Pattern Recognition 155 (2024) 110655

Contents lists available at ScienceDirect

Pattern Recognition

journal homepage: www.elsevier.com/locate/pr

Toward comprehensive and effective palmprint reconstruction attack

Licheng Yan [a], Fei Wang [a], Lu Leng [a,*], Andrew Beng Jin Teoh [b]

[a] Jiangxi Province Key Laboratory of Image Processing and Pattern Recognition, Nanchang Hangkong University, 696 Fenghe Nan Avenue, Nanchang, 330063, Jiangxi, PR China

[b] School of Electrical and Electronic Engineering, College of Engineering, Yonsei University, 50 Yonsei-ro, Seodaemun-gu, 120749, Seoul, Republic of Korea

ARTICLE INFO

Keywords:
Palmprint recognition
Reconstruction attack
Double reuse training strategy
Scale-adaptive multi-texture complementarity
Generative adversarial network

ABSTRACT

The challenge posed by the template-based reconstruction attack significantly impacts the security and privacy of biometric systems. Current reconstruction techniques rely on extensive training data or encounter limitations in adaptability, resulting in subpar reconstruction performance. In this paper, we propose a black-box palmprint template reconstruction method based on the modified Progressive GAN (ProGAN), which achieves a substantial success rate in attacking deep-learning-based and hand-crafted-based templates. Our approach incorporates the dropout mechanism into the generator of ProGAN and introduces a Double Reuse Training Strategy to enable effective training of the reconstruction network despite limited data. Furthermore, we devise a novel Scale-Adaptive Multi-Texture Complementarity loss, enhancing the texture quality of reconstructed images. We conduct extensive experiments on diverse palmprint recognition techniques. The resulting reconstructed images exhibit exceptional image quality. Additionally, we thoroughly examine the security and privacy aspects of the palmprint recognition algorithm based on the insights gained from the reconstruction attacks.

1. Introduction

Biometric authenticating rely on unique human traits like palmprint and face. This method surpasses traditional passwords in usability but comes with privacy concerns. During enrollment, a representative template is stored in a database, referred to during subsequent verification. While original data is discarded for security, templates can be stolen or leaked without proper safeguards, allowing attackers to create fake biometric images to gain unauthorized access and compromise privacy.

Existing template-based reconstruction attacks demand a substantial quantity of training data [1–3] or lack versatility [4–9], in which the attack technique cannot be efficiently utilized across various feature extraction algorithms. Furthermore, the intricate characteristics inherent in reconstruction methods give rise to a significant challenge concerning the overall fidelity of the resultant image [10]. Nonetheless, exploring this facet remains limited, necessitating a more exhaustive evaluation criterion to establish a confident and comprehensive appraisal of the reconstructed image quality. This paper centers on reconstructive attacks on palmprint biometric systems, which are valued for their unique, stable, user-friendly, and reliable traits. The pipeline of the palmprint reconstruction attack is depicted in Fig. 1.

Here are the necessary terminology in this paper: (1) Deep-learning-based method: Deep neural network-based palmprint recognition methods. (2) Hand-crafted-based method: Hand crafted-based palmprint recognition methods. (3) Deep template: Template derived from deep-learning-based methods. (4) Hand template: Template derived from hand-crafted-based methods.

This paper introduces a novel black-box palmprint template-based reconstruction attack technique. The proposed method leverages a Progressive GAN (ProGAN) [11] to reconstruct highly realistic images using only one palmprint template. To address the challenges of limited training data and potential overfitting, a dropout mechanism is incorporated into the ProGAN. Furthermore, a novel loss function called Scale-Adaptive Multi-Texture Complementarity (SAMTC) loss is introduced to minimize the texture feature discrepancies between the target and reconstructed images across multiple scales and orientations. Moreover, a Double Reuse Training Strategy (DRTS) is devised to maximize the utilization of a small training dataset during the training process of our reconstruction model.

The method proves effective for both hand-crafted and deep-learning palmprint templates despite limited data. Single-algorithm attacks often hit 100% success, regardless of algorithm strength, and cross-algorithm attacks still perform well. Impressive results extend to cross-dataset scenarios. The reconstructed palmprint images meet quality standards, including similarity, naturalness and realism. Security assessments show deep-learning methods resisting reconstruction attacks better than hand-crafted approaches.

* Corresponding author.
E-mail addresses: 2116085400002@stu.nchu.edu.cn (L. Yan), 18726485467@163.com (F. Wang), leng@nchu.edu.cn (L. Leng), bjteoh@yonsei.ac.kr (A.B.J. Teoh).

https://doi.org/10.1016/j.patcog.2024.110655
Received 10 December 2023; Received in revised form 4 April 2024; Accepted 1 June 2024
Available online 4 June 2024

Table 1
Template-based reconstruction methods for various biometrics.

Ref.	Year	Modality	Template	Methodology	Training samples	Image quality S/N/R	Attack success rate
[1]	2018	Face	Deep	Neighbor deconvolution network	2,093,002	M/L/L	H
[2]	2021	Face	Deep	ProGAN with bijection metric loss	490,000	H/H/M	H
[3]	2022	Face	Deep	[2] with attention	490,000	H/H/M	H
[4]	2021	Face	Deep	Pretrained StyleGAN2 and regression network	–	L/H/M	L
[5]	2022	Face	Deep	Pretrained StyleGAN2 and genetic algorithm	–	M/H/H	L
[10]	2020	Iris	Hand Deep	Generator constituted by pretrained U-Net	64,980	M/M/M	H M
[6]	2019	Fingerprint	Hand	Pix2pix	1,900	H/M/M	H
[7]	2021	Finger vein Hand vein	Hand	Pix2pix	19,000 3,000	H/M/M	H
[8]	2022	Palmprint	Hand	Style transfer	S:1 M:600	S:L/M/M M:L/L/L	H H
[9]	2022	Palmprint	Hand	Reinforcement strategy	–	H/H/H	H
Ours	2023	Palmprint	Hand Deep	ProGAN with dropout, SAMTC loss, and DRTS	5,880	H/H/H	H

S/N/R = Similarity/Naturalness/Realism.
H/M/L = High/Medium/Low.
S/M = Single-training-sample mode/Multi-training-sample mode.

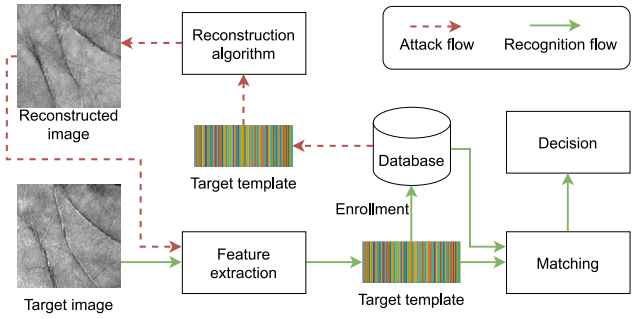


Fig. 1. Pipeline of palmprint template-based reconstruction attack.

The main contributions are summarized as follows.

(1) A versatile black-box template-based reconstruction approach is proposed for deep learning-based and hand-crafted-based palmprint recognition techniques. The resulting reconstructed images possess exceptional quality, effectively fulfilling various evaluation indices, simultaneously encompassing similarity, naturalness, and realism.

(2) Multiple strategies are devised to enhance the performance of the palmprint image reconstruction. Firstly, incorporating dropout into the ProGAN generator and utilizing the proposed DRTS facilitate training the reconstruction network even with limited data availability. Additionally, by introducing a novel loss function, SAMTC loss improves the texture and overall quality of the reconstructed images.

(3) A broad set of experiments and analyses are conducted, wherein we execute reconstruction attacks on diverse palmprint recognition techniques. Based on the findings from the reconstruction attacks, the security and privacy aspects are thoroughly examined on the palmprint recognition algorithms, which can serve as the objective and quantitative measurements of the security and privacy of the recognition method.

The subsequent sections of this paper are structured as follows: Section 2 presents an overview of the relevant prior research. Section 3 delineates the reconstruction methods employed and outlines the metrics utilized for evaluation. Section 4 presents comprehensive experiments on the reconstruction attack and its effectiveness. Lastly, Section 5 encompasses the conclusions drawn from the study and discusses potential avenues for future research.

2. Related works

2.1. Biometrics template-based reconstruction attacks

In biometric systems, each feature extractor has its own extracted unique features. A template-based reconstruction attack is generally tailored to a specific feature extractor. If the system under attack does not consider image quality, the reconstructed images may not closely resemble the target images. Conversely, the biometrics system can be easily deceived if the template extracted from the reconstructed image closely matches the target template. In recent years, several biometrics template-based reconstruction attacks have been proposed. Table 1 displays a list of relevant works on this topic.

Face template-based reconstruction commonly requires a large amount of data for training, such as [1–3], or a model pre-trained with a massive high-quality face dataset, such as [4,5]. Reconstruction attacks using deep templates typically necessitates more training samples, which can be challenging to acquire. Additionally, the attack success rates of [4,5] are unsatisfactory as they rely on pre-trained models. The reconstruction methods for iris [10], fingerprint [6], finger vein and hand vein [7], and palmprint [8,9], are commonly based on hand templates. Hand templates and their target images correlate strongly, making reconstruction methods fairly simple. Extending hand template reconstruction methods to deep templates is challenging due to the highly non-linear correlation between templates and target images, leading to a lack of versatility.

Existing palmprint reconstruction techniques [8,9] have shown limited versatility and are only suitable for specific hand-crafted-based methods. Furthermore, the reconstructed image quality attained by [8] is subpar, whereas [9] necessitates online attacks and falls short of meeting the requirements of a black box environment. On the other hand, Shen et al. proposed a palmprint generation method [12] similar to the reconstruction process, which utilized synthetic palm creases

Table 2
Various palmprint recognition methods.

Ref.	Year	Type	Name	Methodology	Template size and format
[15]	2003	Hand	PalmCode	Gabor filtering	2 × 32 × 32, B
[16]	2004	Hand	CompCode	Neural Gabor filtering with winner -take-all coding in six directions	1 × 32 × 32, I
[17]	2004	Hand	FusionCode	Gabor filtering at four directions, fusion strategy	2 × 32 × 32, B
[18]	2005	Hand	OrdinalCode	Gaussian filtering in 3 groups	3 × 32 × 32, B
[19]	2008	Hand	RLOC	Modified finite Radon transform filtering six directions, competitive coding, pixel-to-area matching	1 × 32 × 32, I
[20]	2009	Hand	BOCV	Gabor filtering at six directions, fusion at score level	6 × 32 × 32, B
[21]	2012	Hand	E-BOCV	Based on [20], fragile bit mask	12 × 32 × 32, B
[22]	2015	Hand	Fast-CC Fast-RLOC	Based on [16] which using two directions only Based on [19] which using one to one matching	1 × 32 × 32, I
[23]	2016	Hand	DoN	3D descriptor for 2D palmprint and ordinal measure	3 × 128 × 128, I
[24]	2016	Hand	DOC	Based on [16], Top-2 competitive codes	2 × 32 × 32, I
[25]	2016	Hand	DRCC	Competitive code and neighbor ordinal feature	1 × 32 × 32, I 1 × 32 × 32, B
[14]	2019	Deep	PalmNet	2-Layer Gabor PCA	15 × 25 × 2^15, R
[26]	2020	Hand	EDM	Optimizing downsampling	6 × 32 × 32, B
[27]	2021	Deep	CompNet	Learnable Gabor network	1 × 512, R
[13]	2022	Deep	DHN	Deep hash network	1 × 128, B
[28]	2022	Hand	MTCC	Multi-order Gabor features	12 × 32 × 32, B
[29]	2022	Deep	SLCN	Extracting direction and edge ordinal measure vectors	2 × 16448, R
[30]	2023	Deep	CO3Net	Coordinate attention and contrastive loss	1 × 2048, R
[31]	2023	Deep	CCNet	Channels competition, multi-order textures	1 × 2048, R

B/I/R = binary/integer/real numbers.
Deep/Hand = Deep-learning-based methods/Hand-crafted-based methods.

to generate realistic palmprint for recognition, but is only effective for one specific type of template. In contrast, our proposed method demonstrates broader applicability across various palmprint recognition algorithms and delivers superior image quality.

2.2. Palmprint recognition

Through extensive research for decades, hand-crafted-based and deep-learning-based palmprint feature extraction techniques have garnered significant recognition, as evidenced by their prominence in Table 2. Deep templates are usually vectors with sizes of at least 128 [13] and can reach 12,288,000 [14]. The large-size templates require enormous storage costs and matching computations. On the other hand, the matching complexity of Hamming distance between binary templates is much lower than that of Euclidean distance between real-number templates. In this paper, we demonstrate the versatility of our method by comparing it to the palmprint recognition methods listed in Table 2.

3. Methodology

In this section, we will first formalize the reconstruction attacks and threat models before comprehensively presenting our reconstruction methods.

3.1. Preliminary

3.1.1. Palmprint recognition and reconstruction attack

Let $\mathcal{E}(\cdot)$ be the feature extractor and $\mathcal{M}(\cdot,\cdot)$ denote the matcher used to measure the similarity score between the two templates. Both of them constitute a palmprint recognition method. Given a palmprint image I, a template T can be obtained through $T = \mathcal{E}(I)$. The T is stored in the database during enrollment as identity representation. For matching, the features extracted from query image I', $T' = \mathcal{E}(I')$ will be compared with T via $\mathcal{M}(\cdot,\cdot)$ to make a decision. Different palmprint recognition algorithms may have distinct $\mathcal{E}(\cdot)$ and $\mathcal{M}(\cdot,\cdot)$, and so do T and T'.

Let $\mathcal{R}(\cdot)$ denote the reconstruction method and a reconstructed image F can be obtained through $\mathcal{R}(T)$. The reconstruction attack deceives recognition systems by achieving high similarity scores in $\mathcal{M}(\mathcal{E}(F),\mathcal{E}(I))$. The higher the similarity score, the better the attack performance.

3.1.2. Threat models

We examine a scenario involving an attacker capable of retrieving a T from a compromised gallery or an intercepted query T'. The T or T' is then utilized to reconstruct the corresponding palmprint image F. The adversarial activity occurs within a black-box framework, where the internal structure of $\mathcal{E}(\cdot)$ and $\mathcal{M}(\cdot,\cdot)$ remain unknown to the attacker. However, the attacker can observe and infer the input–output behavior exhibited by the system.

Given either T or T', we demonstrate the attacker's capability to achieve a notably high success rate in reconstructing F. The F closely approximates the identity under attack. In contrast to previous works [8,9], which predominantly focus on quantifying the success rate of attacks, our work considers the realism and naturalness exhibited by the F.

Moreover, the quality of the F is contingent not only upon the $\mathcal{R}(\cdot)$, which determines the extent of privacy facets explored within T (or

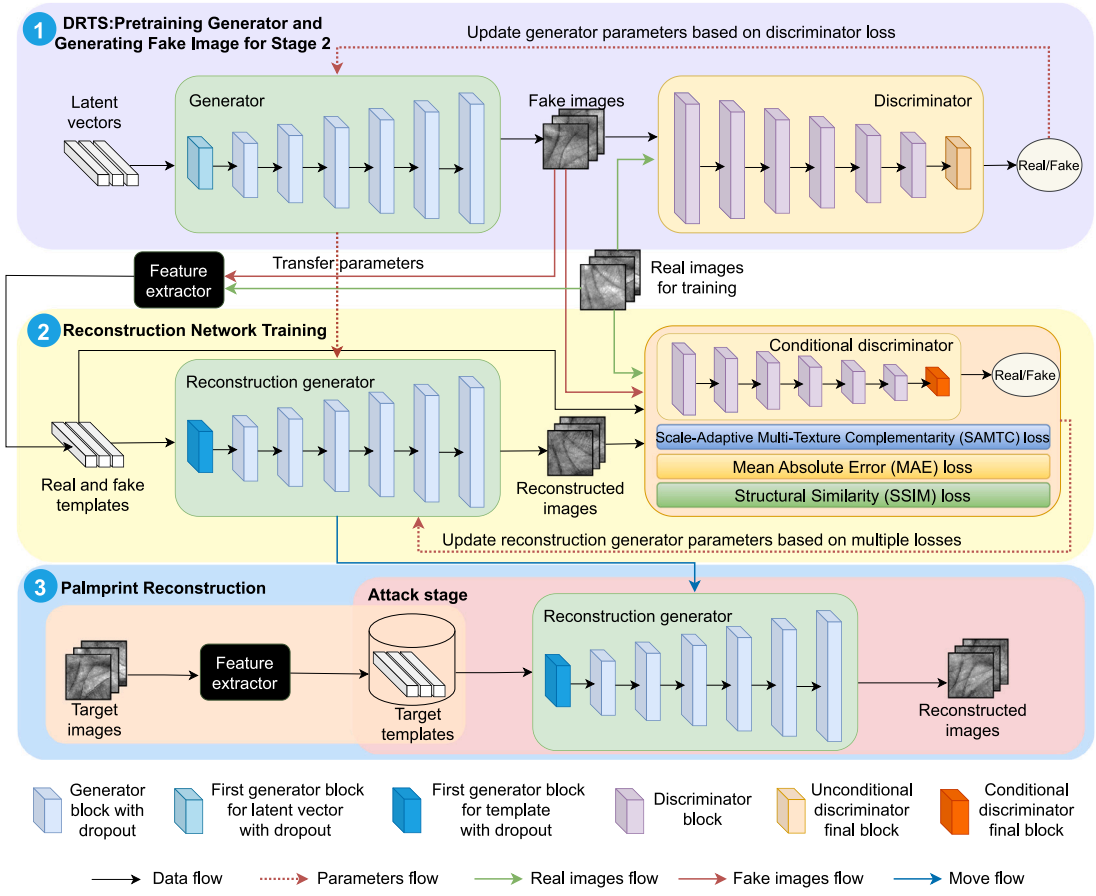


Fig. 2. Pipeline of the proposed palmprint template-based reconstruction method.

T') but also upon the $\mathcal{E}(\cdot)$, which governs the incorporation of privacy into T (or T'). Consequently, the privacy concern within palmprint recognition algorithms predominantly hinges on the behavior of $\mathcal{E}(\cdot)$.

In this work, the same $\mathcal{R}(\cdot)$ with distinct parameters are employed with respect to each different palmprint recognition method. The parameters are acquired through a consistent routine, independent of $\mathcal{E}(\cdot)$ and $\mathcal{M}(\cdot,\cdot)$, thereby rendering $\mathcal{R}(\cdot)$ versatile.

3.2. Overall pipeline of our method

The pipeline of the proposed reconstruction method is illustrated in Fig. 2. The entire procedure can be delineated into three distinct stages. The initial stage encompasses the implementation of DRTS (Section 3.5). Specifically, the ProGAN incorporating DRTS is first trained. Subsequently, the images produced by the DRTS-enabled ProGAN are utilized for data augmentation, aiding in the training process of the reconstruction network $\mathcal{R}(\cdot)$ in stage 2. The parameters obtained from the generator are passed on to initialize $\mathcal{R}(\cdot)$.

The second stage entails training our proposed reconstruction network $\mathcal{R}(\cdot)$, which will be discussed in Section 3.3. The fake images' corresponding templates are derived by inputting the images into a feature extractor, which remains a black box to the adversary. These extracted templates, both fake and real, are then utilized as pairs for training $\mathcal{R}(\cdot)$. In particular, the generator within $\mathcal{R}(\cdot)$ generates reconstructed images. Subsequently, the discriminator loss is computed using the reconstructed and original (or generated) images. Additionally, the three generator losses outlined in Section 3.4 are computed to facilitate updating the generator parameters of $\mathcal{R}(\cdot)$.

The final stage encompasses the palmprint reconstruction process. An adversary may retrieve the template stored in the database or query and feed it into $\mathcal{R}(\cdot)$ to generate the reconstructed palmprint image, enabling impersonation as a genuine user.

3.3. Modified progan for reconstruction

Generative Adversarial Networks (GANs) and their variants are prevalent in biometric template reconstruction due to their proficiency in generating realistic and high-quality data [2–7,10].

ProGAN [11] are adept at mapping complex patterns, making them ideal for reconstructing palmprint templates. They accurately replicate textures, essential for effective attacks, and improve image quality progressively during training. Despite limited data, ProGAN adapts well. To produce target-specific palmprint images, ProGAN must undergo structural changes. Such tweaks ensure the synthetic images match the distribution of real images and maintain relevance and likeness to the target, involving use of template vectors as inputs and a projection conditional discriminator [32].

Furthermore, using an overparameterized generator can result in overfitting when training data is scarce, whereby the generator may generate high-quality images during training, and the performance deteriorates during testing. While batch normalization offers some mitigation against overfitting in the generator, its efficacy is limited. Consequently, we have incorporated dropout [33] for the first time to augment the image quality generated by the generator. In addition, this empowers the generator to prioritize the pertinent template information about the target image.

In image reconstruction, 2D dropout outperforms 1D dropout, as it relies on channel rather than pixel information. While 1D dropout targets individual pixels randomly, 2D dropout suspends entire channels with a set probability, allowing a more diversified channel contribution and resulting in higher target image fidelity. Yet, understanding the correct use of dropout is vital in the reconstruction process. Too little can render it ineffective, excessively can lead to blurry images. Furthermore, excessively small or large dropout probabilities can detrimentally

Table 3
Modified reconstruction network architecture and configuration.

Block	Layer	Configuration
Initial Generator Block	Transpose Conv	InTS, Out512, k4s1p0, BN, LR0.2
	Conv	In512, Out512, k4s1p1, BN, LR0.2
	2D Dropout	Probability = 0.2
Standard Generator Block	Interpolate	Factor = 2
	Conv	In512, Out512, k3s1p1, BN, LR0.2
	2D Dropout	Probability = 0.2
	Conv	In512, Out512, k3s1p1, BN, LR0.2
Standard Discriminator Block	Conv	In512, Out512, k3s1p1, LR0.2
	Conv	In512, Out512, k3s1p1, LR0.2
	Average Pool	k3s2p0
Final Conditional Discriminator Block	Mini-batch [34]	Batch = 4
	Conv1	In513, Out512, k3s1p1, LR0.2
	Conv2	In512, OutFL, k4s1p0, LR0.2
	Conv3	InTS, Out1, k1s1p0
	Projection [32]	–

Conv = Convolution layer.
In/Out = Number of input/output channels.
k/s/p = Size of Conv kernel/stride/padding.
BN/LR = Batch normalization/Leaky ReLU.
TS = Template size.

affect the effectiveness or convergence speed. Therefore, to achieve optimal outcomes, it is recommended to apply dropout to the generator at the initial block end and within the middle of the standard block, with a dropout probability of 0.2.

Our modified network structure and configuration are detailed in Table 3. In addition, the RGB layer is used to convert images and channels in the generator's last layer and the discriminator's first layer.

3.4. Palmprint reconstruction losses

Our proposed model comprises four losses: RaLS loss, SAMTC loss, MAE Loss, and SSIM Loss. The RaLS loss is the adversarial loss for our modified ProGAN, while the SAMTC, MAE, and SSIM losses are designed to restore image texture, ensure pixel accuracy, and uphold structural integrity, respectively. Each of these losses will be explained in further detail below.

3.4.1. Relativistic average least square loss for adversarial learning

For reliable adversarial training in reconstruction tasks, we adopt the stable and effective Relativistic average Least Square (RaLS) loss [35]. which can also accurately evaluates the reconstructed image's realism. The discriminator loss and the generator loss of RaLS loss are defined as $\mathcal{L}_D$ and $\mathcal{L}_G$, respectively.

3.4.2. SAMTC loss for texture reconstruction

Palmprint recognition methods rely on palmprint textures to achieve favorable outcomes in matching performance. Achieving proficient reconstruction of palmprint images necessitates emphasizing high-caliber texture quality. To address this concern, we introduce Scale-Adaptive Multi-Texture Complementarity (SAMTC) loss, guaranteeing satisfactory texture quality in the reconstructed palmprint images. The SAMTC loss leverages the texture disparity between the reconstructed and target images to improve texture information restoration.

To capture the maximum amount of palmprint texture information without resorting to complex operations, we employ Gabor filters to convolve the image in six directions, followed by a second round of convolution. The first round of filtering extracts first-order texture features, while the second round extracts second-order texture features, generating 12 texture response maps with complementary characteristics.

Subsequently, we employ the mean absolute error (MAE) to quantify the disparities among the 12 texture response maps generated from the reconstructed and target images. The MAE values for each response map are calculated, and the average of these 12 differences is obtained, serving as the multi-texture complementary loss. Additionally, we apply instance normalization to each response map to mitigate numerical attenuation arising from the filtering process.

In the ProGAN generator, the resolution of the generated image varies across different training stages. To effectively utilize the textures presented in images of varying resolutions, it is imperative to dynamically adjust the size of the convolution kernel to correspond with the image scale. In other words, the convolution kernel needs to be scale-adaptive, ensuring optimal texture extraction and synthesis. Let n be the shorter side length of an image; the convolution kernel size is given as $2rd + 1$ where $rd = \lfloor n/6 \rfloor$ is the kernel radius according to the Gabor kernel size in 128×128 images and $\lfloor\ \rfloor$ is a flooring function. A scale-adaptive convolution kernel can adjust and accommodate the texture feature loss across varying image resolutions.

The SAMTC loss is defined as follows:

$$(tf_{r|f})_i^1 = \varphi(x_{r|f}, g_i) = IN(Conv(x_{r|f}, g_i)) \tag{1}$$

$$(tf_{r|f})_i^2 = \varphi((tf_{r|f})_i^1, g_i) \tag{2}$$

$$\mathcal{L}_{SAMTC} = \frac{\sum_{n=1}^{2}\sum_{i=1}^{6}\mathcal{L}_{MAE}((tf_r)_i^n, (tf_f)_i^n)}{12} \tag{3}$$

where $Conv$ is the convolution operation, $r|f$ denotes the real or fake, g_i denotes the Gabor convolution kernel at ith direction, $i = [1, 2, 3, 4, 5, 6]$ corresponds to 0, 30, 60, 90, 120, and 150-degree directions, respectively. IN is instance normalization, φ is texture feature extractor, and $(tf)_i^n$ denotes the texture feature of the image filtered with the ith convolutional kernel for nth time.

Given that images with a resolution below 16×16 contain limited significant texture feature information, the SAMTC loss is only applied when the image resolution is equal to or exceeds 16×16. This ensures that the SAMTC loss is activated solely when sufficient texture feature information is available to enhance the reconstruction process.

3.4.3. MAE loss for pixel reconstruction

Mean Absolute Error (MAE) loss is commonly used for pixel reconstruction in GAN-based models due to its sensitivity to pixel differences, robustness to outliers, stable gradients, and inherent L1 regularization effect. In addition, it captures fine details, preserves high-frequency information, and produces sharp and clean reconstructions. The MAE loss is defined as $\mathcal{L}_{MAE}$.

3.4.4. SSIM loss for structure reconstruction

Structural Similarity (SSIM) is a perceptual metric that considers structural information and luminance similarity and measures the similarity between two images based on luminance (brightness), contrast, and structural similarity. By considering these factors, SSIM provides a more perceptually meaningful evaluation of image similarity compared with pixel-wise metrics. The range of SSIM is $[0, 1]$, and the more similar the two images are, the higher the score is.

When SSIM is leveraged as a loss in reconstruction network training, it encourages the generator to produce images with similar pixel values and exhibit similar structural patterns and visual quality as the real images. The SSIM loss used in this work is:

$$\mathcal{L}_{SSIM} = 1 - SSIM(x_f, x_r) \tag{4}$$

3.4.5. Total loss

To sum up, the total reconstruction generator loss is given as:

$$\mathcal{L}_{Rec} = \mathcal{L}_G + \lambda_{SAMTC}\mathcal{L}_{SAMTC} + \lambda_{MAE}\mathcal{L}_{MAE} + \lambda_{SSIM}\mathcal{L}_{SSIM} \tag{5}$$

where λ_{SAMTC}, λ_{MAE} and λ_{SSIM} denote the weights of SAMTC, MAE, and SSIM losses, respectively.

Table 4
Four scenarios for reconstruction attacks.

	Single-Sample	Cross-Sample
Single-Algorithm	S1	S2
Cross-Algorithm	S3	S4

3.5. Double reuse training strategy

Deep learning models require extensive data to learn complex image-feature relationships, but data scarcity and overfitting are challenges. The Double Reuse Training Strategy (DRTS) employs Data Reuse Training Strategy (DRTS-D) and Parameter Reuse Training Strategy (DRTS-P) to overcome these issues. DRTS utilizes a modified ProGAN—DRTS-GAN—which replaces certain generator and discriminator blocks to initially create an unconditional GAN that generates synthetic images for DRTS-D and transfers parameters for DRTS-P.

DRTS-D harnesses the training data to train the DRTS-GAN, which generates synthetic images, supplementing the training dataset. This strategy leverages the inherent information within the training data, enhancing the overall reconstruction efficacy. Including these supplementary samples effectively mitigates the limitations imposed by the scarcity of training data, leading to enhanced model generalization. It is worth noting that a clear distinction arises between the distributions of real and synthetic training samples. Specifically, only the genuine training samples are employed for meticulous fine-tuning during the final epochs of the reconstructed network training process.

DRTS-P reuses parameters from the DRTS-GAN generator in the reconstruction network to harness pre-trained knowledge, providing a better starting point for training. This reduces the time and computational resources needed. It is effective as both image generation and reconstruction share goals: producing images that fit the real image distribution. The commonality justifies using generator parameters to initialize the reconstruction network.

3.6. Evaluation metrics

This subsection describes the evaluation metrics used for assessing the performance of our proposed palmprint template-based reconstruction model. Specifically, it focuses on two key metrics: the attack success rate and the quality of the reconstructed images.

3.6.1. Attack success rate

Attack success rate (ASR) is defined as:

$$ASR = \frac{1}{N}\sum_{n=1}^{N}\{s_n > \delta\} \tag{6}$$

where N denotes the total number of reconstructed images, s_n is the matching similarity score of the nth reconstructed image, and δ is the threshold. Only one reconstructed image is generated for each target template. The threshold is set according to False Acceptance Rate (FAR). $FAR = 0.1\%$, $FAR = 0.01\%$, and $FAR = 0\%$ are for low-, medium-, and high-security scenarios.

Table 4 tabulates the four distinct attack scenarios employed in reconstruction attacks, as outlined in [36]. The Single-Sample scenario denotes matching the reconstructed image's template with the target templates. The Cross-Sample scenario involves matching the reconstructed image's template with the target user's other templates where the target template is excluded. A Single-Algorithm scenario signifies a situation where the system for obtaining the reconstructed image's template and the attacked system share the same recognition algorithm. Lastly, the Cross-Algorithm scenario indicates that different recognition algorithms are applied to obtain a template and the system is attacked. Scenarios S1 to S4 represent the four reconstruction attack scenarios categorized based on their difficulty levels, ranging from easy to challenging.

3.6.2. Algorithmic security and template privacy

Our investigation revealed that including the four attack scenarios enables a comprehensive assessment of security and privacy considerations, while previous studies [1–7,10] failed to analyze their implications for recognition algorithms. Our approach involves a thorough analysis of the four scenarios from the perspective of recognition algorithms, leading to conclusions regarding the Algorithmic Security (AS) and Template Privacy (TP) of these algorithms.

AS concerns the vulnerability of an algorithm to attacks and is evaluated through scenarios S1 and S3. S1 and S3, representing Single-Sample scenarios, pose a more significant threat to the algorithm than S2 and S4. Low AS indicates a higher susceptibility to successful attacks, implying that the algorithm lacks robust security compared to others. TP refers to the extent to which a template contains limited information exploitable in reconstruction attacks and is assessed through scenarios S2 and S4. S2 and S4, being Cross-Sample scenarios, better represent the template's availability than S1 and S3. Low TP implies the potential leakage of more information, resulting in more severe privacy issues associated with the algorithm's templates than others.

The analysis methods for AS and TP are not limited to specific reconstruction attack methods or recognition algorithms. They can be applied to general biometric methods capable of performing template-based reconstruction attacks. A series of anchor recognition algorithms are selected to analyze a target recognition algorithm, and the target is also included in the anchor. A reconstruction method is then employed to execute all four attack scenarios on the anchor and target algorithms. The AS of the target is quantified by the mean Attack Success Rate (mASR) of the anchor's reconstructed palmprints attacking the target algorithm. Similarly, the TP of the target is determined by the mASR of the target's reconstructed palmprints attacking the anchor algorithms. A higher mASR indicates lower AS or TP.

The results of AS and TP may vary significantly based on the choice of anchor algorithms and the reconstruction method employed. A larger number and greater diversity of chosen anchor algorithms, along with enhanced performance of the reconstruction methods, contribute to more reliable AS and TP assessments. This analytical approach evaluates AS and TP in potential recognition algorithms, aiding in the selection process according to the need for high AS or high TP.

3.6.3. Image quality evaluation

The quality of the reconstructed image serves as a crucial indicator in the assessment of reconstruction attacks. A proficient reconstruction attack should adhere to similarity, naturalness, and realism criteria. Similarity evaluates the degree of resemblance between the reconstructed image and the target image within the image domain. Naturalness measures the fidelity of the reconstructed image. Specifically, the level of distortion introduced. Realism assesses the distribution difference between the reconstructed and target image, determining its believability.

This paper evaluates image quality for similarity, including SSIM, MS-SSIM (Multi-Scale SSIM), and PSNR (Peak Signal-to-Noise Ratio). Furthermore, for assessing naturalness, BRISQUE (Blind/Referenceless Image Spatial Quality Evaluator), PIQE (Perceptual Image Quality Evaluator), and CaHDC (Cascaded CNN with Hierarchical Degradation Concatenation) are employed. Finally, to measure the realism of the synthesized images, the metrics MMD (Kernel Maximum Mean Discrepancy), FID (Fréchet Inception Distance), and MS (Mode Score) are utilized.

4. Experiments

The experimental environment is as follows. Intel (R) Xeon (R) Platinum 8222CL CPU @3.00 GHz, 64 GB internal storage, NVIDIA 3090Ti GPU, Ubuntu 20.04.3 LTS 64 bit operating system, Python 3.7 Interpreter, Pytorch 1.8.0 and Torchvision 0.9.0 API. Our model takes approximately one day of training with a single GPU, where the precise time cost is contingent upon the training data's scale. The

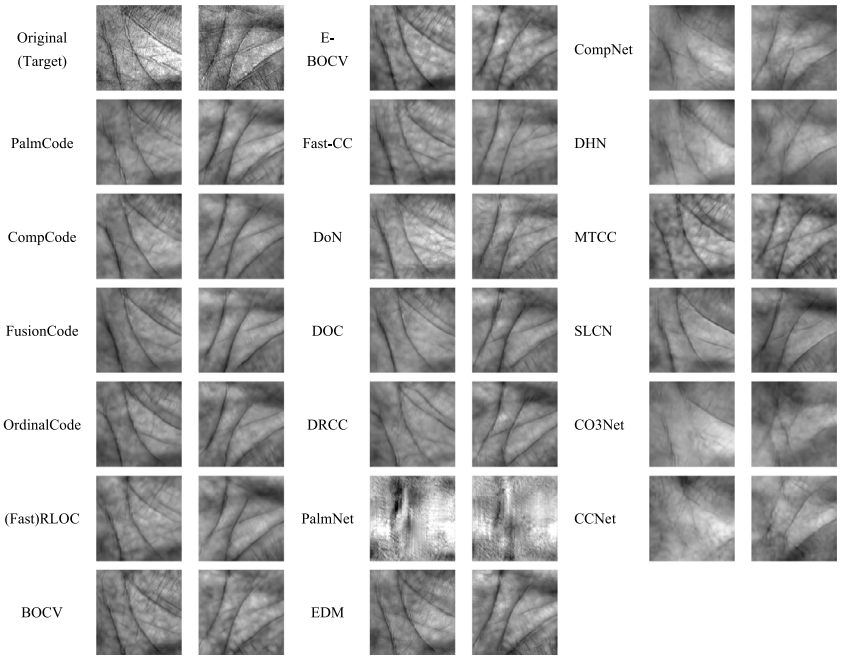


Fig. 3. Reconstructed palmprint images from target templates.

reconstruction model exclusively generates five reconstructed images per second in the inference stage through CPU processing.

The threshold δ in Eq. (6) at a specific False Acceptance Rate (FAR) is determined based on the testing sets. All templates are converted into vectors to serve as inputs for the reconstruction network. During the training of the reconstruction network, the image resolutions of [4, 8, 16, 32, 64, 128] are incrementally generated in six stages. The batch sizes for the stages are set as [256, 128, 64, 32, 16, 8], and the training process for each stage consists of 50 epochs. The weights assigned to the objective functions of the reconstruction, namely λ_{SAMTC}, λ_{MAE} and λ_{SSIM}, are set to 100, 100, and 10, respectively, reflecting their respective importance in the reconstruction process.

The DRTS involves the utilization of training samples and generators. DRTS-D employs approximately four times the training dataset, resulting in 20,000 generated samples used for data augmentation. To mitigate the influence of generated samples on real samples, the last 20 epochs of the final stage do not involve training with generated samples. Instead, the network is fine-tuned exclusively using real training samples.

Given the large template size in DoN [23] and PalmNet [14], only a $1 \times 128 \times 128$ template is used in our experiment for DoN and principal component analysis is employed to reduce the template size from 12,288,000 to 24,000 for PalmNet. Our experiments are carried out under the same-dataset and cross-dataset reconstruction attack protocol.

4.1. Same-dataset reconstruction attack

Under the same-dataset reconstruction attack protocol, we adopt the PolyU palmprint dataset [15], which comprises 7,752 samples from 386 palms, averaging around 20 samples per palm. 80% of the samples are allocated to training for experimentation, while the remaining 20% are reserved for testing. The training and testing sets are mutually exclusive, ensuring they do not share the same palms throughout our experimentation.

4.1.1. Single-algorithm scenario

Table 5 illustrates the results of single-algorithm attacks conducted in Scenarios S1 and S2. It is observed that most recognition algorithms achieve a perfect $ASR = 100\%$, even in the strictest case of S1 (@ $FAR = 0\%$). On the other hand, the highest ASR obtained is 99.55% for S2 @ $FAR = 0\%$. All hand-crafted-based methods can be successfully attacked in Scenario S1. Our proposed method demonstrates a notably high ASR for recognition algorithms that employ filtering features in Scenario S2, such as PalmCode, OrdinalCode, BOCV, E-BOCV, EDM, and MTCC. However, our method exhibits relatively lower ASRs for the recognition algorithms that additionally encode the filtering features, such as CompCode, FusionCode, RLOC, DOC, and DRCC. Despite the notable accuracy achieved by CCNet, our method achieves $ASR = 98.75\%$ in S1 @ $FAR = 0.1\%$. Even at a more stringent $FAR = 0\%$, the ASR only decreases to 72.5%.

Our method exhibits a significant ASR, even considering hashing methods like DHN, indicating that DHN is partially reversible. However, SLCN appears utterly immune to our reconstruction attack, which will be further examined in Section 4.4. The relatively low ASR for PalmNet can be attributed to substantial information loss caused by dimensionality reduction.

Table 5
ASR (%) in scenarios S1 and S2.

Scenario	S1			S2		
FAR	0.1%	0.01%	0%	0.1%	0.01%	0%
PalmCode [15]	100	100	100	98.61	97.03	89.19
CompCode [16]	100	100	100	92.78	85.50	66.42
FusionCode [17]	100	100	100	95.54	91.07	78.40
OrdinalCode [18]	100	100	100	98.83	96.84	89.06
RLOC [19]	100	100	100	96.61	90.51	61.22
BOCV [20]	100	100	100	99.96	99.87	99.54
E-BOCV [21]	100	100	100	99.96	99.89	99.55
Fast-CC [22]	100	100	100	98.38	95.95	88.79
Fast-RLOC [22]	100	100	100	97.09	92.02	75.06
DoN [23]	100	100	100	99.73	99.55	99.12
DOC [24]	100	100	100	98.23	95.47	83.65
DRCC [25]	100	100	100	95.03	88.30	62.86
PalmNet [14]	0.12	0.12	0.06	0.15	0.11	0.07
EDM [26]	100	100	100	99.12	98.20	95.42
CompNet [27]	100	98.75	84.40	97.65	91.74	63.12
DHN [13]	100	99.82	89.58	91.74	84.66	56.59
MTCC [28]	100	100	100	99.92	99.83	99.30
SLCN [29]	0	0	0	0	0	0
CO3Net [30]	99.58	98.33	77.02	98.75	95.52	66.01
CCNet [31]	98.75	94.40	72.50	96.12	88.36	58.27

Table 6
Reconstructed image quality evaluation.

Template type	Similarity↑			Naturalness			Realism		
	SSIM	PSNR	MS-SSIM	BRISQUE↓	PIQE↓	CaHDC↑	MMD↓	FID↓	MS↑
Original	0.23	17.93	0.62	37.89	47.99	40.95	–	–	1.324
PalmCode	0.29	18.64	0.60	44.33	62.53	27.27	0.224	0.091	1.219
CompCode	0.27	17.45	0.53	43.19	59.60	27.41	0.225	0.101	1.206
FusionCode	0.30	18.09	0.58	46.13	62.13	27.73	0.227	0.097	1.198
OrdinalCode	0.31	18.81	0.67	41.51	61.40	28.07	0.243	0.098	1.191
(Fast)RLOC	0.28	17.99	0.58	39.68	58.61	30.47	0.226	0.109	1.209
BOCV	0.35	19.18	0.73	43.47	43.30	32.33	0.224	0.079	1.197
E-BOCV	0.35	19.28	0.73	42.18	40.85	33.88	0.220	0.078	1.204
Fast-CC	0.29	17.74	0.57	47.10	64.24	24.96	0.426	0.137	1.089
DoN	0.33	18.17	0.61	42.48	29.36	37.50	0.374	0.104	1.151
DOC	0.29	18.09	0.61	41.87	51.95	31.61	0.222	0.090	1.216
DRCC	0.28	17.99	0.58	41.90	58.47	30.95	0.228	0.105	1.206
PalmNet	0.12	12.55	0.18	35.79	33.19	36.60	0.368	0.258	1.165
EDM	0.32	19.24	0.71	31.01	19.95	37.03	0.154	0.064	1.269
CompNet	0.22	17.41	0.45	40.72	63.91	22.06	0.195	0.100	1.249
DHN	0.23	17.98	0.48	42.10	70.01	20.34	0.212	0.105	1.219
MTCC	0.36	19.40	0.74	45.44	50.45	30.43	0.238	0.078	1.191
SLCN	0.26	19.03	0.58	36.91	60.97	26.76	0.213	0.109	1.233
CO3Net	0.22	17.46	0.45	41.58	64.24	20.01	0.406	0.191	1.064
CCNet	0.22	17.25	0.43	39.89	60.98	21.76	0.374	0.104	1.151

Comparing the ASRs in S1 and S2, deep-learning-based methods demonstrate greater resistance to reconstruction attacks than hand-crafted-based methods. Nonetheless, our method effectively performs reconstruction attacks on various algorithms.

Fig. 3 presents the reconstructed palmprint images. While the principal lines in the reconstructed images are discernible and exhibit similarity, there are noticeable variations in details and textures. These differences arise due to the distinct information contained within the individual templates. Hence, our method is not constrained to a specific template but can be applied to diverse templates extracted from numerous feature extractors. However, the reconstructed images of PalmNet yield limited valuable information, primarily due to the dimensionality reduction process that results in the loss of discriminative information. Given that both Fast-RLOC and RLOC utilize the same extractor, their templates are identical, resulting in indistinguishable reconstructed images from both methods.

Table 6 presents the evaluation of image quality. The "Original" column refers to the original palmprint image, and its similarity is assessed by comparing it with genuine palmprint images. The symbols ↑ and ↓ indicate that higher or lower values, respectively, correspond to better attack performance.

Regarding similarity, MTCC exhibits the highest quality, while CC-Net demonstrates the lowest quality. These results align with those obtained for ASR (except SLCN). Most reconstructed images display similarity levels comparable to, or even higher than, genuine images. In terms of naturalness, the reconstructed images exhibit slightly lower naturalness compared to the original images, but the difference is relatively small. Finally, for realism, all reconstructed images have lower realness values than real images, as expected, but they remain within an acceptable range.

It is worth noting that the quality of fake palmprint images reconstructed from different templates varies across the evaluated indices. However, our method can simultaneously satisfy these indices, ensuring a balanced performance in terms of image quality.

4.1.2. Cross-algorithm scenario

Tables 7 and 8 illustrate the results of cross-algorithm attacks conducted in Scenarios S3 and S4. Four hand-crafted-based methods can be categorized into BOCV and MTCC, based on filtering features, while RLOC and DRCC encode the filtering features further. The remaining are three deep-learning-based methods.

In both tables, Column 1 indicates the templates for reconstructing the fake images, while Row 1 represents the targeted recognition algorithms that are attacked or deceived. For instance, in Table 7, the ASR of reconstructing from DRCC templates and targeting the CompNet is 85.48%.

Table 7
ASR (%) in S3 @ $FAR = 0.01\%$. The underlined are S1 results.

	RLOC	BOCV	DRCC	MTCC	DHN	CompNet	SLCN
RLOC	100	100	100	100	26.79	79.76	0
BOCV	100	100	100	100	80.00	100	2.02
DRCC	100	100	100	100	27.56	85.48	0
MTCC	100	100	100	100	84.82	100	1.96
DHN	25.65	25.83	21.49	18.93	99.82	28.81	0
CompNet	27.38	28.63	24.05	22.08	36.49	98.75	0
SLCN	90.36	89.35	81.67	84.11	63.27	58.75	0

Table 8
ASR (%) in S4 @ $FAR = 0.01\%$. The underlined are S2 results.

	RLOC	BOCV	DRCC	MTCC	DHN	CompNet	SLCN
RLOC	90.51	96.83	85.95	96.45	20.89	68.32	0
BOCV	98.79	99.87	98.22	99.82	65.96	99.26	0.21
DRCC	91.46	97.53	88.30	97.21	21.28	74.01	0
MTCC	98.86	99.87	98.22	99.83	70.40	99.37	0.20
DHN	19.87	22.33	17.69	16.77	84.66	24.91	0
CompNet	19.35	21.82	17.31	16.79	27.76	91.74	0
SLCN	62.17	65.55	51.58	57.31	47.82	47.29	0

Generally, the reconstructed images obtained from BOCV and MTCC templates exhibit the highest cross-algorithm ASR, followed by RLOC, DRCC, and SLCN; DHN and CompNet demonstrate the lowest ASR. This trend can be attributed to the relative susceptibility of RLOC, DRCC, BOCV, and MTCC to cross-algorithm attacks, the moderate vulnerability of DHN and CompNet, and the robustness of SLCN, which proves to be the most challenging to attack.

Fig. 4 depicts the attack-matching distributions, specifically the distributions of matching scores for the reconstructed images in S3 and S1. For example, Fig. 4(f) depicts the matching distributions of the fake images reconstructed from different templates to launch an attack on the CompNet. In most cases, the attack-matching distributions fall between the genuine and imposter distributions.

The matching similarities derived from BOCV and MTCC templates exhibit high values, whereas those originating from DHN and Comp-Net templates yield low values. Notably, the distribution shown in Fig. 4(g) is distinct, where most attack-matching similarities are lower than those of the imposters. While the fake images reconstructed from

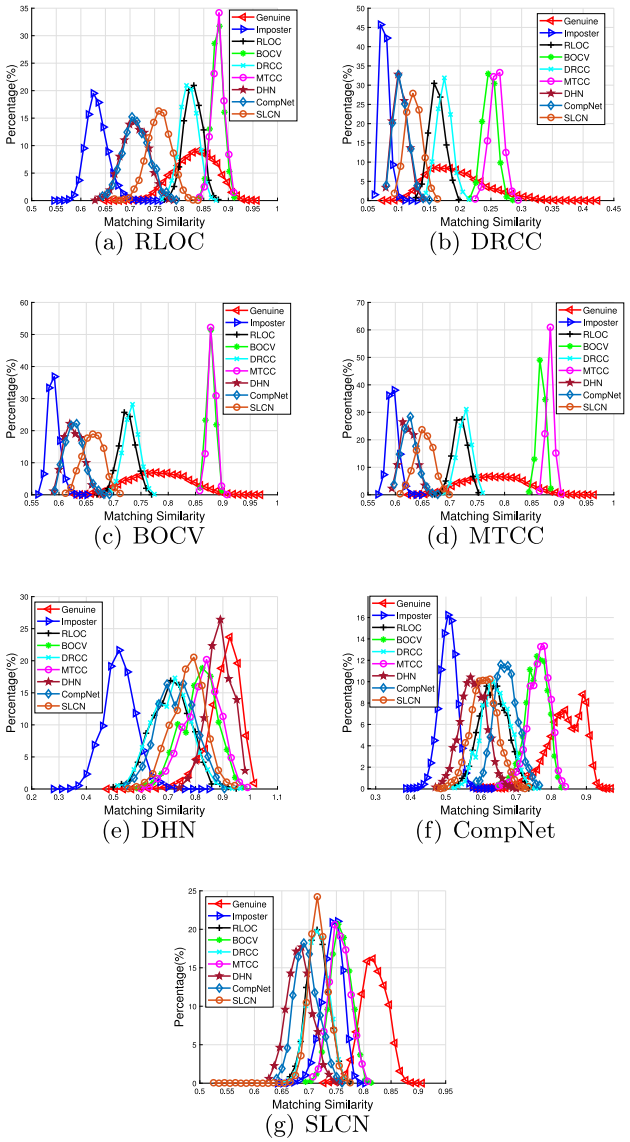


Fig. 4. Matching similarity distribution in scenario S3.

SLCN templates can successfully attack other algorithms, SLCN remains immune to any reconstructed images. Our method achieves a high cross-algorithm ASR for most palmprint recognition algorithms, even in S3 (and S4) @ $FAR = 0.01\%$.

4.2. Cross-dataset reconstruction attack

In this evaluation, we incorporate two additional contactless palmprint datasets: IITD [37] and Tongji [38]. The IITD dataset encompasses 2,601 samples collected from 460 palms, averaging around five samples per palm. In contrast, the Tongji dataset consists of 12,000 samples obtained from 600 palms, with an average of approximately 20 samples per palm. In this evaluation, 20,000 generated samples are also employed in the DRTS to ensure comparable results for IITD, Tongji and PolyU datasets.

Notably, the cross-dataset protocol involves training and testing data derived from distinct datasets, allowing us to assess the generalization capability of our model in a more challenging scenario. For all cross-dataset experiments, we utilize MTCC [28], an advanced recognition algorithm, to further scrutinize the performance of our method in the presence of varied datasets and recognition algorithms.

Table 9
ASR (%) of IITD and Tongji in scenarios S1 and S2.

Dataset	Algorithm	S1(FAR=)			S2(FAR=)		
		0.1%	0.01%	0%	0.1%	0.01%	0%
IITD	MTCC	100	100	100	96.67	95.36	93.89
	CCNet	99.05	94.86	75.43	94.33	85.00	65.04
Tongji	MTCC	100	100	100	99.12	98.64	97.60
	CCNet	98.71	93.08	44.17	86.80	71.83	22.88

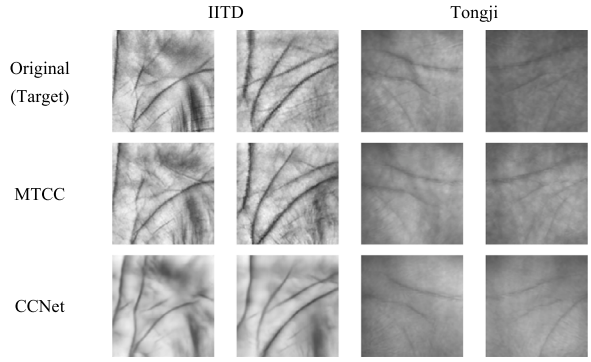


Fig. 5. Reconstructed palmprint images from target templates in IITD and Tongji.

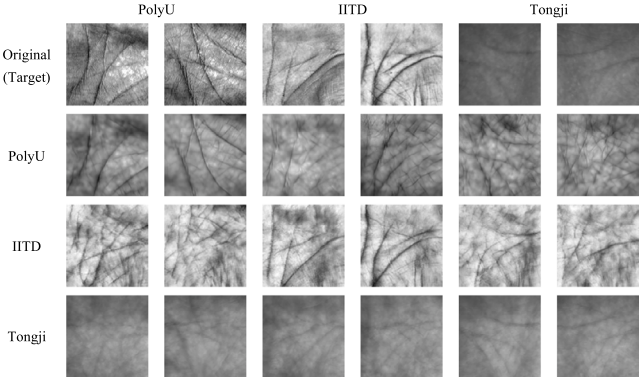


Fig. 6. Reconstructed palmprint images from cross-dataset on MTCC template.

Before initiating the cross-dataset experiment, we assess the performance of our method using hand-crafted-based MTCC and the deep-learning-based CCNet [31]. Table 9 demonstrates that our proposed method maintains a notable ASR even within contactless palmprint datasets. Moreover, the evaluation of image visual quality and results presented in Table 10 and Fig. 5, respectively, indicate our method's satisfactory performance in these scenarios.

The cross-dataset attack performance is detailed in Table 11, where the ASR remains at 100% in Scenario S1 and exceeds 92% in Scenario S2. Notably, the ASR differences across these cross-dataset scenarios are negligible, irrespective of the dataset on which the model was trained or tested. This suggests that our model has effectively learned essential information for reconstructing palmprints from templates. The results underscore the capability of our method to achieve satisfactory attack performance even when the reconstruction model encounters a target image style it has not seen before.

Fig. 6 displays the reconstructed images from the cross-dataset, while their evaluation is summarized in Table 12. Notably, the three palmprint datasets exhibit significant differences in appearance and style, as evident in the first row of Fig. 6. Given that our method primarily emphasizes attack performance and the templates contain minimal appearance information, the reconstructed palmprints from the cross-dataset exhibit lower visual quality. Furthermore, the model's training data influences these palmprints' appearance.

Table 10
Reconstructed contactless palmprint image quality evaluation.

Dataset	Template type	Similarity↑			Naturalness			Realism		
		SSIM	PSNR	MS-SSIM	BRISQUE↓	PIQE↓	CaHDC↑	MMD↓	FID↓	MS↑
IITD	Original	0.31	18.34	0.50	32.79	22.73	32.92	–	–	1.283
	MTCC	0.53	20.47	0.78	30.96	11.57	33.95	0.286	0.044	1.231
	CCNet	0.35	17.26	0.65	48.72	75.63	29.07	0.376	0.100	1.164
Tongji	Original	0.81	24.35	0.85	33.80	25.94	38.09	–	–	1.290
	MTCC	0.82	21.98	0.87	31.34	21.66	39.09	0.200	0.063	1.259
	CCNet	0.77	21.51	0.76	28.58	23.69	38.93	0.301	0.060	1.196

Table 11
ASR (%) on MTCC of cross-dataset in scenarios S1 and S2.

Dataset		S1(FAR=)			S2(FAR=)		
Training	Testing	0.1%	0.01%	0%	0.1%	0.01%	0%
PolyU	IITD	100	100	100	95.71	93.81	92.94
	Tongji	100	100	100	98.63	97.98	96.29
IITD	PolyU	100	100	100	99.84	99.67	98.71
	Tongji	100	100	100	98.55	97.76	95.85
Tongji	PolyU	100	100	100	99.92	99.77	99.02
	IITD	100	100	100	95.95	94.17	92.74

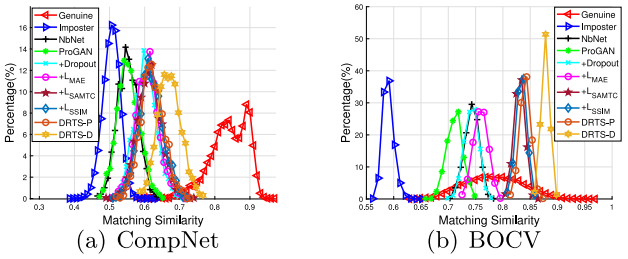


Fig. 7. Ablation experiments of matching similarity distributions in scenario S1.

4.3. Ablation study

In this section, we present the impact of each component in our proposed model, as depicted in Table 13. The ProGAN serves as the basic model, and the symbol "+" indicates adding an extra module to the basic model step by step. We evaluate the performance using two distinct feature extractors: BOCV, a representative hand-crafted-based method, and CompNet, a representative deep-learning-based method. The baseline model used for comparison is NbNet [1] which is widely used for comparison in reconstruction attack work.

Table 13 and Fig. 7 show that our proposed model effectively enhances the ASR and image similarity. Notably, the inclusion of dropouts significantly positively impacts improving ASR. Additionally, both $\mathcal{L}_{SAMTC}$ and DRTS contribute significantly to enhancing both ASR and image similarity. Our method outperforms NbNet and achieves a remarkable $ASR = 100\%$ attack rate for CompNet. However, successfully attacking CompNet @ $FAR = 0.1\%$ in S1 proves challenging. Furthermore, Fig. 8 visually demonstrates that each module implemented in our proposed model enhances the visual quality of the generated images.

4.4. Security and privacy

Table 14 provides an analysis and summary of Algorithmic Security (AS) and Template Privacy (TP). The AS is evaluated by mean ASR (mASR) for each algorithm targeted by the fake images reconstructed from different templates, represented by the column averages in Table 7. TP is assessed by calculating the mASR for each algorithm, in which the fake images are reconstructed from its templates and used to attack different algorithms, represented by the row averages in Table 8.

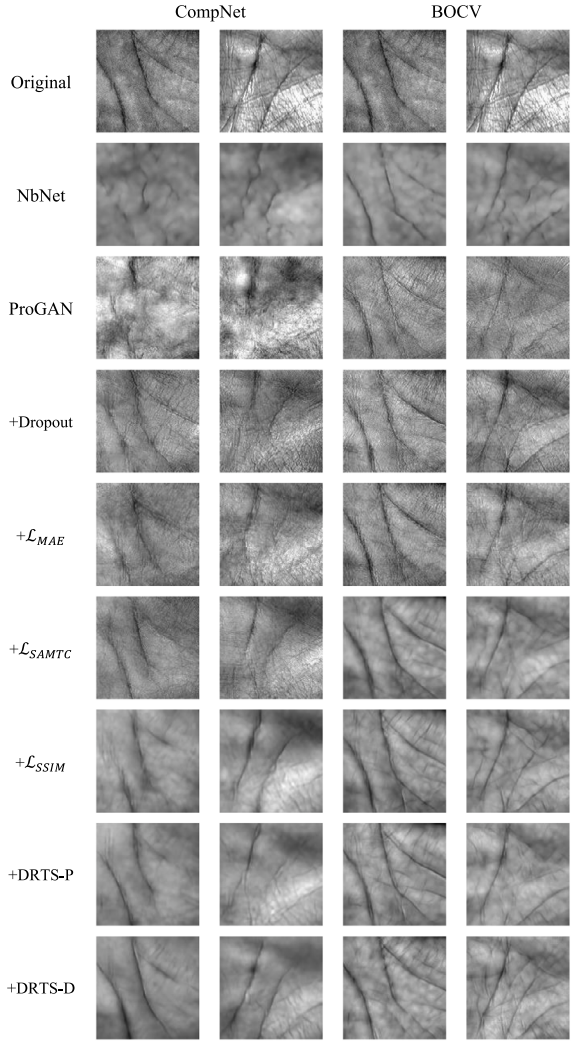


Fig. 8. Illustration of reconstructed palmprint images.

The levels of H (high), M (medium), and L (low) are distinguished based on the mASR. Specifically, H, M, and L levels are defined at $mASR < 30\%$, $30\% \leq mASR \leq 70\%$, and $mASR > 70\%$, respectively. The lower the mASR is, the higher the AR and TP are.

For AS, the SLCN demonstrates a high level of immunity against reconstruction attacks from different templates. This is due to its utilization of the differences between filtering features in various directions instead of relying on specific filtering features. As a result, SLCN is highly sensitive to even minor changes, making it challenging for the network to reconstruct the distinctive features used by SLCN accurately. On the other hand, DHN, a deep-learning-based method, exhibits a moderate AS because it considers more comprehensive information and is less susceptible to being misled by certain details.

Table 12
Reconstructed image quality evaluation on MTCC of cross-dataset.

Dataset		Similarity↑			Naturalness			Realism		
Training	Testing	SSIM	PSNR	MS-SSIM	BRISQUE↓	PIQE↓	CaHDC↑	MMD↓	FID↓	MS↑
PolyU	IITD	0.50	13.85	0.65	45.80	46.64	26.76	0.573	0.123	0.957
	Tongji	0.61	18.57	0.61	45.49	42.96	29.52	0.661	0.211	0.761
IITD	PolyU	0.29	13.68	0.57	31.15	11.13	33.92	0.404	0.088	1.193
	Tongji	0.40	12.35	0.38	30.96	10.83	33.91	0.469	0.133	1.102
Tongji	PolyU	0.27	17.35	0.51	34.97	20.92	39.13	0.581	0.141	1.024
	IITD	0.42	12.98	0.42	33.98	21.15	39.20	0.646	0.152	0.875

Table 13
Ablation experiments on ASR (%) and image similarity.

Template	Method	S1 (%)		S2 (%)		Image Similarity↑		
		FAR=0.1	FAR=0	FAR=0.1	FAR=0	SSIM	PSNR	MS-SSIM
CompNet	NbNet (Baseline)	18.51	0.18	13.90	0.04	0.20	17.38	0.35
	ProGAN	22.62	0.48	16.50	0.16	0.11	14.60	0.28
	+Dropout	77.26	13.21	62.12	6.15	0.12	16.14	0.35
	+$\mathcal{L}_{MAE}$	81.73	18.63	66.89	10.01	0.13	16.57	0.37
	+$\mathcal{L}_{SAMTC}$	86.25	24.29	74.37	12.76	0.15	16.71	0.39
	+$\mathcal{L}_{SSIM}$	89.40	27.14	77.29	14.94	0.21	17.24	0.41
	+DRTS-P	91.67	30.06	79.10	16.38	0.21	17.32	0.42
	+DRTS-D	**100**	**84.40**	**97.65**	**63.12**	**0.22**	**17.41**	**0.45**
BOCV	NbNet (Baseline)	**100**	**100**	99.51	93.89	0.28	18.56	0.60
	ProGAN	**100**	**100**	97.51	82.51	0.17	17.34	0.53
	+Dropout	**100**	**100**	99.40	92.96	0.18	17.17	0.56
	+$\mathcal{L}_{MAE}$	**100**	**100**	99.59	95.72	0.21	17.82	0.60
	+$\mathcal{L}_{SAMTC}$	**100**	**100**	99.93	99.35	0.32	18.72	0.68
	+$\mathcal{L}_{SSIM}$	**100**	**100**	99.93	99.38	0.33	18.77	0.69
	+DRTS-P	**100**	**100**	99.94	99.40	0.33	18.82	0.69
	+DRTS-D	**100**	**100**	**99.96**	**99.54**	**0.35**	**19.18**	**0.73**

Table 14
Algorithmic Security (AS) and Template Privacy (TP) for each method in scenario $FAR = 0.1\%$.

Method	mASR (%)	AS	mASR (%)	TP
RLOC	77.63	L	65.56	M
BOCV	77.69	L	80.30	L
DRCC	75.32	L	67.11	M
MTCC	75.02	L	80.96	L
DHN	59.82	M	26.60	H
CompNet	78.79	L	27.82	H
SLCN	0.57	H	47.39	M

Notably, the algorithms, like BOCV and MTCC, which possess more information in their templates than RLOC and DRCC, yield significantly higher ASR on DHN. On the other hand, CompNet, similar to most hand-crafted-based methods, employs Gabor filters, resulting in relatively low AS. Other hand-crafted-based methods focusing on intuitive textures also demonstrate lower AS.

Deep-learning-based methods such as DHN and CompNet exhibit relatively higher TP for template privacy. This is because their templates contain abstract high-level features, excluding some useful but non-discriminative information. Consequently, these methods achieve high ASR in single-algorithm attacks but have lower ASR in cross-algorithm attacks. Although SLCN is a deep-learning-based method, it slightly lags in TP due to its shallow network nature, which retains more information regarding the differences between different directions in the templates.

The hand-crafted-based methods, which encode the filtering features, demonstrate slightly higher TP, as the encoding reduces the template's information while increasing the mapping complexity. Conversely, the hand-crafted-based methods utilizing filtering features show lower TP, primarily due to the superficial mapping relationships between templates and images.

5. Conclusions and future works

This paper introduced a novel, versatile palmprint template-based reconstruction method utilizing a modified ProGAN leveraged by dropout as its foundational model. The inclusion of SAMTC loss and DRTS enhanced both the attack success rate and image quality. The proposed method demonstrated its adaptability to various palmprint recognition methods and its generalization in cross-dataset scenarios. An in-depth analysis and comparison of security and privacy aspects were also conducted using various palmprint algorithms. Generally, hand-crafted-based methods exhibited lower Algorithmic Security (AS) and Template Privacy (TP) than deep-learning-based methods. We plan to extend the application of our method to biometric modalities closely related to palmprints, such as those involving veins and knuckle wrinkles, which share similar characteristics. Since template-based reconstruction attacks involve the extraction of templates from the target biometric system, it becomes crucial to investigate the capability of biometric systems to safeguard templates from unauthorized access. Moreover, the reconstruction attack on the protected template will be explored.

CRediT authorship contribution statement

Licheng Yan: Writing – original draft, Visualization, Validation, Software, Methodology, Investigation, Formal analysis, Conceptualization. **Fei Wang:** Software, Investigation, Data curation. **Lu Leng:** Writing – review & editing, Supervision, Resources, Funding acquisition. **Andrew Beng Jin Teoh:** Writing – review & editing, Supervision, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgments

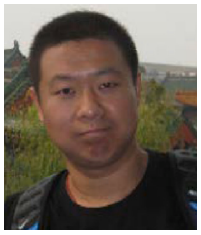
This research was supported by the Jiangxi Province Key Laboratory of Image Processing and Pattern Recognition [grant numbe 2024SSY03111]; the National Natural Science Foundation of China [grant number 61866028]; the Technology Innovation Guidance Program Project (Special Project of Technology Cooperation, Science and Technology Department of Jiangxi Province) [grant number 20212 BDH81003]; and the Innovation Foundation for Postgraduate Students of Nanchang Hangkong University [grant number YC2022-S765].

References

[1] G. Mai, K. Cao, P.C. Yuen, A.K. Jain, On the reconstruction of face images from deep face templates, IEEE Trans. Pattern Anal. Mach. Intell. 41 (5) (2018) 1188–1202.
[2] C.N. Duong, T.-D. Truong, K. Luu, K.G. Quach, H. Bui, K. Roy, Vec2face: Unveil human faces from their blackbox features in face recognition, in: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2020, pp. 6132–6141.
[3] T.-D. Truong, C.N. Duong, N. Le, M. Savvides, K. Luu, Vec2Face-v2: Unveil human faces from their blackbox features via attention-based network in face recognition, 2022, arXiv preprint arXiv:2209.04920.
[4] X. Dong, Z. Jin, Z. Guo, A.B.J. Teoh, Towards generating high definition face images from deep templates, in: 2021 International Conference of the Biometrics Special Interest Group, BIOSIG, IEEE, 2021, pp. 1–11.
[5] X. Dong, Z. Miao, L. Ma, J. Shen, Z. Jin, Z. Guo, A.B.J. Teoh, Reconstruct face from features using GAN generator as a distribution constraint, 2022, arXiv preprint arXiv:2206.04295.
[6] H. Kim, X. Cui, M.-G. Kim, T.H.B. Nguyen, Reconstruction of fingerprints from minutiae using conditional adversarial networks, in: Digital Forensics and Watermarking: 17th International Workshop, IWDW 2018, Jeju Island, Korea, October 22-24, 2018, Proceedings 17, Springer, 2019, pp. 353–362.
[7] C. Kauba, S. Kirchgasser, V. Mirjalili, A. Uhl, A. Ross, Inverse biometrics: Generating vascular images from binary templates, IEEE Trans. Biometr. Behav. Identity Sci. 3 (4) (2021) 464–478.
[8] Z. Yang, L. Leng, B. Zhang, M. Li, J. Chu, Two novel style-transfer palmprint reconstruction attacks, Appl. Intell. 53 (6) (2023) 6354–6371.
[9] Y. Sun, L. Leng, Z. Jin, B.-G. Kim, Reinforced palmprint reconstruction attacks in biometric systems, Sensors 22 (2) (2022) 591.
[10] S. Ahmad, B. Fuller, Resist: Reconstruction of irises from templates, in: 2020 IEEE International Joint Conference on Biometrics, IJCB, IEEE, 2020, pp. 1–10.
[11] T. Karras, T. Aila, S. Laine, J. Lehtinen, Progressive growing of GANs for improved quality, stability, and variation, in: International Conference on Learning Representations, 2018.
[12] L. Shen, J. Jin, R. Zhang, H. Li, K. Zhao, Y. Zhang, J. Zhang, S. Ding, Y. Zhao, W. Jia, RPG-palm: Realistic pseudo-data generation for palmprint recognition, in: Proceedings of the IEEE/CVF International Conference on Computer Vision, 2023, pp. 19605–19616.
[13] T. Wu, L. Leng, M.K. Khan, A multi-spectral palmprint fuzzy commitment based on deep hashing code with discriminative bit selection, Artif. Intell. Rev. (2022) 1–18.
[14] A. Genovese, V. Piuri, K.N. Plataniotis, F. Scotti, PalmNet: Gabor-PCA convolutional networks for touchless palmprint recognition, IEEE Trans. Inf. Forensics Secur. 14 (12) (2019) 3160–3174.
[15] D. Zhang, W.-K. Kong, J. You, M. Wong, Online palmprint identification, IEEE Trans. Pattern Anal. Mach. Intell. 25 (9) (2003) 1041–1050.
[16] A.-K. Kong, D. Zhang, Competitive coding scheme for palmprint verification, in: Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004, Vol. 1, IEEE, 2004, pp. 520–523.
[17] A.W.-K. Kong, D. Zhang, Feature-level fusion for effective palmprint authentication, in: International Conference on Biometric Authentication, Springer, 2004, pp. 761–767.
[18] Z. Sun, T. Tan, Y. Wang, S. Li, Ordinal palmprint representation for personal identification., in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2005.
[19] W. Jia, D.-S. Huang, D. Zhang, Palmprint verification based on robust line orientation code, Pattern Recognit. 41 (5) (2008) 1504–1513.
[20] Z. Guo, D. Zhang, L. Zhang, W. Zuo, Palmprint verification using binary orientation co-occurrence vector, Pattern Recognit. Lett. 30 (13) (2009) 1219–1227.
[21] L. Zhang, H. Li, J. Niu, Fragile bits in palmprint recognition, IEEE Signal Process. Lett. 19 (10) (2012) 663–666.
[22] Q. Zheng, A. Kumar, G. Pan, Suspecting less and doing better: New insights on palmprint identification for faster and more accurate matching, IEEE Trans. Inf. Forensics Secur. 11 (3) (2015) 633–641.
[23] Q. Zheng, A. Kumar, G. Pan, A 3D feature descriptor recovered from a single 2D palmprint image, IEEE Trans. Pattern Anal. Mach. Intell. 38 (6) (2016) 1272–1279.
[24] L. Fei, Y. Xu, W. Tang, D. Zhang, Double-orientation code and nonlinear matching scheme for palmprint recognition, Pattern Recognit. 49 (2016) 89–101.
[25] Y. Xu, L. Fei, J. Wen, D. Zhang, Discriminative and robust competitive code for palmprint recognition, IEEE Trans. Syst. Man Cybern.: Syst. 48 (2) (2016) 232–241.
[26] Z. Yang, L. Leng, W. Min, Extreme downsampling and joint feature for coding-based palmprint recognition, IEEE Trans. Instrum. Meas. 70 (2020) 1–12.
[27] X. Liang, J. Yang, G. Lu, D. Zhang, Compnet: Competitive neural network for palmprint recognition using learnable gabor kernels, IEEE Signal Process. Lett. 28 (2021) 1739–1743.
[28] Z. Yang, L. Leng, T. Wu, M. Li, J. Chu, Multi-order texture features for palmprint recognition, Artif. Intell. Rev. 56 (2) (2023) 995–1011.
[29] L. Fei, S. Zhao, W. Jia, B. Zhang, J. Wen, Y. Xu, Toward efficient palmprint feature extraction by learning a single-layer convolution network, IEEE Trans. Neural Netw. Learn. Syst. (2022).
[30] Z. Yang, W. Xia, Y. Qiao, Z. Lu, B. Zhang, L. Leng, Y. Zhang, CO 3 net: Coordinate-aware contrastive competitive neural network for palmprint recognition, IEEE Trans. Instrum. Meas. (2023).
[31] Z. Yang, H. Huangfu, L. Leng, B. Zhang, A.B.J. Teoh, Y. Zhang, Comprehensive competition mechanism in palmprint recognition, IEEE Trans. Inf. Forensics Secur. (2023).
[32] T. Miyato, M. Koyama, cGANs with projection discriminator, in: International Conference on Learning Representations, 2018.
[33] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, R. Salakhutdinov, Dropout: a simple way to prevent neural networks from overfitting, J. Mach. Learn. Res. 15 (1) (2014) 1929–1958.
[34] T. Salimans, I. Goodfellow, W. Zaremba, V. Cheung, A. Radford, X. Chen, Improved techniques for training gans, Adv. Neural Inf. Process. Syst. 29 (2016).
[35] A. Jolicoeur-Martineau, The relativistic discriminator: a key element missing from standard GAN, in: International Conference on Learning Representations, 2018.
[36] M. Gomez-Barrero, J. Galbally, Reversing the irreversible: A survey on inverse biometrics, Comput. Secur. 90 (2020) 101700.
[37] Kumar, Iit delhi touchless palmprint database version 1.0, 2009.
[38] L. Zhang, L. Li, A. Yang, Y. Shen, M. Yang, Towards contactless palmprint recognition: A novel device, a new benchmark, and a collaborative representation based identification approach, Pattern Recognit. 69 (2017) 199–212.

Licheng Yan is currently pursuing his M.S. degree in software engineering from the School of Software, Nanchang Hangkong University, China. His research interests include biometrics, security analysis, and image generation.

Fei Wang received his M.S. degree from School of Software, Nanchang Hangkong University, Nanchang, P. R. China, in 2021. His research interests include biometrics, image generation.



Lu Leng (Member, IEEE) received his Ph.D. degree from Southwest Jiaotong University, Chengdu, P. R. China, in 2012. He performed his postdoctoral research at Yonsei University, Seoul, South Korea, and Nanjing University of Aeronautics and Astronautics, Nanjing, P. R. China. He was a visiting scholar at West Virginia University, USA, and Yonsei University, South Korea. Currently, he is a full professor at Nanchang Hangkong University. He has published more than 100 international journal and conference papers. He has been granted several scholarships and funding projects in his academic research. He is the reviewer of several international journals and conferences. His research interests include computer vision, biometric template protection, and biometric recognition. Dr. Leng is a member of the Institute of Electrical and Electronics Engineers (IEEE), Association for Computing Machinery (ACM), China Society of Image and Graphics (CSIG), and China Computer Federation (CCF).

Andrew Beng Jin Teoh (Senior Member, IEEE) obtained his BEng (Electronic) in 1999 and a Ph.D. degree in 2003 from the National University of Malaysia. He is currently a full professor in the Electrical and Electronic Engineering Department, College Engineering of Yonsei University, South Korea. His research for which he has received funding focuses on biometric applications and biometric security. His current research interests are Machine Learning and Information Security. He has published more than 350 international refereed journal papers, and conference articles, edited several book chapters, and edited book volumes. He served and is serving as a guest editor of the IEEE Signal Processing Magazine, and associate editor of IEEE TRANSACTIONS ON INFORMATION FORENSIC AND SECURITY, IEEE Biometrics Compendium and Machine Learning with Applications, Elsevier.