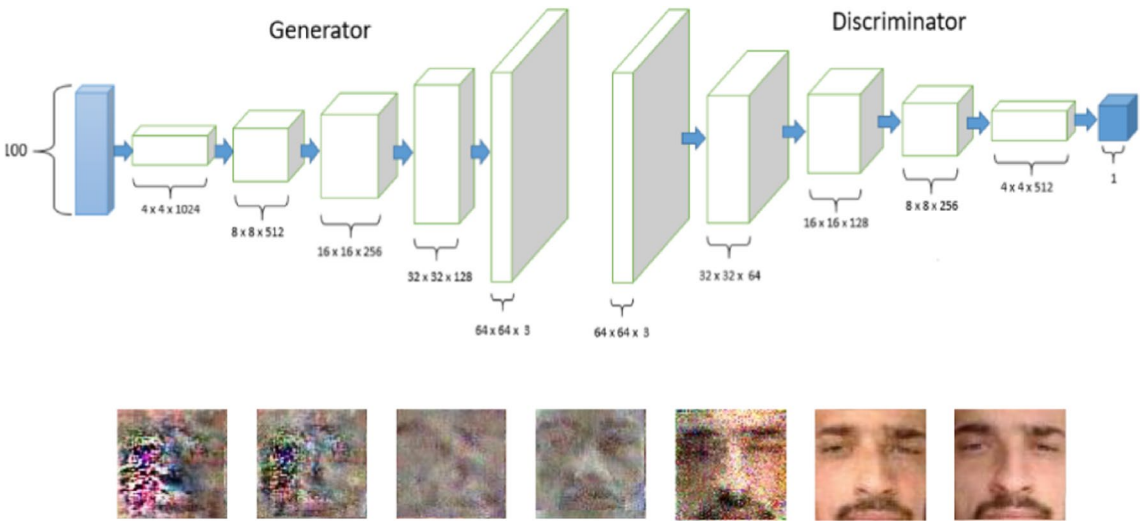

Fig. 5 Illustration of DCGAN framework and the evolving output of synthetic face images

Table 1 Summary of the uses of the DCGAN framework for generating quality biometrics

References	Model description	Biometric modalities	Datasets	Performance
2019				
Choi et al. [14]	Use of Hamming distance, Person correlation of histogram, and intersection of union verification methods to determine data generated by DCGAN are similar to real data	Fingerprint	–	From immense experimentation, in terms of the four similarity measures, it was concluded that the generated synthetic data could be used to enhance the fake fingerprint data
Liu et al. [15]	DCGAN	Face	CelebA	The synthetic faces generated are of quality to be used to build a synthetic face model database, resolving the issues of insufficient data sources when training traditional machine learning
2020				
Xiangli et al. [16]	RealnessGAN (based on DCGAN)	Face	CelebA and FFHQ	The proposed model achieved high FID and SWD scores, demonstrating its ability of efficiently capturing the underlying data distribution on both the synthetic and genuine datasets
2021				
Shariff et al. [17]	DCGAN	Face	CelebA	The SSIM results verified the generated synthetic facial images could be used to enhance the training of other models for a variety of supervised learning tasks
Liu et al. [18]	DCGAN generation for low computing resources	Face	CelebA	Results showed that training reached equilibrium between the generation effect and the time cost after four epochs
Barni et al. [19]	DCGAN	Iris	CASIA-IrisV4 and IITD-IrisV1	Results verified that the proposed iris deidentification method maintains the original features of the iris and generates images that are identifiable by both humans and modern biometric recognition methods functioning solely on iris patterns
Vincent et al. [20]	DCGAN	Fingerprint	Anguli synthetic fingerprint generator	Experimental results showed that the DCGAN generated synthetic fingerprint had better resolution in terms of ridge structure, ridge endings and bifurcations. The performance of the proposed network for fingerprint generation was substantiated with respect to the SSIM and FID scores

Table 1 (continued)

References	Model description	Biometric modalities	Datasets	Performance
2022				
Bamoriya et al. [21]	Deep leaning based synthetic biometric GAN (DSB-GAN): based on a convolutional autoencoder (CAE) and DCGAN	Fingerprint, iris, and palmprint	PolyU fingerprint, PolyU palmprint, IITD iris, and IITD palmprint	According to the FID and MS-SSIM metrics, the generated synthetic images produced by the proposed framework are diverse with high variations. Results verified high similarity in the generated images and low variation between the genuine input images and the reconstructed biometric images
2023				
Canan et al. [22]	DCGAN	Face	CelebA	The results indicated that the quality of generated synthetic face images was accurately proportional to increases in training data and training epochs
Kumar et al. [23]	DCGAN	Face	CelebA	After ten successive iteration, the Inception Score (IS) and FID values both indicated the generate image are of high quality and standards
Kapalavai et al. [24]	DCGAN to generate images and ESRGAN to enhance the quality of generated images	Face	CelebA	The SSIM scores obtained from the generated images verified the proposed model's proficiency in generating facial images

of insufficient data sources when training traditional machine learning [15]. These results advocate the use of synthetic face images in the future, in the field of semi-supervised learning.

In 2020, Xiangli et al. [16] proposed a framework called RealnessGAN, as an extension of the DCGAN architecture. In the RealnessGAN framework, the scalar output of the discriminator is substituted with a discrete realness distribution. As the discriminator approximates realness from numerous angles, more instructive guidance is provided to the generator for more realistic image generation. Experiments were conducted over real world datasets including CelebA and FFHA face datasets. Compared to the baseline models, on both datasets, the RealnessGAN obtained higher scores in using the Fréchet Inception Distance (FID) and Sliced Wasserstein Distance (SWD) metrics. With a smoother and steadier learning process, results proved the RealnessGAN framework demonstrated the ability of efficiently capturing the underlying data distribution on both the synthetic and genuine datasets.

In 2021, Shariff et al. [17] proposed implementing the DCGAN framework to train and generate human faces at scale. The CelebA dataset was used to generate synthetic faces comparable to that of genuine celebrities to illustrate its effectiveness in rendering naturalistic images. SSIM was used to provide a quantitative assessment of the trained DCGAN model. SSIM is utilized to calculate the similitude between the real and generated artificial images by transforming varying extracted features from the images. Experiments showed the DCGAN generated synthetic face images had a maximum SSIM score of 0.34 compared to the genuine images from the CelebA dataset [17]. The results verified the DCGAN generated synthetic facial images could be used to enhance the training of other models for a variety of supervised learning tasks.

Liu et al. [18] also explored face generation using the DCGAN framework. Using the CelebA dataset, experiments were conducted from the standpoint of limited or inadequate computing resources. The goal of this work was to find an optimal training round that balances the generation effect with the time cost. The number of training epochs along with the algorithm's parameters was fine-tuned to attain equilibrium between the quality of images generated and computing resources used. During the experiments using the CelebA dataset, the quantitative parameters were recorded after each of the eight rounds of training. Results showed that for the CelebA dataset, training reached equilibrium between the generation effect and the time cost after four epochs. Although increasing the number of training epochs have some positive effects towards enhancing the generative model and its output, at the fourth epoch, the generator and the discriminator models mutually demonstrated convergence to the distribution of the CelebA dataset. Regarding the trade-off between the time cost and the training effect of the DCGAN model, after four epochs on the training set, the effect of increasing the number of training epochs becomes less significant [18].

Barni et al. [19] proposed an iris deidentification method based on the DCGAN framework. The proposed method generates novel photorealistic synthetic images, wherein all distinguishing biometric features of the iris textures are automatically removed and replaced. The aim of the proposed method is to generate a synthetic texture comparable to those attained by normalizing a genuine iris region using the rubber sheet model (RSM) algorithm but stripped of any biometric data associated with the original iris. For experiments, portions of public iris databases CASIA-IrisV4 and the Indian Institute of Technology Delhi (IITD)-IrisV1 was used. The DCGAN framework is trained utilizing these datasets of iris RSMs to generate synthetic iris textures and compared against a fractal algorithm. The deidentification capabilities of the proposed method were analyzed with results showing that the existing iris recognition algorithms were unable to extract distinguishing features from the generated synthetic samples. Results also showed that the proposed deidentification method assures robustness against reidentification attacks [19]. The attained results verified that the proposed iris deidentification method maintains the original features of the iris and generates images that are identifiable by both humans and modern biometric recognition methods functioning solely on iris patterns.

Vincent et al. [20] implements a modified DCGAN framework for synthetic fingerprint image generation. The loss function in the proposed DCGAN framework derives an efficient loss computation, which reflects upon both Binary Cross-Entropy (BCE) loss and Hinge Embedding loss. The Anguli synthetic fingerprint generator dataset is used for training the DCGAN framework. The graphical quality of generated fingerprints is analyzed using the SSIM and FID scores. The SSIM values obtained were in the range of 0.86 to 0.90 and a FID of 150.3 [20]. Compared against a DCGAN model trained on BCE loss alone, the proposed architecture had a better convergence in respect to the generator and discriminator loss. Experimental results showed that the DCGAN generated synthetic fingerprint had better resolution in terms of ridge structure, ridge endings and bifurcations. The performance of the proposed network for fingerprint generation was substantiated with respect to the SSIM and FID scores.

Bamoriya et al. [21] proposed a deep learning based synthetic biometric GAN (DSB-GAN) based on the DCGAN framework and a convolutional autoencoder (CAE). The DSB-GAN framework has a lower number of trainable parameters, compared to other modern methods, making it effective for real-time use. The generated synthetic samples from the

generator model and the augmented data samples from the CAE are merged and rearranged to generate a large dataset. These data samples are used as input to the discriminator model of the proposed DSB-GAN, which attempts to discern between the genuine and synthetic samples. The generative model architecture enables the proposed framework to encapsulate the complex textures of input data, resulting in better model training. The generated synthetic images produced from this proposed method were determined to be diverse and complete [21]. The proposed DSB-GAN framework is assessed on three biometric modalities: fingerprint, iris, and palmprint. Experiments included the PolyU fingerprint, PolyU palmprint, IITD iris, and IITD palmprint datasets. The performance of the DSB-GAN was evaluated on two parameters, FID and multi-scale SSIM (MS-SSIM). The DSB-GAN's performance was compared against various other GANs, with the proposed framework having minimal reconstruction error and a high SSIM score [21]. Compared to DSB-GAN, all other methods have a higher FID and MS-SSIM value. According to the FID and MS-SSIM metrics, the generated synthetic images produced by the DSB-GAN framework are diverse with high variations. Results verified high similarity in the generated images and low variation between the genuine input images and the reconstructed biometric images.

In 2023, Canan et al. [22] produced an examination of synthetic face images generated by the DCGAN framework. Experiments were conducted on the CelebA dataset with varying dataset sizes and training epochs. The results indicated that the quality of generated synthetic face images was accurately proportional to increases in training data and training epochs.

In Kumar et al. [23], researchers take a deep dive into deepfake creation and detection in social media. Comparing existing techniques, the DCGAN framework was chosen for implementation using the CelebA dataset. Images were trained for ten successive iterations and its performance was evaluated. It was observed that the discriminator's and the generator's loss value varied over time as the DCGAN framework accuracy increased during each iteration. The metrics used for evaluation were the Inception Score (IS) and FID. In these experiments, the IS obtained values of 1.074 and the FID of 49.3. The achieved values indicated that the images generated from the DCGAN framework are of high quality and standards.

In Kapalavai et al. [24], high-resolution face image generation is proposed by combining the DCGAN framework with Enhanced Super-Resolution GANs (ESRGAN). ESRGAN, an extension of the Super-Resolution GAN, is a deep learning framework designed to enhance the quality of low-resolution images. In the ESRGAN framework, the perceptual loss function evaluates the high-level properties of the generated image compared to that of the target image. During this process, the model is enabled to produce synthetic images that are sharper and more photorealistic. In this work, the DCGAN framework is used to generate human faces from random noise, using the CelebA dataset, as the ESRGAN framework is used to enhance the quality of the synthetic images. SSIM is used to quantitatively evaluate the quality of the generated synthetic images. The SSIM scores obtained from the generated images, an average of 0.31, verified the proposed model's proficiency in generating facial images [24].

3.2 Improving biometric systems

The second category, Improving Biometric Systems, often involves using the DCGAN framework and its variants in combination with a recognition model. In the referenced work, the DCGAN framework is use to generate quality synthetic biometric samples. Those fabricated biometrics are then used to with notable recognition models in a multitude of ways to improve biometric systems including data augmentation, presentation attacks, and false acceptance attacks. As data augmentation, the artificial biometrics are used to expand the dataset of real data during training to improve the recognition model's performance and generalizability. For spoofing (presentation attacks and false acceptance attacks), the quality of the recognition models is evaluated by comparing the real and fake datasets for access into the biometric system. The most common metrics for biometric systems include true acceptance rate (TAR), false acceptance rate (FAR), and false rejection rate (FRR). The TAR measures the probability that the recognition model correctly verifies a sample as genuine. The FAR measures the probability that the recognition model incorrectly verifies a sample as genuine. FRR is the measure of likelihood a system incorrectly rejects an access attempt by an authorized user as an unauthorized user. The TAR and FAR are stated as the ratio of the number of true and false acceptances divided by the total number of classification attempts. The FFR is stated as the ratio of the number of false rejections divided by the total number of classification attempts. The combination of these measure are used to denote a system's recognition accuracy along with other verification metrics, such as the widely used equal error rate (EER). EER represents the equilibrium of the FAR and FRR. Below we review those referenced work that used the DCGAN framework to improve biometric systems. Figure 6 below shows an illustration of real and synthetic data being used as the input to a typical recognition model. The referenced work is also shown and summarized in Table 2.

In 2017, Kohli et al. [25] proposed the use of the DCGAN architecture in experiments for generating iris presentation attacks. The propose iDCGAN (iris DCGAN) was used to generate presentation attacks with an iris image quality assessment as a performance metric. To detect presentation attacks the state-of-the-art DESIST framework was used. Experiments include datasets such as IIITD Contact Lens Database, IIT Delhi Iris Database, and MultiSensor Iris Database. The input of the iDCGAN framework uses segmented iris data; only the iris and pupil regions are fed into the framework. After conducting a comparative analysis of the generated iris images' quality, the metrics indicated that the synthetic images produced from the iDCGAN framework very closely resembled the genuine iris images. The state-of-the-art DESIST framework achieved a Presentation Attack Detection (PAD) performance of 92.17% with an equal error rate (EER) of 7.09% on SDB, an existing synthetic database. With the proposed iDCGAN framework, the DESIST framework achieved an accuracy of 85.95% with an EER of 14.19% [25]. Experiments showed that the synthetic iris images generated from the proposed framework are less likely to be detected by the DESIST framework. Compared to an existing synthetic iris database, EER were approximately 2 times higher when using the proposed iDCGAN framework.

In 2018, Wang et al. [26] proposed an improved DCGAN architecture as a data augmentation technique for palmprint recognition. As small datasets can provide insufficient representation for training and lead to overfitting, data augmentation is often necessary in deep learning training. The proposed framework improves upon the DCGAN architecture by applying SSIM into the loss function. Experiments include datasets from CASIA Palmprint and IIT Delhi Palmprint for a mix of GAN-based generation and classical data augmentation strategies for training. For palmprint recognition, the Xception model was used. With the proposed strategies for data augmentation and palmprint recognition, results showed effective recognition with EER of 0.37% on the CASIA Palmprint and 1.52% on IIT Delhi Palmprint datasets [26].

In 2019, Gupta et al. [27] proposed detecting presentation attacks using a single image. Utilizing Support Vector Machines (SVM) for one-class classification and DCGANs to learn the manifold of live samples, a liveness scoring scheme called AnoGAN (Anomaly GAN) is proposed for palm PAD. The proposed framework assures security against an anomaly sample while training solely with live samples, by applying a GAN-based anomaly detection algorithm. AnoGAN utilizes the DCGAN framework to learn the volatility in an abundance of diverse live samples. This process is accompanied by an anomaly-scoring scheme focused on the mapping from image space to latent space. An infinite number of samples can be generated from the DCGAN model used in AnoGAN as it generates synthetic images that are deemed genuine by the system. This method is utilized to improve the overall accuracy of the system and produce improved results while calculating the residual score. Unsupervised learning is used to detect anomalies in the images as prospective fake images. To evaluate the proposed method, a custom-made database containing live and synthetically generated palm samples is created. Results showed the AnoGAN framework reached a 96.8% area under the curve (AUC) and a 3% half total error rate (HTER) [27].

Engelsma et al. [28] proposed a one-class classifier for fingerprint spoof detection. The proposed framework was formed from the discriminator model of the DCGAN framework while being trained solely on live fingerprint images. The DCGAN architecture was chosen due to its inclusion of a classification loss for training the discriminator. As the generator model produces increasingly more realistic fingerprint images to deceive the discriminator, the discriminator model learns more ways to differentiate between the genuine and synthetic fingerprints. For experiments, a custom-made dataset was created. The created dataset was considerably larger and more diverse, in regards to the quantity of subjects, fingers used, materials used, and collection locations, than previously existing Liveness Detection datasets. The proposed algorithm achieved an average True Detection Rate (TDR) of 49.8%, besting the baseline algorithm (binary-CNN) with a TDR of 40.3% [28].

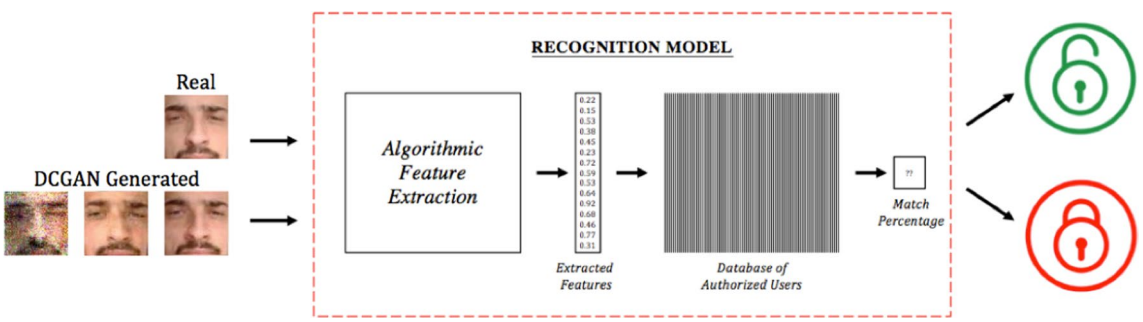

Fig. 6 Illustration of a typical recognition model with the input of real and synthetic images

Table 2 Summary of the uses of the DCGAN framework in biometric systems

References	Model description	Biometric modalities	Datasets	Performance
2017				
Kohli et al. [25]	iDCGAN to generate presentation attacks and DESIST to detect	Iris	IIITD Contact Lens Database, IIT Delhi Iris Database, and MultiSensor Iris Database	Experiments showed that the synthetic iris images generated from the proposed framework are less likely to be detected by the DESIST framework compared to an existing synthetic iris database, with an EER approximately 2 times higher
2018				
Wang et al. [26]	DCGAN for data augmentation and Xception model used for recognition	Palmprint	CASIA Palmprint and IIT Delhi Palmprint	Proposed method generates higher quality images and outperforms other existing methods in recognition
2019				
Gupta et al. [27]	Detecting presentation attacks using a single image with proposed AnoGAN (based on DCGAN) liveness scoring scheme	Palmprint	*Custom-made*	Results showed the proposed framework reached higher Area Under the Curve (AUC) and Half Total Error Rate (HTER) than traditional one-class SVM methods
Engelsma et al. [28]	One-class classifier built from the discriminators of DCGAN	Fingerprint	*Custom-made*	The proposed algorithm achieved a higher True Detection Rate (TDR) than the baseline binary-CNN
Yang et al. [29]	FV-GAN (inspired on DCGAN and CycleGAN)	Finger vein	THU-FVFDT2 and SDU	The experimental results showed that the proposed framework could robustly extract vein patterns that produced higher verification accuracies, verifying the value and efficacy of adversarial training
Xuan et al. [30]	Generate fake samples with DCGAN, WGAN-GP, and PGGAN to improve generalizability of forensics CNN	Face	CelebA-HQ	The experimental results showed that adding an image preprocessing step of GAN generation before training CNN is effective in improving generalization
2020				
Jenkins et al. [31]	DCGAN to generate and GEFE to mitigate presentation attacks	Periocular	BIPLab	The results showed that the proposed technique generates FEs that optimizes the anti-spoofing fitness. From the displacement of the generated FEs, the canthi (eye corners) were found as essential to the identification and mitigation of presentation attacks
Lv et al. [32]	DCGAN to generate images and CNN with ELBP for recognition	Face	CelebA	Experiments showed that the DCGAN framework can effectively expand the training set and improve recognition rates

Table 2 (continued)

References	Model description	Biometric modalities	Datasets	Performance
Ammar et al. [33]	DCGAN to generate images and FaceNet as recognition model	Face	LFW and ChokePoint	Experimental results showed the effectiveness of the proposed approach compared to LBP and PCA methods. Compared to the application of the VGG-16 network, the proposed method also offered higher recognition results
Wang et al. [34]	False Acceptance Attacks (FAA) generation with DCGAN	Palmprint	PolyU	Compared to the fake images in previous existing datasets, the synthetic images generated are considered as genuine images by the normalized Hamming distance
2021				
Li et al. [35]	DCGAN & ProGAN (or PGGAN) to generate fake images and Modified GLCM for detected	Iris	LivDet-Iris-2017-Clarkson	In the experimental results, the proposed method performed considerably better than the conventional texture analysis method of feature matrix combined with SVM classification, as the Modified-GLCM significantly improves upon the original GLCM method
Khaldi et al. [36]	Conditional DCGAN to colorize images and CNN-based models for classification	Ear	AMI ear and Annotated Web Ear (AWE)	The experimental results showed an increase in classification accuracies when using the proposed framework compared to training and testing with grayscale images
2022				
Siddiqui et al. [37]	DCGAN to generate and modified VGGNet to detect the presentation attacks	Iris and periocular	MICHE-I, VISOB, and UBI-Pr	Comparing the test accuracies of the proposed 'modified VGGNet' to the conventional AlexNet and Spoof Net, The best results were achieved using the 'modified VGGNet'
Ammar et al. [38]	DCGAN to generate images and FaceNet as recognition model	Face	LFW, VGGFace2, and ChokePoint	The efficacy of the proposed approach was validated by numerous experiments and compared against commonly used data augmentation and face recognition models. The proposed data augmentation technique generated quality synthetic images with the ability to boost the performance of face recognition systems
2023				
Jabberi et al. [39]	DCGAN and ESRGAN to generate quality images and VGG-Face as recognition model	Face	Youtube Face (YTF), Labeled Face in the Wild (LFW), and Labeled Face Part in the Wild (LFPW)	Using DCGAN and ESRGAN to generate additional facial images for face recognition, results showed the proposed method enlarges facial dataset without degrading recognition rates with face obfuscation

Table 2 (continued)

References	Model description	Biometric modalities	Datasets	Performance
Feng et al. [40]	DCGAN and CNN for Face-based gender recognition	Face	CelebA	Experimental results verified the power of the DCGAN framework for data enhancement and the images generated by the proposed framework effectively improved the performance of the CNN classifier
Ghous et al. [41]	DCGAN for fake video detection	Face	Celeb-DF and Deep Fake Detection Challenge (DFDC)	Experiments showed that the proposed DCGAN produced better results using DFDC and Celeb-DF datasets. The proposed model outperformed in comparison with existing models for detecting fake videos
Guo et al. [42]	DCGAN to generate fake images and Siamese network (based on MobileNet) for recognition	Fingerprint	FVC2002 and FVC2004	Experimental results showed that the DCGAN framework has a superior ability to generate synthetic fingerprint images, as the ridges and valleys of the fingerprints generated are within a reasonable range. Verified by these results, it is evident that a traditional fingerprint recognition system can be deceived by the synthetic fingerprint images generated by the DCGAN framework
Tsai et al. [43]	DCGAN, WGAN, and CycleGAN for generating images and MesoNet as classifier	Palmprint	PolyU palmprint	Multiple adversarial generative networks were used to generate manipulated biometric features and applied deepfake detection techniques. The MesoNet method proved effective in detecting tampered images, and a proposed solution for determining palmprint image manipulation showed promising results
Tangari et al. [44]	Biometric reconstruction inspired from DCGAN and Deep Neural Network (DNN) for recognition	Face and fingerprint	Facescrub, VGGFace2, FlickR-Faces-HQ, PolyU, and Sokoto Coventry Fingerprint Database	Extensive experiments showed the proposed attack could successfully deduce the original recognition model. Using an architecture inspired by the DCGAN framework, biometric reconstructions were effectively crafted and successfully authenticated
Qin et al. [45]	DCGAN for data augmentation and AdveinAU for classification	Palm	PolyU multispectral, Tongji University palmprint, VERA PalmVein	The experimental results showed that the proposed method generates photorealistic and diverse synthetic palm-vein images and drastically improves the classifier's identification accuracy

In Yang et al. [29], the FV-GAN (finger vein GAN) framework was proposed for finger vein extraction and verification. Inspired by DCGAN and CycleGAN, the proposed framework adapts CycleGAN to finger veins with the architectural constraints of DCGANs to build the network's structure. Comparable to CycleGAN, the FV-GAN framework is built with two generators. Utilizing the cycle consistency loss for adversarial training, the Image Generator transforms the data across the raw vein image space and the Pattern Generator transforms the data across the latent vein pattern space. The FV-GAN framework was designed to calculate the probability of vein pixels within the finger vein images and extract the vein patterns from the images. This process is achieved through the FV-GAN framework learning deep pattern representations. FV-GAN learns from the mutual distribution of finger vein images and pattern maps oppose to their direct mapping. The goal of the proposed framework is to achieve more robustness against outliers and vessel breaks. For experiments, the Tsinghua University Finger Vein and Finger Dorsal Texture Database 2 (THU-FVFDT2) and the ShanDong University finger vein database (SDU) were used. The baseline methods, centered on detecting finger vein valleys, performed favorably on existing finger vein databases, but did not perform as well on the THU-FVFDT2 and SDU databases; which were deemed more realistic. The experimental results showed that the FV-GAN framework could robustly extract vein patterns that produced higher verification accuracies, verifying the value and efficacy of adversarial training [29].

In Xuan et al. [30], the generalization ability of image forensic models is evaluated. The proposed approach is to improve a CNN forensic model by applying preprocessed images from GANs. By utilizing this step before CNN training, it forces the discriminator to learn more features that are underlying and transferable. To generate fake datasets, the DCGAN, WGAN-GP (Wasserstein GAN + Gradient Penalty), and PGGAN (Progressive Growing GAN) frameworks were applied to the CelebA dataset for face images. The CNN model was train only on the genuine images from the CelebA dataset and the synthetic images generated by the PGGAN framework. The data generated by the DCGAN and WGAN-GP frameworks were used to test the trained model's generalizability; treated as unseen generated images. Through extensive experiments, results show that the proposed approach is effective in improving the CNN forensic model's overall generalizability [30].

In Jenkins et al. [31], the DCGAN framework was paired with a genetic-based feature extraction technique for the purpose of mitigating presentation attacks. In this work, the DCGAN framework is applied as a data augmentation technique to generate realistic synthetic periocular samples, as the Genetic and Evolutionary Feature Extraction (GEFE) technique is used to train and identify subjects from the genuine and synthetic samples. GEFE is used to optimize the size and displacement of feature extractors (FEs) from texture based technique local binary pattern (LBP), generating distinguishing FEs for subject recognition. The pairing of the DCGAN framework and GEFE was used to identify discriminative biometric features of the periocular region that can be used for subject recognition, as well as mitigate synthetic presentation attacks. For the experiments, the BIPLab dataset of periocular images was used. The results showed that the GEFE + GAN technique generates FEs that optimizes the anti-spoofing fitness, outperforming LBP and GEFE alone. From the displacement of the generated FEs, the canthi (eye corners) were found as essential to the identification and mitigation of presentation attacks [31]. The generated FEs from the GEFE + GAN technique favored the lateral and medial canthus compared to using most of the eye area, using the FEs generated by GEFE only.

In Lv et al. [32], an improved facial recognition algorithm is proposed based on CNN with Extended LBP (ELBP) and the DCGAN framework. ELBP used a circularized LBP operator, which takes the calculated pixels as the center of the circle. The circular operator can use any size and adjust the coverage area arbitrarily tightly. The ELBP algorithm can effectively reduce the influence of illumination. The eigenvalues extracted by the ELBP algorithm have gray and rotation invariance, and are very robust to illumination; which greatly improves the recognition rate. The DCGAN algorithm solves the problem of insufficient training set through data augmentation. Experiments were conducted using the CelebA face dataset. Results showed the traditional CNN method achieved a recognition rate of 70% as the proposed CNN with ELBP and DCGAN increased the recognition rate to 85% [32]. Experiments showed that the DCGAN framework can effectively expand the training set and improve recognition rates.

Ammar et al. [33] also proposed data augmentation using the DCGAN framework to increase the total number of samples in a face dataset. The proposed method uses the DCGAN framework to generate more face samples as the FaceNet model is used for image classification. For experimentation, the Labeled Faces in the Wild (LFW) Database and Chockepoint video Database were used. Results showed the using the DCGAN framework for data augmentation followed by using the FaceNet model for face recognition was more effective than using standard data augmentation methods, showing an increase in recognition rates as more DCGAN generated images were added. The proposed approach was compared against conventional face recognition techniques such as Principal Component Analysis (PCA) and LBP. Experimental results showed the effectiveness of the proposed approach with DCGAN-based data augmentation compared to

LBP and PCA methods. Compared to the application of the VGG-16 network, the proposed DCGAN and FaceNet-based method also offered higher recognition results [33].

Wang et al. [34] proposed the use of the DCGAN framework to generate fake palmprint images for False Acceptance Attacks (FAA). The DCGAN framework improves upon the mode collapse problem in most GANs by generating diverse samples. With FAA, the success rate is proportional to the diversity of the synthetic samples. FAA do not require users' image samples to be genuine and can be initiated merely with synthetic images of high naturalness. In experiments, the PolyU dataset was used. To measure the dissimilitude of genuine and synthetic images, the normalized Hamming distance was used. Compared to the fake images in previous existing datasets, the synthetic images generated with the DCGAN framework are considered as genuine images [34].

In 2021, Li et al. [35] proposed an iris presentation attack detection method. The proposed method, Modified-GLCM, is a combination of an improved Gray Level Co-occurrence Matrix and a binary classification neural network. The LivDet-Iris-2017-Clarkson iris dataset was used to test the performance of the proposed method. For the purpose of verifying the iris adversarial samples' aggressiveness, the DCGAN and ProGAN (Progressive GAN, also known as PGGAN) frameworks were used to train and generate iris adversarial samples. The accuracy of the proposed method was evaluated by training the Modified-GLCM with and without iris adversarial samples. The proposed method showed, in the experimental results, that it performed considerably better than the conventional texture analysis method of feature matrix combined with SVM classification, as the Modified-GLCM significantly improves upon the original GLCM method. The proposed method achieved a live samples rejection rate of 2.22% and a spoof samples acceptance rate of 1.97% [35].

In Khaldi et al. [36], a novel approach to ear recognition is proposed. To supplement the negative impact of grayscale and dark images on recognition, a two-model framework was proposed using the DCGAN to colorize images and CNN-based classification. The CNN models used for training and testing included AlexNet, VGG-16, and VGG-19. For the experiments conducted, the AMI ear and AWE (Annotated Web Ears) datasets were used. Training with grayscale images only show a significant reduction in recognition rate compared to the original color images. Results indicated that training the models solely on grayscale images might not be sufficient enough to identify grayscale test images. The proposed model addresses the concerns of the absence of color data in test images when fed into a model trained with colored images. Results using the proposed framework indicated higher classification accuracies, with improvement of 3.28% and 9.35% on VGG-16 and VGG-19 models respectively [36].

In 2022, Siddiqui et al. [37] proposed mitigating presentation attacks using a combination of the DCGAN framework and a modified VGGNet. The MICHE-I, VISOB, and UBI-Pr datasets, containing iris and periocular images, were used to generate synthetic photorealistic images for presentation attacks. The DCGAN generated images were used in training the modified VGGNet. To validate results, performance accuracies were compared with the conventional Alex-Net and Spoof Net as a baseline. Results showed significantly high detection accuracies, with the proposed method outperforming the two baseline classifiers. The modified VGGNet produced high true positive rate, with the UBI-Pr periocular dataset performing higher accuracy than all the other datasets.

Ammar et al. [38], proposed a face identification method utilizing the DCGAN framework and basic image manipulation for data augmentation. The proposed method uses a Multi-task Cascaded Convolutional Neural Network (MTCNN) for face detection, processing, and cropping by exploiting facial landmarks. The DCGAN framework uses the output of the MTCNN as the input to generate synthetic images. Basic image manipulations, including geometric transformations, brightness change, and filter operations, are also employed on the images generated by the DCGAN framework. The additional images are added to the dataset, thus both expanding the dataset for training and enhancing the generalizability of the recognition model. For face recognition, the FaceNet model with SVM is proposed. Experiments were conducted using the LFW dataset, the VGGFace2 dataset, and the ChokePoint video dataset. The efficacy of the proposed approach was validated by numerous experiments and compared against commonly used data augmentation and face recognition models. The proposed DCGAN-based data augmentation technique generated quality synthetic images with the ability to boost the performance of face recognition systems.

In 2023, Jabberi et al. [39] proposed using DCGAN and ESRGAN to generate high quality face images as data augmentation. The main objective of this research is to explore more novel data augmentation techniques opposed to traditional geometric and photometric transformations. For experiments, the Youtube Face (YTF), Labeled Face in the Wild (LFW), and Labeled Face Part in the Wild (LFPW) datasets were used. Controlled pose variations from theses datasets were generated and fed into the DCGAN framework to generate additional realistic face images. The ESRGAN model was the used to improve the quality of the synthetic images, making them more photorealistic. After image generation, face recognition using the pretrained VGG-Face model was performed with outstanding classification accuracies. Results showed the proposed method enlarges facial dataset without degrading recognition rates with face obfuscation [39].

In Feng et al. [40], a method for face-based gender recognition was proposed. Fake face images generated by the DCGAN framework and the complementary real faces are used to train a CNN classifier for the gender classification of human faces. Experiments were conducted using the CelebA dataset as the input to the DCGAN and CNN models. Three types of datasets were formed for training the CNN model, an all-real dataset, an all-fake dataset, and a real-fake mixed dataset. Experimental results verified the power of the DCGAN framework for data enhancement and the face images generated by the DCGAN framework effectively improved the performance of the CNN classifier.

Ghous et al. [41] proposed fake face video detection using the DCGAN framework. Image frames were extracted from videos in the Celeb-DF and Deep Fake Detection Challenge (DFDC) datasets. From the extracted face images, the DCGAN framework is used to detect real and fake faces. Existing techniques, such as VGG-16 and Resnet-50, were also used for fake video detection, as a baseline comparator. Experimental results showed the DCGAN framework produced a high of 95.6% and 93.5%, on the Celeb-DF and DFDC datasets respectively. For the baseline methods, fake face detection achieved an accuracy of 84.0%, on the Celeb-DF datasets, for both the VGG-16 and the Resnet-50 models. On the DFDC datasets, the baseline methods produced a high of 81.0% accuracy and 68.0% accuracy, on the VGG-16 and Resnet-50 models respectively [41]. The proposed model outperformed existing models, producing better results on the Celeb-DF and DFDC datasets.

Guo et al. [42] proposed using the DCGAN framework for generating fake fingerprints and using a Siamese Network matching model for fingerprint recognition. Utilizing FVC2002 and FVC2004 datasets in the DCGAN model, the generated fingerprints are passed into the Siamese Network, along with its complement data, to determine if a match is successfully found. The proposed Siamese Network, based on MobileNet, is used to verify the trustworthiness of fingerprint recognition systems. The process involves two distinctive images being fed simultaneously into two similar or identical networks to acquire their feature representations. The similitude of the two feature representations is calculated for two-class classification. Experimental results showed that the DCGAN framework has a superior ability to generate synthetic fingerprint images, although some images showed gaps between the fingerprint patterns. The generated synthetic fingerprint images exhibited a substantial resemblance to genuine fingerprints as the ridges and valleys of the fingerprints generated are within a reasonable range [42]. Verified by these results, it is evident that a traditional fingerprint recognition system can be deceived by the synthetic fingerprint images generated by the DCGAN framework.

In Tsai et al. [43], deepfake detection for palmprint authentication is proposed. To generate fake datasets, the DCGAN, WGAN, and CycleGAN frameworks were applied to the Poly-U palmprint database. The MesoNet model, a binary classifier built as a relatively shallow CNN trained to classify images into one of two classes, is used to detect deepfakes. The proposed DCGAN framework revealed a gradual improvement in the graphical fidelity of the generated synthetic images as the training epochs increased. The WGAN framework demonstrated improved stability and generated high-quality images with reduced mode collapse compared to traditional GANs. The CycleGAN framework exhibited high fidelity and captured essential palmprint features. All datasets were evaluated using the MesoNet model with an average AUC value 0.66 [43].

In Tangari et al. [44], an investigation on the reconstruction of biometric representation is conducted. In the case of an attacker being able to retrieve a feature-space representation without full access to the original image dataset or learned model, research propose using the DCGAN framework for biometric reconstruction and the use of Deep Neural Networks (DNN) for recognition. A two-pronged attack is proposed, first inferring the original DNN by manipulating the embedding to gain the model footprint. Next, the raw data is reconstructed by utilizing the inferred model. To show the practicality of the attacks, two modalities, face and fingerprints, were used in the experiments. For the face datasets, Facescrub, VGGFace2, and FlickR-Faces-HQ were used. For the fingerprint datasets, PolyU and Sokoto Coventry Fingerprint Database were used. Results showed that an attack could successfully deduce the original recognition model, with a mean accuracy of 83% for the face datasets and a mean accuracy of 86% for the fingerprint datasets [44]. Using an architecture inspired by the DCGAN framework, biometric reconstructions were effectively crafted and successfully authenticated.

Qin et al. [45] proposed Adversarial vein AUtomatic AUgmentation (AdveinAU), a novel adversarial learning-based data augmentation method. The proposed approach utilizes the DCGAN framework for data augmentation and trains a vigorous classifier for vein identification by optimizing training in the vein classifier and the latent variable set search concurrently. During the training, the conditional DCGAN's focus is to learn the sample distribution. The generator of the DCGAN model is linked with the target classifier to construct the AdveinAU network. The resulting classifier is employed for vein classification. For experiments, the PolyU multispectral, Tongji University palmprint, and VERA PalmVein datasets were used. The experimental results showed that AdveinAU generates photorealistic and diverse synthetic palm-vein images and drastically improves the classifier's identification accuracy [45].

4 Discussion

In the first category of the literature survey, we focused on the reference papers that concentrated on generated quality biometrics. Choi et al. [14] generated quality synthetic fingerprint samples. Using numerous evaluating metrics such as Hamming distance, Pearson correlation of histograms, and Intersection of Union, experiments found the generated fingerprints to be of quality to that of actual fake fingerprint. A deeper analysis in fake fingerprint generation occurred in Vincent et al. [20]. Experimental results showed the performance of the DCGAN framework fingerprint generation was validated using the Structural Similarity Index (SSIM) and Fréchet Inception Distance (FID). The generated fingerprint showed high quality in terms of ridge structure and ridge endings, with a better resolution than that of existing synthetic datasets. Barni et al. [19] focused on iris generation from the DCGAN framework. With the purpose of iris deidentification, the objective was to generative photorealistic synthetic iris samples deprived of any distinctive biometric data associated to the original iris. The deidentification capabilities of the proposed method were analyzed with results showing that the existing iris recognition algorithms were unable to extract distinguishing features from the generated synthetic samples. In Bamoriya et al. [21], a variant of DCGAN, DSB-GAN was proposed and evaluated on fingerprint, iris, and palmprint modalities. The performance of DSB-GAN had minimal reconstruction error and a high SSIM score. Compared to DSB-GAN, all other methods have a higher FID and MS-SSIM value. According to the FID and MS-SSIM metrics, the generated synthetic images produced by the DSB-GAN framework are diverse with high variations. Results verified high similarity in the generated images and low variation between the genuine input images and the reconstructed biometric images [21].

The generation of fake faces using the DCGAN framework was a major focus in a number of experiments. In Liu et al. [18], the focus was on generation with low computing resources. Although increasing the number of training epochs have some positive effects towards enhancing the generative model and its output, at the fourth epoch, the generator and the discriminator models mutually demonstrated convergence to the distribution of the dataset. In Canan et al. [22], results showed that the quality of generated synthetic face images was accurately proportional to increases in training data and training epochs In Shariff et al. [17], SSIM was used to provide a quantitative assessment of the trained DCGAN model. The results verified the DCGAN generated synthetic facial images could be used to enhance the training of other models for a variety of supervised learning tasks. In Xiangli et al. [16], the RealnessGAN was proposed based on the DCGAN framework. RealnessGAN achieved better scores in both FID and Sliced Wasserstein Distance (SWD) metrics, with a smoother and steadier learning process, than baseline approaches. Kapalavai et al. [24] proposed generating face samples with the DCGAN framework and using the Enhanced Super-Resolution GANs (ESRGAN) framework to improve the quality of synthetic images. The SSIM scores obtained from the generated images verified the proposed model's proficiency in generating facial images. The results from these research papers presented the power of the DCGAN framework in generating quality photorealistic images. In terms of a number of metrics, including the commonly used SSIM and FID metrics, the images generated are highly similar to existing real and synthetic datasets while also being quite diverse. The results indicated that the synthetic biometric images generated could be used as spoofing datasets, across a number of modalities and could be helpful as adversarial training in recognition models.

In the second category of the literature survey, we focused on the reference papers that used the DCGAN framework to improve recognition models. A few papers referenced using the DCGAN framework and it variants alone as a model for recognition and spoofing detection. In Gupta et al. [27], a liveness scoring scheme called AnoGAN (Anomaly GAN) was proposed for palmprint presentation attack detection. AnoGAN utilizes the DCGAN framework to learn the volatility in an abundance of diverse live samples. The proposed PAD algorithm achieved high AUC and HTER score, performing better than conventional one-class SVM systems. Engelsma et al. [28] proposed a one-class classifier for fingerprint spoof detection. The proposed framework was formed from the discriminator model of the DCGAN framework while being trained solely on live fingerprint images. The proposed approach bested traditional binary-class spoof detection algorithms. In Yang et al. [29], the FV-GAN (finger vein GAN) framework was proposed for finger vein extraction and verification Inspired by DCGAN and CycleGAN, the proposed framework adapts CycleGAN to finger veins with the architectural constraints of DCGANs to build the network's structure. The experimental results showed that the FV-GAN framework could robustly extract vein patterns that produced higher verification accuracies, verifying the value and efficacy of adversarial training. Ghous et al. [41] proposed fake face video detection using the DCGAN framework. Existing techniques, such as VGG-16 and Resnet-50 were used as a baseline comparator. Experimental results showed the DCGAN framework outperformed existing models, producing better detection results.

Some papers used the DCGAN framework to generated images simply as a data augmentation tool with the goal to expand the dataset to optimized training in recognition models. In Lv et al. [32], the DCGAN algorithm solves the problem

of insufficient training set through data augmentation. DCGAN is used in combination with a CNN + ELBP recognition model. Experiments showed that the DCGAN framework can effectively expand the training set and improve recognition rates, besting traditional CNN methods. The DCGAN framework is used again to expand the dataset in Feng et al. [40] for face-based gender recognition. Experiments were conducted as the real and fake faces were used to train a CNN classifier for the gender classification of human faces. Wang et al. [34] proposed an improved DCGAN architecture as a data augmentation technique for palmprint recognition, as small datasets can provide insufficient representation for training and lead to overfitting. The proposed framework improves upon the DCGAN architecture by applying SSIM into the loss function. Experiments included a mix of GAN-based generation and classical data augmentation strategies for training. The Xception model was for palmprint recognition, with the proposed strategies showing effective recognition results. Ammar et al. [33] also proposed data augmentation using the DCGAN framework to increase the total number of samples in a face dataset. The proposed method uses the DCGAN framework to generate more face samples as the FaceNet model is used for image classification. Results showed the using the DCGAN framework for data augmentation followed by using the FaceNet model for face recognition was more effective than using standard data augmentation methods, showing an increase in recognition rates as more DCGAN generated images were added. Experimental results from these papers verified the power of the DCGAN framework for data enhancement and the images generated by DCGAN effectively improved the performance of the CNN classifiers.

The rest of the research papers in the literature review used the DCGAN framework to generated quality synthetic images as adversarial training to analyze or improve recognition models for potential spoofing attacks, like presentation attacks. Wang et al. [26] proposed generating fake palmprint images for False Acceptance Attacks (FAA), using the DCGAN framework. FAA do not require genuine users' images and can be launched simply with synthetic images with high naturalness. In experiments, compared to the fake images in previous existing datasets, the fake images generated with DCGAN were evaluated as real images with better naturalness. In Tsai et al. [40], deepfake detection for palmprint authentication is proposed. To generate fake datasets, the DCGAN, WGAN, and CycleGAN frameworks were applied. The MesoNet model is used to detect deepfakes, achieving above average recognition results. Guo et al. [42] proposed using the DCGAN framework for generating fake fingerprints and using a Siamese Network matching model for fingerprint recognition. Experimental results showed that the DCGAN framework has a superior ability to generate synthetic fingerprint images, although some images showed gaps between the fingerprint patterns. The generated synthetic fingerprint images exhibited a substantial resemblance to genuine fingerprints as the ridges and valleys of the fingerprints generated are within a reasonable range. Verified by these results, it is evident that a traditional fingerprint recognition system can be deceived by the synthetic fingerprint images generated by the DCGAN framework. In Kohli et al. [25], iDCGAN (iris DCGAN) was proposed for generating synthetic images as iris presentation attacks. To detect presentation attacks the DESIST framework was used. After conducting a comparative analysis of the generated iris images' quality, the metrics indicated that the synthetic images produced from the iDCGAN framework very closely resembled the genuine iris images. Experiments showed that the synthetic iris images generated from the proposed framework are less likely to be detected by the DESIST framework. Compared to an existing synthetic iris database, EER were approximately 2 times higher when using the proposed iDCGAN framework. In Li et al. [35], an iris presentation attack detection method was proposed using a Modified-GLCM (Gray Level Co-occurrence Matrix). For the purpose of verifying the iris adversarial samples' aggressiveness, the DCGAN and ProGAN frameworks were used to train and generate iris adversarial samples. The experimental results showed that the proposed method performed considerably better than the conventional texture analysis method of feature matrix combined with SVM classification, as the Modified-GLCM significantly improves upon the original GLCM method. In Jenkins et al. [31], the DCGAN framework was paired with a genetic-based feature extraction technique, Genetic and Evolutionary Feature Extraction (GEFE), for presentation attack mitigation on periocular images. The results showed that the GEFE + GAN technique optimizes the anti-spoofing fitness of the generated FEs, outperforming the baseline LBP and GEFE alone. From the displacement of the generated FEs, the canthi (eye corners) were found as keys to identification and presentation attack mitigation. The generated FEs from the GEFE + GAN technique favored the lateral and medial canthus over using the entire eye area, from the GEFE FEs. In Siddiqui et al. [37], mitigating presentation attacks on iris and perioculor was proposed using a combination of the DCGAN framework and a modified VGGNet. To validate results, performance accuracies were compared with the conventional Alex-Net and Spoof Net as a baseline. Results showed significantly high detection accuracies, with the proposed method outperforming the two baseline classifiers. The modified VGGNet produced high true positive rate, with the UBI-Pr periocular dataset performing higher accuracy than all the other datasets. In Xuan et al. [30], the generalization ability of image forensic models is evaluated for face images. To generate fake datasets, the DCGAN, WGAN-GP (Wasserstein GAN + Gradient Penalty), and PGGAN (Progressive Growing GAN) frameworks were applied. The CNN model was train only on the real images and the

fake data generated by the PGGAN framework. The data generated by the DCGAN and WGAN-GP frameworks were used for testing the generalization ability of trained model; treated as unseen generated spoof images. Through extensive experiments, results show that the proposed approach was effective in improving the CNN forensic model's generalizability. Ammar et al. [38] proposed face identification using data augmentation based on a combination of the DCGAN framework and basic image manipulation. Basic image manipulations, including geometric transformations, brightness change, and filter operations, are also employed on the images generated by the DCGAN framework. The additional images are added to the dataset, thus both expanding the dataset for training and enhancing the generalizability of the recognition model. For face recognition, the FaceNet model with SVM is proposed. The efficacy of the proposed approach was validated by numerous experiments and compared against commonly used data augmentation and face recognition models. The proposed DCGAN-based data augmentation technique generated quality synthetic images with the ability to boost the performance of face recognition systems. The results from these papers revealed by utilizing the DCGAN framework during the training of biometric recognition models, it forces the model to learn more intrinsic and generalizable features for recognition. By improving the generalizability, it improves the accuracies of the model as it best prepares for potential spoofing attacks.

5 Conclusion

The Deep Convolutional Generative Adversarial Network (DCGAN) is an improved GAN model in generating synthetic images. Throughout the years, there has been an exponential growth in the use of DCGANs in a multitude of fields and applications. There is also an increase in the DCGAN use with biometrics in the cybersecurity space.

This review outlines the most recent research involving DCGAN usage to strengthen biometric authentication systems. Research shows promising results in the DCGAN's capability to render high-quality, realistic yet synthetic biometric samples; often indistinguishable from is genuine counterparts. Often used as a data augmentation technique, the DCGAN technique can provide a larger data set for the training of large neural networks. Through data augmentation and adversarial training, biometric systems' generalizability and performance are often improved. With significant improvements in the verification performance with regards to verification accuracy and EER, the value of the DCGAN framework and the efficacy of adversarial training are corroborated. The research in GANs is vast and this article was composed to consolidate articles specific to the DCGAN architecture with respects to biometric systems and build a concise review. Deepfakes are becoming more prevalent and have a strong capability of spoofing biometric recognition systems. GANs are one of the leading sources to generating deepfakes and the DCGAN framework is one of the most widely used GAN architectures. In the future, we envisioned this review to be used as a directive for the advancement of future biometric systems. This work outlines a multitude of techniques to generating quality synthetic biometrics and its capabilities to mimic authentic biometric samples. These procedures can be review and expanded to improve the process of generating biometrics. This work also outlines techniques in using the generated biometrics as data augmentation and adversarial training to improve biometric recognition models. These procedures can also be followed and expanded to improve existing and future recognition models. As biometric access control systems are becoming common for everyday use, the desire to combat unauthorized access and ensure security is in high demand.

Acknowledgements This research is supported by the National Science Foundation (NSF). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of NSF.

Author contributions J.J. wrote the main manuscript text. K.R. provided conceptual guidance and supervision for manuscript. All authors reviewed the manuscript.

Data availability No datasets were generated or analysed during the current study.

Declarations

Competing interests The authors declare no competing interests.

References

1. Korshunova I, Shi W, Dambre J, Theis L. Fast face-swap using convolutional neural networks. In Proceedings of the IEEE international conference on computer vision. 2017. pp. 3677–85.
2. Wan Z, Zhang Y, He H. Variational autoencoder based synthetic data generation for imbalanced learning. In: 2017 IEEE symposium series on computational intelligence (SSCI). IEEE. 2017. p. 1–7.
3. Goodfellow I, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D, Ozair S, Bengio Y. Generative adversarial nets. Adv Neural Inf Process Syst. 2014;27.
4. Hitawala S. Comparative study on generative adversarial networks. arXiv preprint arXiv:1801.04271. 2018.
5. Xu Q, Huang G, Yuan Y, Guo C, Sun Y, Wu F, Weinberger K. An empirical study on evaluation metrics of generative adversarial networks. arXiv preprint arXiv:1806.07755. 2018.
6. Wiatrak M, Albrecht SV, Nystrom A. Stabilizing generative adversarial networks: a survey. arXiv preprint arXiv:1910.00927. 2019.
7. Sajeeda A, Hossain BM. Exploring generative adversarial networks and adversarial training. Int J Cogn Comput Eng. 2022;3:78–89.
8. Wang Z, She Q, Ward TE. Generative adversarial networks in computer vision: a survey and taxonomy. ACM Comput Surv. 2021;54(2):1–38.
9. Yinka-Banjo C, Ugot OA. A review of generative adversarial networks and its application in cybersecurity. Artif Intell Rev. 2020;53:1721–36.
10. Aggarwal A, Mittal M, Battineni G. Generative adversarial network: an overview of theory and applications. Int J Inf Manag Data Insights. 2021;1(1):100004.
11. Radford A, Metz L, Chintala S. Unsupervised representation learning with deep convolutional generative adversarial networks. arXiv preprint arXiv:1511.06434. 2015.
12. Bushra SN, Maheswari KU. Crime investigation using DCGAN by forensic sketch-to-face transformation (STF)—a review. In: 2021 5th International Conference on Computing Methodologies and Communication (ICCMC). IEEE. 2021. p. 1343–8.
13. Bushra SN, Ali LJ. A review on fuzzy face recognition (FFR) using DCGAN. In: 2021 5th International Conference on Computing Methodologies and Communication (ICCMC). IEEE. 2021. p. 1299–305.
14. Choi SH, Jung SH. Similarity analysis of actual fake fingerprints and generated fake fingerprints by DCGAN. Int J Fuzzy Log Intell Syst. 2019;19(1):40–7.
15. Liu S, Yu M, Li M, Xu Q. The research of virtual face based on Deep Convolutional Generative Adversarial Networks using TensorFlow. Physica A. 2019;521:667–80.
16. Xiangli Y, Deng Y, Dai B, Loy CC, Lin D. Real or not real, that is the question. arXiv preprint arXiv:2002.05512. 2020.
17. Shariff DM, Abhishek H, Akash D. Artificial (or) fake human face generator using generative adversarial network (GAN) machine learning model. In: 2021 Fourth International Conference on Electrical, Computer and Communication Technologies (ICECCT). IEEE. 2021. p. 1–5.
18. Liu W, Gu Y, Zhang K. Face generation using DCGAN for low computing resources. In: 2021 2nd International Conference on Big Data & Artificial Intelligence & Software Engineering (ICBASE). IEEE. 2021. p. 377–82.
19. Barni M, Labati RD, Genovese A, Piuri V, Scotti F. Iris deidentification with high visual realism for privacy protection on websites and social networks. IEEE Access. 2021;9:131995–2010.
20. Vincent DJ, Hari VS. Synthetic finger print image generation using modified deep convolutional GAN. In: 2021 Fourth International Conference on Microelectronics, Signals & Systems (ICMSS). IEEE. 2021. p. 1–5.
21. Bamoriya P, Siddhad G, Kaur H, Khanna P, Ojha A. DSB-GAN: generation of deep learning based synthetic biometric data. Displays. 2022;74:102267.
22. Canan KOÇ, Özyurt F. An examination of synthetic images produced with DCGAN according to the size of data and epoch. Firat Univ J Exp Comput Eng. 2023;2(1):32–7.
23. Kumar M, Sharma HK. A GAN-based model of deepfake detection in social media. Proc Computer Sci. 2023;218:2153–62.
24. Kapalavai H, Mondal S. Generating new human faces and improving the quality of images using generative adversarial networks (GAN). In: 2023 2nd International Conference on Edge Computing and Applications (ICECAA). IEEE. 2023. p. 1647–52.
25. Kohli N, Yadav D, Vatsa M, Singh R, Noore A. Synthetic iris presentation attack using iDCGAN. In: 2017 IEEE International Joint Conference on Biometrics (IJCB). IEEE. 2017. p. 674–80
26. Wang G, Kang W, Wu Q, Wang Z, Gao J. Generative adversarial network (GAN) based data augmentation for palmprint recognition. In: 2018 Digital Image Computing: Techniques and Applications (DICTA). IEEE. 2018. p. 1–7.
27. Gupta V, Nishigaki M, Ohki T. Unsupervised biometric anti-spoofing using generative adversarial networks. Int J Inf Soc. 2019;11(1):5.
28. Engelsma JJ, Jain AK. Generalizing fingerprint spoof detector: learning a one-class classifier. In: 2019 International Conference on Biometrics (ICB). IEEE. 2019. p. 1–8.
29. Yang W, Hui C, Chen Z, Xue JH, Liao Q. FV-GAN: finger vein representation using generative adversarial networks. IEEE Trans Inf Forensics Secur. 2019;14(9):2512–24.
30. Xuan X, Peng B, Wang W, Dong J. On the generalization of GAN image forensics. In: Chinese conference on biometric recognition. Cham: Springer International Publishing; 2019. p. 134–41.
31. Jenkins J, Roy K, Shelton J. Using deep learning techniques and genetic-based feature extraction for presentation attack mitigation. Array. 2020;7:100029.
32. Lv T, Wen C, Zhang J, Chen Y. A face recognition algorithm based on CNN with ELBP and DCGAN. In: 2020 International Symposium on Computer Engineering and Intelligent Communications (ISCEIC). IEEE. 2020. p. 99–102.

33. Ammar S, Bouwmans T, Zaghden N, Neji M. Towards an effective approach for face recognition with DCGANs data augmentation. In: Advances in Visual Computing: 15th International Symposium, ISVC 2020, San Diego, CA, USA, October 5–7, 2020, Proceedings, Part I 15. Springer International Publishing. 2020. p. 463–75.
34. Wang F, Leng L, Teoh ABJ, Chu J. Palmprint false acceptance attack with a generative adversarial network (GAN). Appl Sci. 2020;10(23):8547.
35. Li D, Wu C, Wang Y. A novel iris texture extraction scheme for iris presentation attack detection. J Image Gr. 2021;9(3):1–12.
36. Khaldi Y, Benzaoui A. A new framework for grayscale ear images recognition using generative adversarial networks under unconstrained conditions. Evol Syst. 2021;12(4):923–34.
37. Siddiqui N, Dave R. Mitigating presentation attack using DCGAN and Deep CNN. arXiv preprint arXiv:2207.00161. 2022.
38. Ammar S, Bouwmans T, Neji M. Face identification using data augmentation based on the combination of DCGANs and basic manipulations. Information. 2022;13(8):370.
39. Jabberi M, Wali A, Alimi AM. Generative data augmentation applied to face recognition. In: 2023 International Conference on Information Networking (ICOIN). IEEE. 2023. p. 242–7
40. Feng H. Face-based gender recognition with small samples generated by DCGAN using CNN. In Fifth International Conference on Computer Information Science and Artificial Intelligence (CISAI 2022). Vol. 12566. SPIE. 2023. p. 634–40.
41. Ghous H, Malik MH, Qadri S, Ahmad N. Detection of fake videos using convolutional generative method. J Comput Biomed Inf. 2023;4(02):8–17.
42. Guo J. Deep learning-enhanced fingerprint generation and security verification in the context of Siamese network matching models. In: 2023 4th International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE). IEEE. 2023. p. 293–7
43. Tsai MJ, Cheng-Tao C. Deepfake detection for palmprint authentication. In: 2023 International Conference on Systems, Man, and Cybernetics (SMC). IEEE. 2023.
44. Tangari G, Keskar S, Asghar HJ, Kaafar D. On the adversarial inversion of deep biometric representations. arXiv preprint arXiv:2304.05561. 2023.
45. Qin H, Xi H, Li Y, El-Yacoubi MA, Wang J, Gao X. Adversarial learning-based data augmentation for palm-vein identification. In: IEEE Transactions on Circuits and Systems for Video Technology. 2023.