# FLeX: Fingerprint Leakage Evaluation across Super-Resolution and Cross-Domain Matching

Van-Truong Le[1,2][0009−0008−7015−7392][✉], Le-Khanh Nguyen[1,2][0009−0006−2245−9148], Tran-Chau Vo Han[1,2][0009−0008−5029−5405], Hieu-Hoc Tran Minh[1,2][0009−0003−3787−6719], and Minh-Triet Tran[1,2][0000−0003−3046−3041][✉]

[1] University of Science, VNU-HCM, Vietnam
[2] Vietnam National University, Ho Chi Minh City, Vietnam
lvtruong@selab.hcmus.edu.vn, 23120052@student.hcmus.edu.vn, 23120003@student.hcmus.edu.vn, 23120006@student.hcmus.edu.vn, tmtriet@fit.hcmus.edu.vn

**Abstract.** Contactless finger-selfies enable convenient biometric capture, but restoration of low-resolution imagery may also expose identity-bearing ridge information. We investigate whether super-resolution increases this leakage. Our evaluation links reconstruction quality (PSNR, SSIM, and LPIPS), minutiae extraction, and NBIS-based contactless-to-livescan matching on ISPFDv2. Bicubic and SwinIR are compared on identical sampled images to separate restoration effects from sampling bias. This design treats leakage as identity-specific utility rather than visual plausibility or feature abundance alone. Bicubic outperforms SwinIR in reconstruction fidelity (25.333 PSNR, 0.518 SSIM, and 0.513 LPIPS versus 24.696, 0.485, and 0.572). Although enhancement increases the mean number of extracted minutiae from 51.19 for raw contactless images to 197.50 for SwinIR outputs and 421.94 for clean contactless images, it does not improve identity separation: all evaluated contactless representations yield EERs near 0.5. These results expose a gap between visual restoration, template extractability, and identity-consistent leakage, showing that the first two are insufficient without downstream matching. Code is available at github.com/lee-vtruong/fingerprint-sr-leakage.

**Keywords:** Contactless fingerprint · super-resolution · biometric leakage · minutiae extraction · cross-domain matching · NBIS.

## 1 INTRODUCTION

Commodity cameras make contactless finger-selfie acquisition convenient, but also expose fingerprints to uncontrolled capture and restoration pipelines [19]. Super-resolution can improve apparent ridge visibility; however, plausible detail may not preserve the ridge topology and minutiae correspondence required for biometric identification.

Most super-resolution evaluations emphasize fidelity or perceptual quality, whereas biometric risk depends on whether restored structures remain consistent with a person's reference fingerprint. Likewise, a larger minutiae template may reflect enhancement artifacts rather than additional identity information. Consequently, evaluations based only on image similarity can overstate privacy risk when restored ridge-like details do not support genuine matching. This distinction motivates evaluating restoration and biometric utility within the same pipeline.

We therefore ask: *Does fingerprint super-resolution increase identity leakage in contactless finger-selfie images?* We distinguish three levels of evidence: reconstruction fidelity, minutiae extractability, and identity-consistent matching. This separation prevents intermediate improvements from being interpreted prematurely as evidence of privacy loss. Leakage is established only when restored probes match their genuine references, rather than merely appearing sharper or yielding more detected minutiae.

We compare Bicubic and SwinIR [8] using identical samples from ISPFDv2 [10, 14]. The pipeline measures PSNR, SSIM, and LPIPS, extracts minutiae with MINDTCT, and matches contactless probes to livescan galleries using Bozorth3 [7]. Our contributions are a reproducible multi-level leakage protocol, a controlled comparison of classical and learned restoration under identical degradation conditions, and empirical evidence that increased minutiae extractability does not necessarily imply identity leakage.

## 2 RELATED WORK

### 2.1 Contactless Fingerprint Recognition

Contactless fingerprint recognition is moving from dedicated sensors to camera-based and mobile settings. Finger-selfies offer convenient, hygienic, low-cost capture with commodity devices, but introduce uncontrolled illumination, background clutter, weak ridge contrast, scale variation, pose, perspective distortion, and camera-dependent quality. These factors make contactless-to-livescan matching harder than conventional contact-based recognition.

Prior contactless-to-contact methods combine preprocessing, enhancement, scale correction, unwarping, and handcrafted or CNN-based matching [5,9]. They show that modality-specific distortion and noise affect feature extraction and matching. ISPFDv2 pairs smartphone contactless images with livescan fingerprints for cross-domain evaluation. While prior work emphasizes recognition, we evaluate whether super-resolution and enhancement increase biometric leakage.

### 2.2 Fingerprint Enhancement and Minutiae-Based Matching

Fingerprint systems commonly use ridge endings and bifurcations as compact identity-bearing minutiae [16]. Matchers compare their spatial and angular configurations, while modern alternatives learn fingerprint representations directly.

Reliability depends on stability and correspondence, not only count; noisy or non-corresponding minutiae need not improve recognition.

Fingerprint enhancement is widely used to improve ridge-valley contrast and facilitate minutiae extraction, especially for low-quality fingerprints [6]. In contactless or degraded settings, enhancement may increase ridge visibility and produce more detected minutiae. At the same time, it may also introduce false ridge structures or spurious minutiae when the original image contains weak ridge information, background texture, or restoration artifacts. This distinction is important for biometric leakage assessment: a restored image may appear more fingerprint-like or produce a larger template without necessarily preserving identity-consistent minutiae.

We use the NIST Biometric Image Software (NBIS) toolkit as a transparent backend [7]: MINDTCT extracts minutiae and Bozorth3 performs matching. Although not a state-of-the-art contactless matcher, it provides a controlled, reproducible test of whether restored templates are discriminative.

### 2.3 Super-Resolution for Biometric Images

Super-resolution is commonly studied as a low-level vision task for reconstructing high-resolution images from degraded or low-resolution inputs, including practical real-world restoration [17]. In biometric applications, however, visual reconstruction quality is not the only objective. Identity-aware face super-resolution illustrates the need to preserve recognition-relevant information rather than visual detail alone [4]. For fingerprints, this requirement is especially strict because identity depends on fine ridge-valley patterns, ridge continuity, orientation fields, and minutiae geometry.

Fingerprint super-resolution is therefore different from natural image super-resolution. While a natural image model may produce perceptually plausible textures, the perception–distortion tradeoff implies that perceptual improvement need not correspond to lower reconstruction error [2]. Fingerprint restoration must additionally avoid altering ridge topology or generating false minutiae. Fingerprint-specific super-resolution methods have incorporated ridge orientation and coupled dictionaries to preserve fingerprint geometry [15]. In contrast, generic restoration models may not be optimized for ridge fidelity or identity consistency.

SwinIR is a strong generic image restoration model based on the Swin Transformer and has been used for tasks such as image super-resolution, denoising, and artifact reduction [8]. In this study, SwinIR is used as a representative deep super-resolution baseline rather than as a fingerprint-specialized model. This distinction is important because a generic model may improve visual plausibility without improving biometric consistency.

### 2.4 Biometric Leakage Assessment

Biometric leakage refers to the extent to which a transformed or restored biometric image reveals identity-bearing information [11]. Prior work has shown that

fingerprint images can be reconstructed from standard templates or minutiae points, demonstrating that intermediate biometric representations may themselves expose sensitive ridge information [3, 13]. In fingerprint super-resolution, leakage cannot be assessed solely by image quality metrics such as PSNR, SSIM, or LPIPS. These metrics quantify reconstruction fidelity or perceptual similarity, but they do not directly measure whether the restored image enables reliable identity matching. Similarly, minutiae count alone is insufficient because a template with many minutiae may still fail to match if the detected points are not spatially and structurally consistent with the genuine reference.

This motivates a multi-level protocol covering reconstruction quality, minutiae extractability, and identity-consistent matching. Contactless fingerprint research mainly targets cross-domain recognition, while biometric super-resolution often emphasizes reconstruction quality or recognition utility. Whether super-resolution increases leakage from contactless finger-selfies remains less explored.

Our work addresses this gap by connecting super-resolution, enhancement, minutiae extraction, and NBIS-based matching in one pipeline. This design distinguishes visual restoration quality, extractable fingerprint structure, and actual identity leakage under downstream matching.

## 3 METHOD

This section describes the proposed evaluation methodology for assessing biometric leakage from super-resolved contactless fingerprint images. Unlike conventional super-resolution evaluation, which primarily focuses on image reconstruction quality, our methodology links restoration quality to biometric utility through a sequence of image reconstruction, enhancement, minutiae extraction, and fingerprint matching. The goal is to determine whether super-resolution produces fingerprint representations that are not only visually closer to the reference image, but also more capable of revealing identity-bearing information under a minutiae-based matching protocol.

Figure 1 illustrates the full experimental pipeline. Given a low-resolution contactless finger-selfie input, we generate restored images using two super-resolution baselines: Bicubic interpolation and SwinIR. The reconstructed images are evaluated against the corresponding clean contactless reference using PSNR, SSIM, and LPIPS. In parallel, the restored outputs are passed through a fingerprint enhancement stage and then converted into minutiae templates using MINDTCT from the NBIS toolkit. The extracted probe templates are matched against livescan gallery templates using Bozorth3. The resulting matching scores are used to compute biometric leakage indicators, including genuine and impostor score distributions, FAR, FRR, and EER.

### 3.1 Dataset

We conduct our experiments on ISPFDv2, which contains contactless finger-selfie images and corresponding livescan fingerprint samples [10, 14]. In this study, we

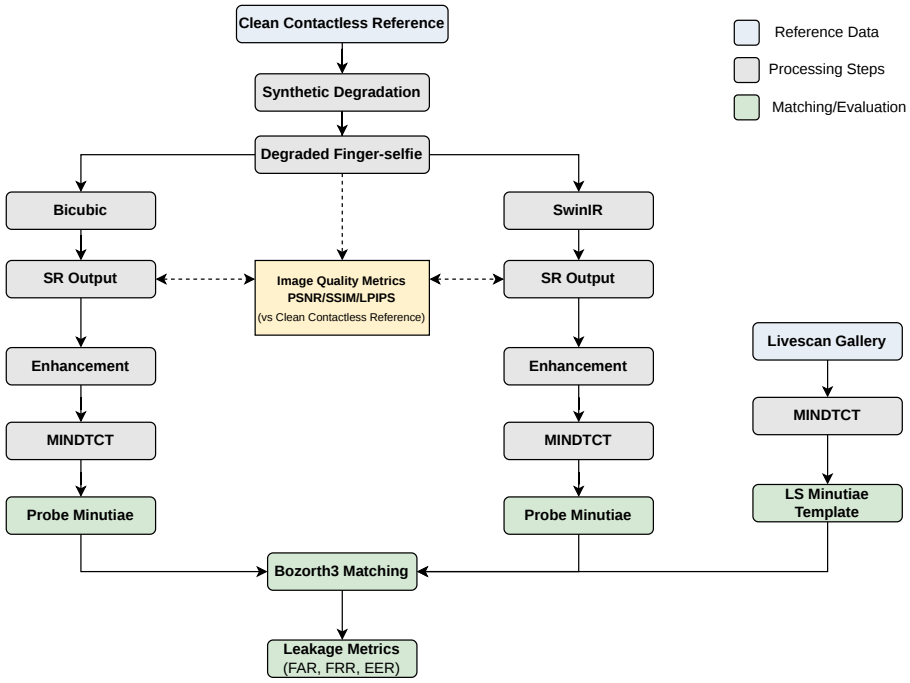



Fig. 1: Full pipeline of the proposed leakage assessment framework. Low-resolution contactless finger-selfie images are reconstructed using Bicubic interpolation and SwinIR. The restored outputs are evaluated using image quality metrics against the clean contactless reference. The same outputs are then enhanced, processed by MINDTCT to extract minutiae templates, and matched using Bozorth3 against livescan templates to assess biometric leakage.

use two contactless subsets, denoted as BI and RES, and one livescan subset, denoted as LS. The BI and RES subsets are used as contactless probe data, while LS is used as the contact-based gallery reference in the matching protocol.

To ensure fair comparison between Bicubic and SwinIR, we evaluate both methods on the same sampled image identities and degradation conditions. Each contactless subset contains 35,520 evaluated images, resulting in 71,040 contactless probe images in total. The livescan set contains 2,368 images. Table 1 summarizes the dataset split used in our experiments.

Each contactless image is associated with a corresponding clean contactless reference for image-quality evaluation. For biometric matching, contactless probe images are mapped to their corresponding livescan templates according to the subject, finger, session, and instance identifiers extracted from the filename. The same mapping protocol is used for all reconstruction methods to ensure a consistent evaluation setting.

Table 1: Dataset statistics used in the evaluation.

| Subset | Description | Images |
|---|---|---|
| BI | Contactless finger-selfie subset | 35,520 |
| RES | Contactless finger-selfie subset | 35,520 |
| LS | Livescan fingerprint subset | 2,368 |

### 3.2 Super-Resolution Methods

We evaluate Bicubic interpolation and SwinIR on 30 synthetic degradation conditions combining downscaling to $s \in \{32, 64, 128, 256, 512\}$, JPEG quality $q \in \{25, 50, 75, 100\}$, Gaussian kernels $k \in \{3, 5, 7\}$, and noise levels $\sigma \in \{5, 10, 20\}$.

**Bicubic interpolation.** Bicubic interpolation is used as a simple and deterministic baseline. Although it does not learn fingerprint-specific priors, it provides a strong reference point for assessing whether a learned super-resolution model offers practical gains over standard resizing. All Bicubic outputs are resized to the common target resolution used in the downstream evaluation.

**SwinIR.** We apply pretrained DIV2K SwinIR-M checkpoints [8] without fingerprint-specific fine-tuning: $\times 2$ for $256 \times 256$ inputs and $\times 4$ for inputs of $128 \times 128$ or smaller; $512 \times 512$ inputs are copied directly.

All outputs are standardized to $512 \times 512$ pixels before metric computation and biometric processing, preventing scale differences from affecting minutiae extraction.

### 3.3 Image Quality Metrics

To assess reconstruction quality, we compute PSNR and SSIM with data range 255 and LPIPS with the AlexNet backbone between each output and its clean contactless reference [18, 20]. The same 71,040 images are used for both restoration methods.

PSNR measures pixel fidelity, while SSIM compares luminance, contrast, and local structure:

$$\mathrm{PSNR}(I, \hat{I}) = 10 \log_{10} \left( \frac{MAX_I^2}{\mathrm{MSE}(I, \hat{I})} \right), \tag{1}$$

$$\mathrm{SSIM}(I, \hat{I}) = \frac{(2\mu_I \mu_{\hat{I}} + C_1)(2\sigma_{I\hat{I}} + C_2)}{(\mu_I^2 + \mu_{\hat{I}}^2 + C_1)(\sigma_I^2 + \sigma_{\hat{I}}^2 + C_2)}.$$

Here, $MAX_I$ is the maximum pixel value; $\mu$, $\sigma^2$, and $\sigma_{I\hat{I}}$ are local means, variances, and covariance; and $C_1, C_2$ ensure numerical stability. Higher PSNR and SSIM are better.

**Learned Perceptual Image Patch Similarity (LPIPS).** LPIPS measures perceptual similarity using deep feature representations. Unlike PSNR and SSIM, which are based on pixel or structural similarity, LPIPS compares images in a learned feature space. Lower LPIPS indicates greater perceptual similarity.

In this work, LPIPS is used as a complementary metric to evaluate whether reconstructed fingerprints are perceptually closer to the clean contactless reference.

These image quality metrics are used to quantify restoration fidelity, but they are not treated as direct evidence of biometric leakage. Therefore, we further evaluate the restored images through minutiae extraction and fingerprint matching.

### 3.4 Minutiae Extraction

To evaluate whether restored images contain extractable fingerprint structures, we use MINDTCT from the NBIS toolkit [7]. MINDTCT extracts minutiae points from fingerprint images and produces minutiae templates in the `.xyt` format. Each minutia is represented by its spatial coordinates and orientation.

Before extraction, contactless outputs are converted to grayscale and enhanced with CLAHE (clip limit 2.0, $8 \times 8$ tiles), $3 \times 3$ Gaussian smoothing, and adaptive Gaussian thresholding (block size 25, constant 5). The enhanced images are then provided to MINDTCT.

The number of extracted minutiae is used as an intermediate biometric indicator. However, we do not assume that a larger number of minutiae necessarily implies higher biometric leakage. Extracted minutiae may include false or unstable points, especially when the input contains weak ridge structures, restoration artifacts, or enhancement-induced texture. Therefore, minutiae count is analyzed together with downstream matching performance.

For the livescan subset, MINDTCT is also applied under the same extraction settings to generate gallery templates. These templates serve as reference identities in the contactless-to-livescan protocol.

To avoid ambiguity, we explicitly define the image representations used in the minutiae extraction and matching experiments. *Raw contactless* denotes the original cropped contactless finger-selfie image before fingerprint enhancement. *Clean contactless + enhancement* denotes the same clean cropped contactless image after applying the fingerprint enhancement stage, without synthetic degradation and without super-resolution. *SwinIR + enhancement* denotes the SwinIR-restored output generated from a synthetically degraded contactless input, followed by the same enhancement stage. *Livescan* denotes the contact-based fingerprint image used as the gallery reference.

Thus, *Clean contactless + enhancement* is a diagnostic of enhancement alone, not a super-resolved output. It measures how strongly enhancement increases MINDTCT extractability on clean images; its high count may reflect amplified ridge-like structures and unstable or non-corresponding detections rather than identity-bearing minutiae.

### 3.5 Matching Protocol

After minutiae extraction, we evaluate whether the generated templates can reveal identity information through fingerprint matching. We use Bozorth3 from

the NBIS toolkit to compute matching scores between probe and gallery minutiae templates [7].

In our main matching protocol, the probe template is extracted from a contactless image after restoration and enhancement, while the gallery contains 2,368 livescan templates. Genuine pairs share subject, finger, session, and instance identifiers; impostor pairs use different finger identities. Each representation produces 71,040 genuine and 71,040 impostor scores.

Formally, let $P_i$ denote the minutiae template extracted from a contactless probe image and $G_j$ denote a gallery template extracted from a livescan fingerprint. Bozorth3 computes a matching score:

$$s_{ij} = \text{Bozorth3}(P_i, G_j), \tag{2}$$

where a higher score indicates stronger minutiae correspondence between the probe and gallery templates. For genuine comparisons, $i$ and $j$ correspond to the same identity. For impostor comparisons, they correspond to different identities.

This protocol allows us to test whether super-resolution and enhancement produce contactless fingerprint templates that are identity-consistent with the corresponding livescan reference.

### 3.6 Leakage Evaluation

We evaluate biometric leakage using genuine and impostor matching scores. A method is considered to reveal stronger identity information if its genuine scores are consistently higher than impostor scores, leading to lower verification error rates. Conversely, if genuine and impostor score distributions overlap substantially, the restored images do not provide reliable identity-consistent matching under the evaluated protocol.

At threshold $\tau$, scores $s \geq \tau$ are accepted. FAR, FRR, and EER are computed according to established biometric performance definitions [1]:

$$\begin{aligned} \text{FAR}(\tau) &= \frac{|\{s_{\text{imp}} \geq \tau\}|}{N_{\text{imp}}}, & \text{FRR}(\tau) &= \frac{|\{s_{\text{gen}} < \tau\}|}{N_{\text{gen}}}, \\ \tau^* &= \arg\min_{\tau} |\text{FAR}(\tau) - \text{FRR}(\tau)|, & \text{EER} &= \tfrac{1}{2}[\text{FAR}(\tau^*) + \text{FRR}(\tau^*)]. \end{aligned} \tag{3}$$

Here, $N_{\text{imp}}$ and $N_{\text{gen}}$ are the numbers of impostor and genuine comparisons.

A lower EER indicates stronger identity separability between genuine and impostor comparisons. In the context of this work, lower EER after super-resolution would suggest stronger biometric leakage, while an EER close to 0.5 indicates near-random matching behavior under the evaluated protocol.

Overall, our methodology separates three levels of analysis: image reconstruction quality, minutiae extractability, and identity-consistent matching. This separation is essential because an image may achieve better visual quality or yield more minutiae without producing a more discriminative biometric template.

# 4 EXPERIMENTAL RESULTS

This section presents the experimental results of the proposed leakage assessment pipeline. We organize the analysis into three levels: image reconstruction quality, minutiae extractability, and identity matching performance. This organization follows the central question of the paper: whether super-resolution improves only visual or structural quality, or whether it also increases identity-consistent biometric leakage. Unless otherwise stated, the image quality comparison between Bicubic and SwinIR is conducted on the same sampled evaluation set [10, 14].

## 4.1 SR Reconstruction Quality

We first evaluate the reconstruction quality of Bicubic interpolation and SwinIR using PSNR, SSIM, and LPIPS. PSNR and SSIM measure pixel-level and structural fidelity with respect to the clean contactless reference, while LPIPS measures perceptual similarity in a learned feature space. Higher PSNR and SSIM indicate better reconstruction quality, whereas lower LPIPS indicates better perceptual similarity.

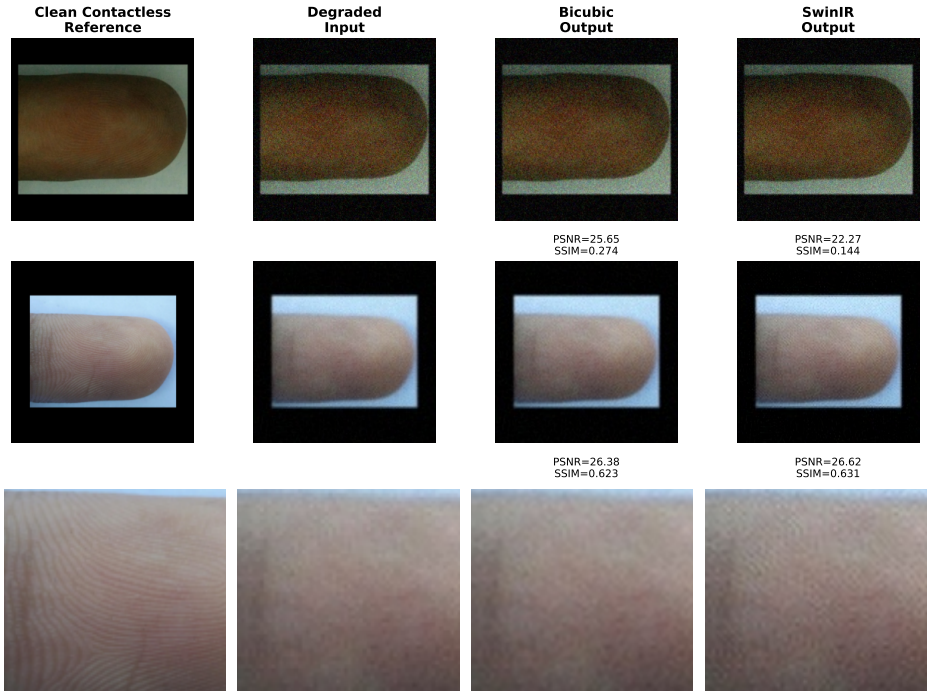
Table 2 reports the average reconstruction quality of the two super-resolution methods. Bicubic interpolation achieves higher PSNR and SSIM than SwinIR, and also obtains a lower LPIPS score. Specifically, Bicubic achieves a PSNR of 25.333, SSIM of 0.518, and LPIPS of 0.513, while SwinIR obtains a PSNR of 24.696, SSIM of 0.485, and LPIPS of 0.572. These results indicate that, under our evaluation setting, the generic SwinIR model does not improve reconstruction fidelity over the Bicubic baseline for contactless fingerprint images.

Table 2: SR reconstruction quality on the fair sampled evaluation set.

| Model | PSNR ↑ | SSIM ↑ | LPIPS ↓ |
|---|---|---|---|
| Bicubic | 25.333 | 0.518 | 0.513 |
| SwinIR | 24.696 | 0.485 | 0.572 |

SwinIR is lower than Bicubic by 0.637 PSNR and 0.033 SSIM, and higher by 0.059 LPIPS. Since lower LPIPS is better, all three metrics consistently favor Bicubic in this setting.

The visual comparison in Figure 2 provides qualitative evidence consistent with the quantitative results. Each row shows the clean reference, the degraded low-resolution input, the Bicubic output, and the SwinIR output. In the representative samples, both reconstruction methods recover the global finger region, but fine ridge structures remain difficult to restore. SwinIR does not visibly recover stable ridge details beyond Bicubic, and in some cases appears to smooth or alter local ridge-like texture. This observation is consistent with the lower PSNR/SSIM and higher LPIPS obtained by SwinIR.




(a) Clean (b) LR input (c) Bicubic (d) SwinIR

Fig. 2: Visual comparison of fingerprint super-resolution outputs. The upper panel shows two representative samples with four columns: clean contactless reference, degraded low-resolution input, Bicubic reconstruction, and SwinIR reconstruction. The lower panel magnifies the same central ridge region from the second sample, making the loss and alteration of fine ridge structure directly visible.

These results suggest a domain mismatch between generic image super-resolution and contactless fingerprint restoration. Fingerprint images require preservation of ridge-valley structures and minutiae-relevant geometry, while a generic image restoration model may not be optimized for such biometric constraints. Therefore, image-level fidelity alone is insufficient to determine biometric leakage, motivating the following analyses on minutiae extraction and identity matching.

### 4.2 Minutiae Extractability

We next evaluate how many minutiae can be extracted from different image representations. Minutiae count is an intermediate indicator of fingerprint template extractability. However, it should not be interpreted directly as identity leakage,

because extracted minutiae may include false, unstable, or non-corresponding points.

Table 3 jointly reports minutiae extractability and downstream matching performance. Raw contactless images yield only 51.19 minutiae on average. SwinIR + enhancement yields 197.50 minutiae, slightly above the livescan average of 164.36, while Clean contactless + enhancement yields 421.94.

Table 3: Minutiae extractability and contactless-to-livescan matching performance.

| Representation | Mean Minutiae | Genuine Mean | Impostor Mean | EER |
|---|---|---|---|---|
| Raw contactless | 51.19 | 0.94 | 0.94 | 0.5008 |
| SwinIR + enhancement | 197.50 | 6.93 | 6.94 | 0.4998 |
| Clean contactless + enhancement | 421.94 | 5.78 | 5.80 | 0.4955 |
| Livescan | 164.36 | – | – | – |

The unusually high count of Clean contactless + enhancement requires care. This image is not super-resolved; it is the clean cropped contactless image after the same enhancement used before MINDTCT and therefore measures the effect of enhancement alone. The pipeline can strongly amplify ridge-like structures and produce many detections that are not necessarily stable or identity-consistent. Table 3 supports this interpretation: despite producing the largest number of extracted minutiae, this representation has an EER of 0.4955.

Relative to raw contactless images, SwinIR + enhancement produces approximately 3.86 times more minutiae, while Clean contactless + enhancement produces approximately 8.24 times more.

These results show that enhancement and super-resolution substantially increase extractability. However, the magnitude requires care: Clean contactless + enhancement produces over twice the livescan count. Such an increase suggests that enhancement introduces ridge-like structures or noise patterns that are detected as minutiae without necessarily being stable or identity-consistent.

Figure 3 visualizes the distributions across all four representations. Beyond the aggregate means in Table 3, it shows whether the increase reflects a consistent distribution-wide shift or instead arises from a subset of images with unusually many detections.

The key observation is that minutiae extractability improves substantially after enhancement and super-resolution. Nevertheless, this does not itself establish biometric leakage. The next subsection therefore evaluates whether the additional minutiae support genuine-versus-impostor identity separation.

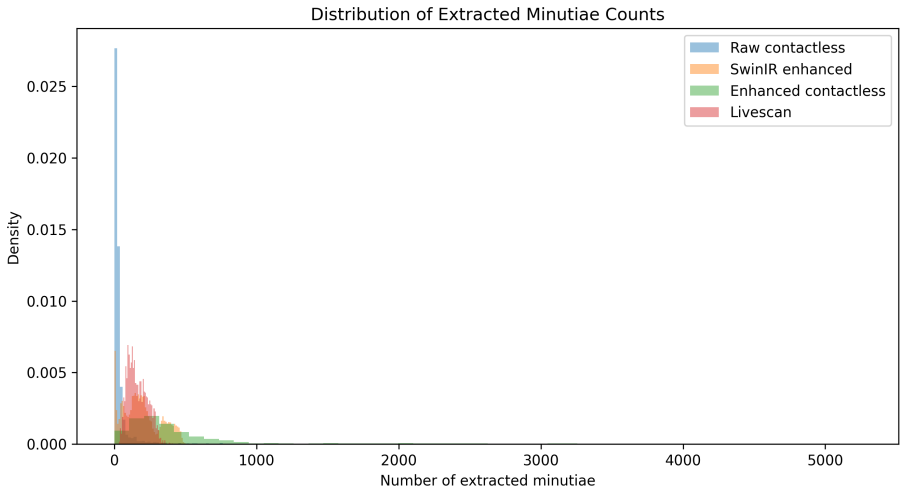



Fig. 3: Distribution of extracted minutiae counts. The figure compares raw contactless, SwinIR + enhancement, Clean contactless + enhancement, and livescan images. This visualization highlights that enhancement and super-resolution increase minutiae extractability, but may also produce unusually high minutiae counts relative to livescan fingerprints.

### 4.3 Identity Matching Performance

Finally, we evaluate whether the extracted templates enable identity-consistent matching using the contactless-to-livescan protocol in Section 3. Contactless templates serve as probes and livescan templates as gallery references. Genuine pairs share an identity, whereas impostor pairs use different finger identities. A representation that leaks identity should produce consistently higher genuine than impostor scores, resulting in a low EER.

Table 3 reports matching performance for the three contactless representations against livescan templates. Genuine and impostor means are nearly identical and all EERs are close to 0.5, indicating near-random verification. Although enhancement and SwinIR raise mean scores relative to raw contactless images, they raise genuine and impostor scores similarly. The higher score level therefore provides no meaningful identity separation or identity-specific leakage under the NBIS protocol.

Figure 4 presents the corresponding ROC curves. All three curves remain close to the chance diagonal over most operating points, consistent with their EER values near 0.5 and confirming that the evaluated representations provide little genuine–impostor discrimination.

The genuine and impostor score distributions overlap substantially in all three experiments, directly explaining the high EERs and confirming that the

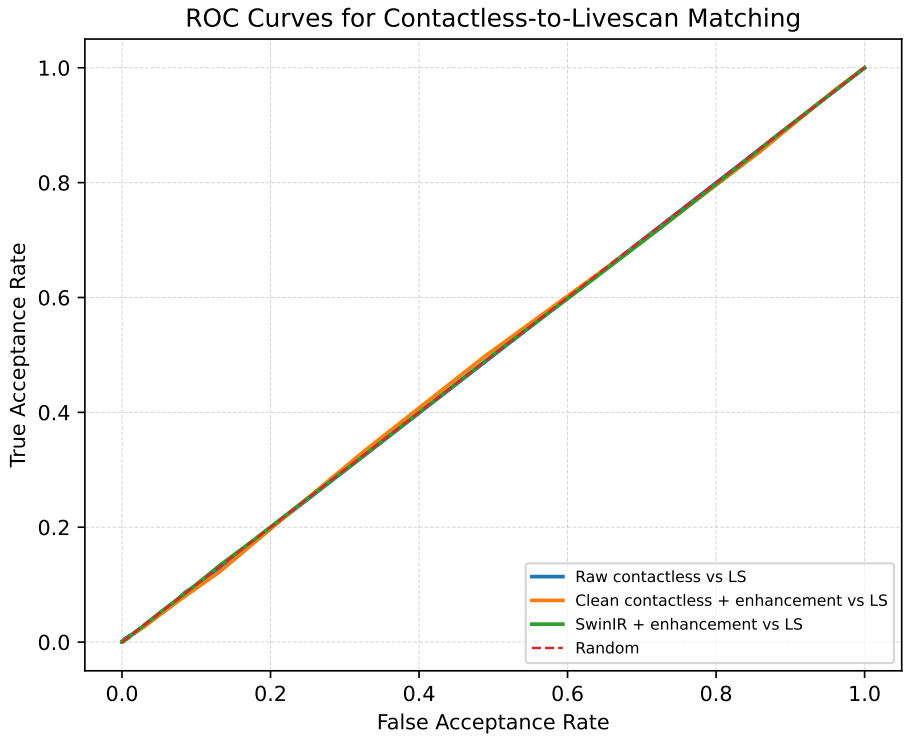



Fig. 4: ROC curves for contactless-to-livescan matching. Raw contactless, Clean contactless + enhancement, and SwinIR + enhancement probes are compared against livescan gallery templates. Curves near the diagonal indicate weak identity separability under the evaluated matching protocol.

extracted minutiae templates are not identity-consistent with the corresponding livescan references.

Overall, the experimental results separate reconstruction quality, minutiae extractability, and identity leakage. Bicubic achieves better image reconstruction metrics than SwinIR, while enhancement and SwinIR increase the number of extractable minutiae. However, the additional detections do not translate into identity-consistent matching against livescan fingerprints. Visual restoration quality and template extractability are therefore insufficient leakage proxies without downstream identity matching.

## 5 DISCUSSION

Enhancement and super-resolution increase minutiae detections without improving identity separation. The similar rise in genuine and impostor scores suggests

that many added detections are unstable or spurious, arising from amplified skin texture, noise, or restoration artifacts rather than corresponding ridge structures.

The contactless-to-livescan domain gap further changes ridge appearance, scale, perspective, and alignment [5, 9]. A same-domain livescan sanity check confirms that the NBIS backend remains discriminative (genuine mean 101.81, impostor mean 9.29, EER 0.0638), whereas the cross-domain EERs remain near 0.5. Thus, our result is limited to the evaluated generic-SR and NBIS protocol; fingerprint-specific restoration, alignment, enhancement, or learned cross-domain matching may yield different leakage behavior.

## 6 THREATS TO VALIDITY

Our conclusions are bounded by four factors. First, MINDTCT and Bozorth3 are reproducible but not optimized for contactless-to-livescan matching [5, 12]. Second, SwinIR is a generic rather than fingerprint-specific restoration model [8]. Third, ISPFDv2 acquisition conditions and the enhancement pipeline may limit generalization. Finally, EER captures minutiae-based verification but not forensic cues or attacks using neural matchers. Consequently, the absence of leakage here does not establish universal safety.

## 7 CONCLUSION

We evaluated fingerprint super-resolution through reconstruction quality, minutiae extraction, and cross-domain matching. Bicubic outperforms SwinIR in PSNR, SSIM, and LPIPS, while enhancement greatly increases minutiae detections. Nevertheless, all contactless representations yield EERs near 0.5 under the evaluated NBIS protocol.

Biometric leakage should therefore be assessed through identity-consistent downstream matching rather than visual quality or minutiae count alone. Future work should test fingerprint-specific restoration, stronger cross-domain matchers, and broader datasets.

**Disclosure of Interests.** The authors have no competing interests to declare that are relevant to the content of this paper.

## References

1. Information technology — biometric performance testing and reporting — part 1: Principles and framework (May 2021), corrected version, 2024-09
2. Blau, Y., Michaeli, T.: The perception-distortion tradeoff. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. pp. 6228–6237 (2018)
3. Cappelli, R., Lumini, A., Maio, D., Maltoni, D.: Fingerprint image reconstruction from standard templates. IEEE Transactions on Pattern Analysis and Machine Intelligence **29**(9), 1489–1503 (2007)

4. Chen, J., Chen, J., Wang, Z., Liang, C., Lin, C.W.: Identity-aware face super-resolution for low-resolution face recognition. IEEE Signal Processing Letters **27**, 645–649 (2020)
5. Grosz, S.A., Engelsma, J.J., Liu, E., Jain, A.K.: C2cl: Contact to contactless fingerprint matching. IEEE Transactions on Information Forensics and Security **17**, 196–210 (2021)
6. Hong, L., Wan, Y., Jain, A.: Fingerprint image enhancement: algorithm and performance evaluation. IEEE transactions on pattern analysis and machine intelligence **20**(8), 777–789 (1998)
7. Ko, K.: User's guide to nist biometric image software (nbis) (2007)
8. Liang, J., Cao, J., Sun, G., Zhang, K., Van Gool, L., Timofte, R.: Swinir: Image restoration using swin transformer. In: Proceedings of the IEEE/CVF international conference on computer vision. pp. 1833–1844 (2021)
9. Lin, C., Kumar, A.: Matching contactless and contact-based conventional fingerprint images for biometrics identification. IEEE Transactions on Image Processing **27**(4), 2008–2021 (2018)
10. Malhotra, A., Sankaran, A., Vatsa, M., Singh, R.: On matching finger-selfies using deep scattering networks (2020)
11. Malhotra, A., Chhabra, S., Vatsa, M., Singh, R.: On privacy preserving anonymization of finger-selfies. In: Proceedings of the IEEE/CVF conference on computer vision and pattern recognition workshops. pp. 26–27 (2020)
12. Priesnitz, J., Weißenfeld, A., Ruzicka, L., Rathgeb, C., Strobl, B., Lessmann, R., Busch, C.: Mclfiq: mobile contactless fingerprint image quality. IEEE Transactions on Biometrics, Behavior, and Identity Science **6**(2), 272–287 (2024)
13. Ross, A., Shah, J., Jain, A.K.: From template to image: Reconstructing fingerprints from minutiae points. IEEE Transactions on Pattern Analysis and Machine Intelligence **29**(4), 544–560 (2007)
14. Sankaran, A., Malhotra, A., Mittal, A., Vatsa, M., Singh, R.: On smartphone camera based fingerphoto authentication. In: Proceedings of the International Conference on Biometrics: Theory, Applications and Systems. pp. 1–7 (2015)
15. Singh, K., Gupta, A., Kapoor, R.: Fingerprint image super-resolution via ridge orientation-based clustered coupled sparse dictionaries. Journal of Electronic Imaging **24**(4), 043015 (2015)
16. Tang, Y., Gao, F., Feng, J., Liu, Y.: Fingernet: An unified deep network for fingerprint minutiae extraction. In: 2017 IEEE International Joint Conference on Biometrics (IJCB). pp. 108–116. IEEE (2017)
17. Wang, X., Xie, L., Dong, C., Shan, Y.: Real-esrgan: Training real-world blind super-resolution with pure synthetic data. In: Proceedings of the IEEE/CVF International Conference on Computer Vision Workshops. pp. 1905–1914 (2021)
18. Wang, Z., Bovik, A.C., Sheikh, H.R., Simoncelli, E.P.: Image quality assessment: from error visibility to structural similarity. IEEE transactions on image processing **13**(4), 600–612 (2004)
19. Yin, X., Zhu, Y., Hu, J.: A survey on 2d and 3d contactless fingerprint biometrics: A taxonomy, review, and future directions. IEEE Open Journal of the Computer Society **2**, 370–381 (2021)
20. Zhang, R., Isola, P., Efros, A.A., Shechtman, E., Wang, O.: The unreasonable effectiveness of deep features as a perceptual metric. In: Proceedings of the IEEE conference on computer vision and pattern recognition. pp. 586–595 (2018)