ISSN 2669-2023 (print) / ISSN 2538-8959 (on-line) **/ https://doi.org/1.47459/cndcgs.2026.29**

Cybersecurity Risks and Countermeasures in Mobile Contactless Fingerprint Acquisition: Presentation Attack Detection and Secure Processing

Martin DRAHANSKÝ[1]*, Jaromír ŠTĚPÁNEK[1], Tomáš VOKÁLEK[2], Radim DVOŘÁK[3], Eliška ŠOLCOVÁ[1]

[1]Department of Criminalistics, Faculty of Security and Law, Police Academy of the Czech Republic in Prague, Lhotecká 559/7, 143 00, Prague, Czech Republic
[2]Department of the Criminalist Technology and Expertise of the Military Police, Rooseveltova 620/23, 160 01, Prague, Czech Republic
[3]TrendBit a.s., Strmá 2811/63, 616 00, Brno, Czech Republic

*Correspondence:*drahansky@polac.cz*

Abstract

This paper analyzes cybersecurity risks in mobile contactless fingerprint acquisition and proposes a two-phase processing and evaluation pipeline. The method estimates fingerprint resolution (DPI) using reference objects and applies preprocessing and normalization for reliable matching. Security threats, including presentation attacks using fingerprint presentation attack instruments, are analyzed according to ISO/IEC standards. Experimental results show that DPI normalization improves matching performance, achieving zero FAR and FRR in the evaluated dataset. The approach provides a basis for secure processing and future integration of presentation attack detection mechanisms in mobile biometric systems.

KEY WORDS: *contactless biometrics, fingerprint recognition, presentation attack detection, mobile devices, DPI estimation, biometric security, ISO/IEC 30107, image preprocessing*

Citation: Drahanský, M.; Štěpánek, J.; Vokálek, T.; Dvořák, R.; Šolcová, E. Cybersecurity Risks and Countermeasures in Mobile Contactless Fingerprint Acquisition: Presentation Attack Detection and Secure Processing. In Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 7-10 September 2026. ISSN 2538-8959, https://doi.org/10.47459/cndcgs.2026.29

1. Introduction

With the rapid advancement of mobile technologies, it is natural to consider whether smartphones equipped with high-resolution cameras can be utilized for biometric purposes, specifically for capturing finger images and extracting fingerprint patterns in a fully contactless manner without specialized hardware. Modern mobile devices offer increasingly sophisticated imaging capabilities at relatively low cost, making such applications technically feasible. At the same time, concerns have emerged regarding the potential misuse of this capability, particularly the extraction of fingerprint information from publicly available images. Notable examples include the 2014 reconstruction of a fingerprint belonging to the then-German Minister of Defense (now President of the European Commission), Ursula von der Leyen [1,2] (see Fig. 1), as well as more recent warnings highlighting the risks associated with gestures such as the "victory sign" in selfies [3,4].

While earlier studies and reports often suggested that the use of mobile devices for contactless fingerprint acquisition is feasible in practice, more recent research presents a more cautious perspective. In particular, experts increasingly emphasize the technical limitations, variability of acquisition conditions, and security implications that complicate reliable deployment of such approaches. This apparent discrepancy reflects the difference between controlled experimental demonstrations and real-world operational requirements. Therefore, this paper aims to provide a comprehensive analysis of the problem, examining both the practical feasibility and the associated risks, and to clarify the conditions under which mobile contactless fingerprint acquisition can be considered reliable and secure.

Peer-review under responsibility of General Jonas Žemaitis Miltitary Academy of Lithuania and University of Defence, Czech Republic.

Fig. 1. A video frame, the corresponding region of interest, and a partially reconstructed fingerprint [2].

2. Rules for testing contactless devices

To ensure interoperability between fingerprint sensors and recognition algorithms – where hardware (e.g., a sensor from one manufacturer) operates independently of software (e.g., a matching algorithm from another) – it is essential to standardize both input and output data. This standardization is defined by international frameworks, particularly ISO/IEC 19794 (data formats and interoperability) and ISO/IEC 19795 (performance evaluation), as well as related standards such as ISO/IEC 30107 (presentation attack detection) and ISO/IEC 24745 (biometric information protection). These standards have long been established in the field of fingerprint recognition and are continuously updated to address specific stages of the biometric process, including acquisition, processing, and matching. A typical example of such standardization is the requirement for fingerprint image resolution, which is commonly defined as 500 DPI for standard applications.

In the case of contact-based fingerprint sensors, maintaining a defined resolution is relatively straightforward, as the position of the finger is fixed on the sensor surface and the acquisition technology (e.g., optical or capacitive sensing) can be designed accordingly. In contrast, contactless acquisition does not constrain the position or distance of the finger, making precise control of image resolution difficult. Nevertheless, most fingerprint comparison algorithms assume a standardized resolution, typically 500 DPI (or up to 1,000 DPI for high-precision, forensic applications). If the input image does not meet the minimum required resolution, or if it deviates significantly from these expected values, the performance of the recognition algorithms may be severely degraded or the comparison may fail entirely. This effect is illustrated in Fig. 2, which presents examples of fingerprint images at different DPI levels.


Fig. 2. Comparison of images with different resolutions (left: 380 DPI, center: 500 DPI, right: 1,000 DPI) [5].

Given that contactless technologies are being used more and more frequently, the National Institute of Standards and Technology (NIST) has issued guidelines for the certification of such sensors. Crucially, every such sensor must meet the following requirements [6]:

1. The tested device must capture fingerprints within the maximum dimensions specified in the EBTS (*Electronic Biometric Transmission Specification* – a specification based on the ANSI/NIST-ITL 1-2011 standard, intended primarily for the FBI) for rolled fingerprints (EBTS P-2, 1.6 by 1.5 inches at 500 DPI).
2. The tested device must capture as much of the surface with ridges as possible, up to the size of a rolled fingerprint (capturing from nail to nail or a 180° angle relative to the finger axis).
3. If the device under test is capable of capturing only a multi-finger image, these must be separated into individual fingers for the purposes of conducting the tests described in this specification.
4. The device under test must operate at a target resolution of 500 DPI and must be capable of capturing and storing the image in 8-bit grayscale.
5. The device under test must store fingerprint images in a lossless format supported by NFRaCT (*NIST Fingerprint Registration and Comparison Tool*), and the images must not be subjected to any lossy compression prior to being saved in this format.

3. The use of mobile phones for fingerprint acquisition

Based on the certification requirements outlined above, the feasibility of using mobile phone cameras for fingerprint acquisition can now be examined. In this context, the third requirement is particularly relevant. Although it is theoretically possible to capture individual fingers separately, practical considerations – especially user convenience – make it more likely

that the entire hand, including multiple fingers, will be captured in a single image. This introduces a significant challenge, as standard camera applications are not designed to automatically distinguish and isolate individual fingers within such images. While manual separation of fingers is technically feasible, it would be impractical and inefficient in real-world use.

However, our experience from a previous project involving the TBS 3D FLY device, where deep learning techniques were applied to detect and extract individual fingers, was highly positive. The neural network demonstrated excellent performance, achieving a very high probability of accurate results.

Rules 1 and 4 are closely related to the fact mentioned above. The fourth rule is actually the requirement for a resolution of 500 DPI and saving in grayscale representation. The first rule specifies the size of the fingerprint image; specifically, it must be 4.1 × 3.8 cm. This rule is rather unsuitable for the situation described, if we consider that the average palm should therefore measure 20 × 10 cm. Furthermore, let's assume the phone will have a resolution of 15 MP (in the mid-range of mobile phones, resolutions are typically 50 MP). For the standard 4:3 aspect ratio, this results in 4,752 × 3,168 px – if we want to achieve 550 DPI at this resolution, we would need to capture an area of up to 22 × 15 cm.

This leaves a sufficient margin for error during scanning, both in terms of palm size and DPI resolution. Mobile phones easily meet these requirements. However, it must be noted that to comply with the resolution rule, the palm must be at a specific distance from the mobile phone (otherwise the DPI will change). In practice, this situation would need to be addressed using a ruler, a tripod, a verification app, or another method. If this were not the case, the person taking the image would have no certainty about the quality of the resulting image. The final condition of the fourth rule is bit depth, which is typically 8- or 10-bit per color (thus more than sufficient for conversion to 8-bit grayscale). However, the conversion to grayscale itself would have to be performed manually by the user.

The second rule concerns the size of the captured fingerprint area. Here, it is only necessary to ensure that the person being scanned cooperates and does not intentionally rotate their fingers to reduce the scanned area. The final, fifth, rule concerns the correct image format. However, standard tools fall short here, as images are saved in JPG format on Android and in HEIC format on iOS. Both of these formats are lossy, and without using a specialized app, it is not possible to obtain a photo in a lossless format (e.g., PNG) that would be supported by the NFRaCT app.

The penultimate point of this analysis is the lighting of the scanned scene. Although lighting is not explicitly mentioned in the rules, it is clear that if the (papillary) ridges cannot be seen due to insufficient lighting, identification will not be possible and the image will be unusable. Optical fingerprint scanners rely almost exclusively on the FTIR (*Frustrated Total Internal Reflection*) principle for capturing fingerprints – simply, the finger is illuminated from the side, which highlights the ridges better than direct illumination. This has two consequences:

1. even relatively intense illumination is not distracting (the light shines at an angle and only on a limited area for the finger, so the user hardly sees it at all),
2. device manufacturers have full control over the angle, type of lighting, and finger position. However, none of this applies to mobile phones.

As a consequence, image quality is highly dependent on ambient lighting conditions. Considering practical deployment, it is useful to examine worst-case scenarios. For instance, capturing images at night in an outdoor environment presents significant challenges. The smartphone flash is typically positioned close to the camera lens, resulting in direct illumination from a single point light source. When multiple fingers are captured simultaneously, this leads to uneven illumination, where some fingers may be overexposed while others remain underexposed. Although certain fingers may incidentally benefit from oblique lighting – partially resembling the principles of FTIR-based sensing – this effect is inconsistent and uncontrolled. While additional light sources, such as flashlights, may be used, achieving uniform and stable illumination across all fingers remains difficult in practice.

An even more challenging scenario arises when fingerprints are captured at night in environments with dynamic and intense lighting conditions, such as roads where emergency vehicles are present with active warning lights. In such situations, ambient illumination fluctuates rapidly, often combining strong blue, red, or orange light sources. The built-in flashlight of a smartphone is typically insufficient to compensate for these conditions, resulting in unstable illumination and, consequently, highly variable fingerprint quality.

Another important factor is the background. Ideally, acquisition should be performed against a dark, uniform, and matte surface. Textured backgrounds may interfere with segmentation and fingerprint detection algorithms, while reflective or bright surfaces can introduce unwanted reflections, reducing contrast and degrading ridge visibility. For instance, capturing fingerprints in environments such as snowy terrain may significantly worsen already suboptimal imaging conditions.

In summary, for mobile devices to meet the requirements for certified contactless fingerprint acquisition, the use of a dedicated application would be necessary. Such an application should ensure controlled image capture (including appropriate lighting and lossless formats), verify key quality parameters (such as dimensions, resolution, and sufficient coverage of the papillary pattern), and perform essential preprocessing steps (e.g., grayscale conversion and separation of individual fingers). Although fingerprint acquisition using standard mobile devices is technically feasible without these constraints, reliable use in sensitive applications – such as personal identification – requires clearly defined procedures and strict adherence to them. Furthermore, operators must be adequately trained to handle the inherent challenges associated with contactless acquisition.

4. The process of comparing fingerprints obtained using contactless technology

Up to this point, the discussion has primarily focused on the capabilities and limitations of the acquisition process itself. It has been established that, under certain conditions, mobile devices can be used for contactless fingerprint capture. In this section, we assume that fingerprint images have been successfully acquired using a mobile phone and that their quality is sufficient for subsequent comparison.

As noted earlier, existing interoperability standards are primarily designed for contact-based sensors. As illustrated in Fig. 3, there are significant differences between contact and contactless fingerprint images. Since most recognition algorithms are optimized for images acquired via contact sensors (as shown on the left in Fig. 3), contactless images must be appropriately processed to meet these expectations. The following discussion is therefore based mainly on recent studies published in 2021–2022, which focus on the performance and usability of contactless fingerprint recognition methods [7,8]. It should be emphasized that the transition from research prototypes to practical, standardized, and interoperable solutions is typically a gradual and time-consuming process; nevertheless, the referenced works provide a useful foundation for understanding current capabilities.

Fig. 3. On the left is an image from a touchscreen; on the right is a photo from a cell phone [7].

The entire preprocessing procedure for a fingerprint image, prior to the application of other standard methods used for fingerprint recognition, is shown in Fig. 4 and consists of the following four steps: (a) conversion to grayscale, (b) quality enhancement, (c) inversion and binarization (thresholding), (d) touch equivalent.

Fig. 4. The preprocessing of a contactless fingerprint image [7].

The initial step (a) consists of converting the acquired color image into a standard grayscale representation. In the subsequent step (b), various enhancement techniques may be applied, including both classical image processing methods and neural network-based approaches. The objective is to compensate for uneven illumination and contrast, improve image sharpness, and normalize intensity distribution. The resulting image is visually suitable for further processing. In this stage, flexion creases (i.e., regions where the finger bends) typically appear as dark structures. In the following step (c), color inversion is applied, resulting in these creases appearing as bright regions. Finally, step (d) involves binarization (thresholding), where the image is converted into a binary representation. This stage is often complemented by additional enhancement procedures commonly used in contact-based fingerprint processing [7].

The final step is to crop the image and obtain a final representation that is virtually identical to the image from the touch sensors. The reason for this cropping is simple: on a touch sensor, the skin deforms and creates an almost perfect plane, which is then captured. However, in the case of contactless scanning, no deformation occurs, and the image thus represents a view of the finger's conical-cylindrical shape. The ridges found at the edges of the fingers may be in significantly different positions due to deformation, which would affect the result of the subsequent recognition process. This cropping naturally affects the reliability of the comparison – currently, it is best to compare fingerprint images obtained using the same method (i.e., contact with contact, non-contact with non-contact) – in which case the final step would not be necessary. However, when relying on databases containing fingerprints obtained using the contact method, we must include this final step.

As noted in the previous section on certification, fingerprint acquisition using mobile devices typically involves capturing all fingers simultaneously within a single image. This introduces additional processing steps, beginning with the extraction of individual fingerprints (see Fig. 5). In the case of video-based acquisition, the captured frames are first transformed into the YCbCr (upper row) and HSV (lower row) color spaces. The Cr and H components are then analyzed, and Otsu thresholding [10] is applied to obtain binary masks (three images on the left). The intersection of these masks is illustrated in Fig. 6d, while subsequent analysis of the largest connected components produces the final segmented image shown in Fig. 6e. It should be noted that this procedure assumes a uniform, dark background; more complex backgrounds would significantly increase the difficulty of segmentation and reduce robustness.

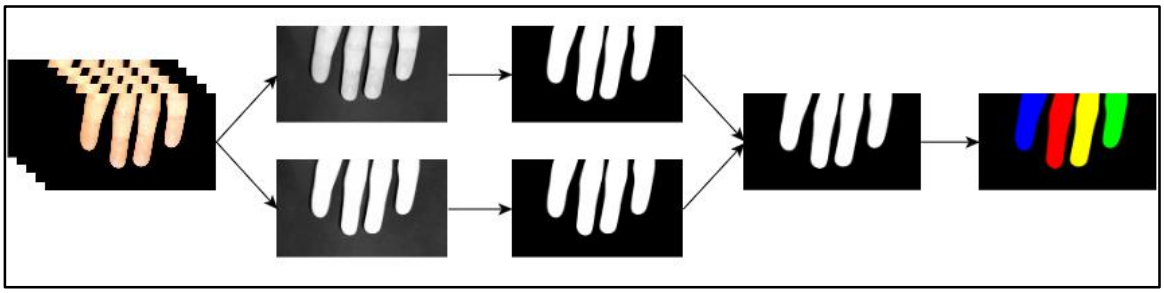

Fig. 5. Overview of finger detection (using video) [7].

The remaining task is to generate individual finger images comparable to those obtained from contact-based sensors, as illustrated on the left in Fig. 3. The procedure is depicted in Fig. 6. In step (b), the fingers are rotated to an upright orientation. Subsequently, in step (c), the image is segmented into individual fingers; it should be noted that insufficient spacing between fingers may significantly complicate or even prevent this process. In Fig. 6d, each segmented finger is further aligned to a vertical position. In the following step (e), only the upper portion of the finger, containing the fingerprint region, is cropped. The final step (f) involves size normalization, which compensates for variations in acquisition distance that lead to differences in image resolution (DPI), even when using the same mobile device. Ideally, this normalization adjusts the images to the standard resolution of approximately 500 DPI.

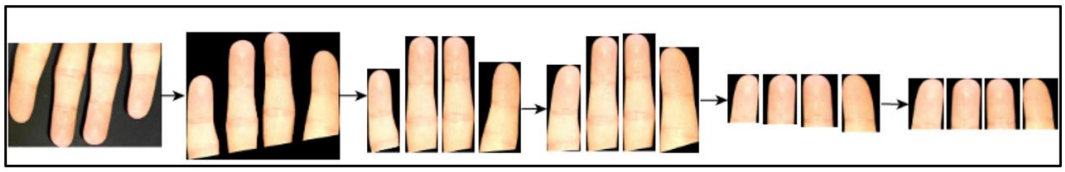

Fig. 6. Overview of the adjustments needed to create fingerprint images from a single image [7].

Next, we need to examine the quality of fingerprints obtained by placing the finger on the scanner in a contactless manner, using a stand, and in a contact manner (see Fig. 7). A comparison of quality (using the standardized NFIQ 2.0 tool) showed that the first method had an EER of 10.71%, the second method (using a phone) had an EER of 30.41%, and the third method (contact) had an EER of 8.19%. Taking photos using only a phone without a tripod would likely result in an even higher error rate. Although this is technically possible, this method of scanning has many pitfalls, including issues related to further image processing and comparison. [7]

Fig. 7. Example of scanning setups using various scanners (from left: contactless "box" scanner, phone on a tripod, touchscreen scanner) [7].

In [9], a complete work of conversion of fingerprints captured by a mobile device into a standardized format has been described. The proposed algorithm for converting fingerprints captured by mobile devices into a standardized grayscale format was implemented in C++ using the OpenCV library. A trained neural network was employed for detecting fingertip regions from hand images, enabling reliable extraction of regions of interest (ROI) for further processing.

The processing pipeline (see Fig. 8) consists of several consecutive image enhancement steps. After ROI extraction, background removal is applied, followed by contrast enhancement using the CLAHE method. Noise reduction is performed using a median filter, and intensity normalization is applied to standardize the image. Subsequently, ridge orientation and frequency are estimated, and a Gabor filter is used to enhance the ridge–valley structure of the fingerprint. This sequence of operations results in a grayscale image with emphasized papillary lines and suppressed noise, suitable for further biometric analysis. [9]

The algorithm was experimentally evaluated on a dataset comprising 26 hands (104 fingers). Various parameter configurations were tested, and the final setup was selected based on empirical optimization. The quality of fingerprints was assessed before and after processing using two independent evaluation methods: the standardized NFIQ 2 metric and the Innovatrics quality estimation algorithm. [9]

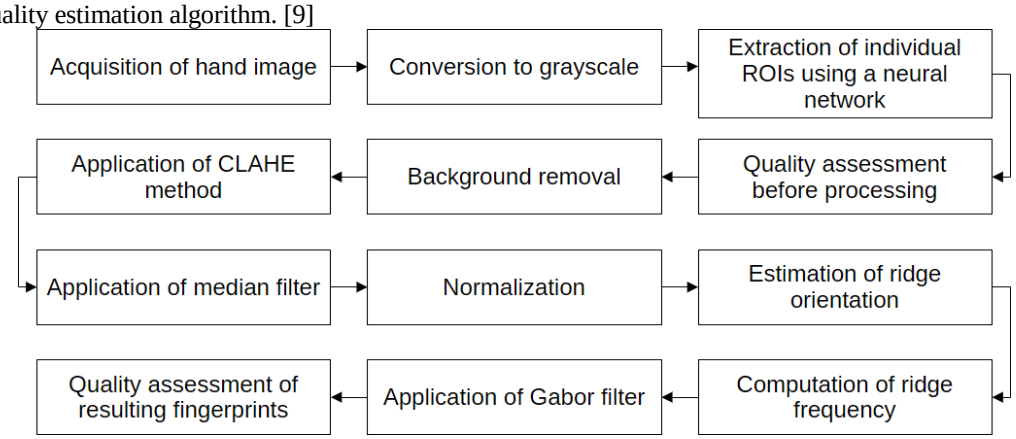

Fig. 8. Processing pipeline from capturing the image by a mobile device to a final standardized image [9].

The results demonstrate that the proposed processing pipeline significantly improves fingerprint quality according to the NFIQ 2 measure, with an average increase of 11.97 points (from 41.56 to 53.53). In contrast, the Innovatrics-based quality score showed a slight decrease of 1.20 points on average (from 58.15 to 56.95). Despite this discrepancy, both evaluation methods indicate that the processed fingerprints reach a quality level sufficient for reliable biometric comparison. [9]


Fig. 9. Examples of the fingerprints (from left): original; CLAHE; median filter; normalized; final [9].

Overall, the implementation confirms that appropriate preprocessing and enhancement techniques can substantially improve the usability of contactless fingerprint images acquired by mobile devices, although the effect may vary depending on the quality assessment method used. [9]

5. Security threat model and countermeasures

The deployment of mobile devices for contactless fingerprint acquisition introduces a range of security risks that extend beyond traditional contact-based biometric systems. Unlike controlled sensor environments, mobile acquisition is inherently unconstrained, making it more susceptible to manipulation, presentation attack, and variability in acquisition conditions. To systematically address these risks, this work adopts a threat model consistent with international biometric standards, particularly ISO/IEC 30107 (presentation attack detection, PAD), as well as related standards such as ISO/IEC 19795 and ISO/IEC 24745.

Threat model

According to ISO/IEC 30107, a presentation attack is defined as an attempt to subvert a biometric system by presenting an artificial or altered biometric characteristic to the sensor. The artifact used in such an attack is referred to as a presentation attack instrument (PAI). In the context of mobile contactless fingerprint acquisition, the range of possible PAIs is significantly broader than in traditional systems due to the lack of controlled sensing conditions.

A primary threat is the use of fingerprint presentation attack instruments (PAIs = spoofs), which represents one of the highest-risk attack vectors. These PAIs may take several forms, including printed fingerprint images, high-resolution displays showing fingerprint patterns, or physically fabricated replicas created using materials such as silicone, latex, or gel. Unlike contact sensors, which often rely on physical interaction or subsurface imaging, mobile cameras capture only surface appearance, making them inherently more vulnerable to such attacks. Furthermore, advances in imaging technology and publicly available high-resolution photographs increase the feasibility of reconstructing usable fingerprint patterns without the subject's consent.

Another critical threat is scale manipulation, which is particularly relevant in contactless acquisition. Since the distance between the camera and the finger is not fixed, an attacker may intentionally alter the scale of the captured fingerprint. This can lead to incorrect ridge frequency representation and may either degrade matching performance or, in some cases, produce misleading similarity scores. This type of attack is not typically considered in traditional PAD frameworks but becomes highly relevant in mobile scenarios.

The acquisition environment itself also represents a potential attack surface. Illumination manipulation, including overexposure, shadows, or colored lighting, can obscure ridge structures or introduce artifacts that affect both quality assessment and matching. Similarly, background interference may complicate segmentation and introduce noise that can be exploited to bypass simple preprocessing techniques.

Finally, replay and injection attacks must be considered in mobile systems, particularly when images are processed by external applications. An attacker may attempt to inject pre-captured or synthetically generated fingerprint images into the processing pipeline, bypassing the acquisition stage entirely.

Countermeasures

To mitigate the identified threats, the proposed pipeline incorporates several mechanisms that can be interpreted as implicit security countermeasures, even though they were originally designed for preprocessing and evaluation purposes.

A key component is DPI (resolution) estimation, which directly addresses scale-related vulnerabilities. By estimating the physical scale of the captured fingerprint using reference objects (e.g., rulers or calibration patterns), the system enforces consistency between the observed ridge frequency and expected biometric characteristics. This significantly reduces the feasibility of scale manipulation attacks, as artificially resized or projected fingerprints are less likely to conform to physically plausible parameters.

Segmentation and region-of-interest extraction also contribute to security by isolating the finger region and suppressing background artifacts. This reduces the attack surface for presentation attacks that rely on embedding fingerprint patterns within complex scenes or backgrounds. In combination with morphological filtering, this step improves robustness against visual noise and partial presentation attack attempts.

Another important element is the use of multiple independent quality assessment algorithms, including NFIQ, Innovatrics IDKit, and Neurotechnology VeriFinger. Each of these algorithms evaluates fingerprint quality using different criteria, such as ridge clarity, contrast, and structural consistency. Discrepancies between these quality measures can serve as indicators of anomalous inputs, including potential presentation attacks. For example, PAI artifacts may exhibit unnatural texture properties or inconsistent ridge patterns that are detected differently by each algorithm.

Similarly, the use of multiple matchers provides an additional layer of robustness. Genuine biometric samples are expected to produce consistent similarity scores across different recognition systems, whereas spoofed or manipulated samples may result in divergent outputs. Monitoring such inconsistencies can form the basis for decision-level PAD mechanisms.

From a broader perspective, the proposed framework aligns with the concept of multi-factor biometric validation, where decisions are not based solely on a single score but on a combination of quality, consistency, and plausibility checks. This approach is particularly important in unconstrained environments such as mobile acquisition, where no single method is sufficient to guarantee security.

Relation to ISO/IEC PAD Framework

Within the ISO/IEC 30107 framework, PAD performance is typically evaluated using metrics such as Attack Presentation Classification Error Rate (APCER) and Bona Fide Presentation Classification Error Rate (BPCER). While these metrics are not explicitly computed in this work, the presented pipeline establishes the necessary foundation for their future evaluation. In particular, the availability of normalized fingerprint images, quality metrics, and matcher outputs enables the definition of PAD decision criteria and the construction of evaluation datasets containing both bona fide and attack presentations.

Practical Implications

The results of this study indicate that, without appropriate countermeasures, mobile contactless fingerprint systems are highly vulnerable to presentation attacks and acquisition-related manipulations. However, by integrating scale normalization, multi-algorithm quality assessment, and cross-matcher validation, it is possible to significantly improve both performance and security.

For real-world deployment, additional measures should be considered, including:

- the use of dedicated calibration targets (e.g., fiducial markers) to improve scale estimation accuracy,
- controlled acquisition applications that enforce image format, resolution, and quality constraints,
- and integration of explicit PAD algorithms, potentially based on machine learning or liveness detection techniques.

6. Experimental evaluation

This work presents a two-phase pipeline for evaluating fingerprints acquired using mobile phone cameras against standard 500 DPI (equivalent to DPI; DPI will be used further in this subsection) dactyloscopic references. The primary challenge addressed is the absence of known physical scale in contactless fingerprint images, which significantly affects ridge frequency and, consequently, matching performance. To address this limitation, the proposed approach estimates the physical resolution (DPI) directly from the acquisition and subsequently evaluates biometric performance under normalized conditions.

The first phase focuses on *geometric* and *photometric preprocessing* together with *DPI estimation*. Input images are optionally *resized* to a bounded resolution to ensure stable processing. Finger *segmentation* is performed in the HSV color space, where skin regions are extracted while suppressing bright, low-saturation areas corresponding to the ruler or background. *Morphological filtering* and connected-component analysis are then used to isolate the dominant finger region. In parallel, *candidate reference objects are detected* using multiple complementary strategies, including luminance-based detection in the Lab color space, color-based filtering in HSV, and periodicity analysis supported by vertical Hough line detection. These candidates are evaluated, and the most plausible ruler region is selected.

Once a reference object is identified, it is *geometrically rectified* via perspective transformation to a canonical orientation. The rectified region is analyzed to detect periodic tick marks using vertical gradient profiles. Peaks corresponding to tick edges are identified, and their spacing is analyzed using robust statistical measures such as median spacing, autocorrelation lag, and median absolute deviation. Based on this analysis, the physical spacing between ticks is inferred and used to compute the pixel-to-millimeter ratio. This ratio is subsequently converted to DPI using the standard factor of 25.4 mm per inch. The estimated DPI is accepted only if it falls within predefined physical bounds, ensuring robustness against spurious detections. The output of this phase consists of masked grayscale fingerprint images with embedded metadata describing the estimated DPI, as well as optionally rescaled versions normalized to 500 DPI.

In the second phase, the biometric utility of the processed probes is evaluated against reference fingerprints with known resolution. The *evaluation pipeline* begins with file discovery and parsing of identity metadata, including user ID, finger ID, and acquisition attributes. Both references and probes are subjected to quality assessment using available tools, including NFIQ and matcher-specific quality estimators. In addition to a standard evaluation mode, a masked-rescale strategy is employed, in which multiple DPI variants of each probe are generated. For each probe, a shared optimal DPI is selected based on genuine matching evidence obtained from one of the matchers, and this DPI is then used for final evaluation across both matchers.

Pairwise comparisons are performed between all probes and references. Each comparison is labeled as genuine if both user and finger identifiers match, and as impostor otherwise. Matching is carried out using two independent matchers, and decisions are derived using fixed operating thresholds. Performance is summarized using standard biometric metrics, particularly the false acceptance rate (FAR) and false rejection rate (FRR), together with descriptive statistics of genuine and impostor score distributions. The evaluation results are aggregated by device type and processing variant to analyze the impact of acquisition conditions.

Experimental Results

The evaluation was conducted using the masked-rescale shared-DPI mode on a dataset comprising samples from two users, each contributing multiple fingerprint impressions across different devices. The resulting dataset contains 96 quality records, 108 match records, and 6 aggregated FAR/FRR summaries. The operating thresholds were set to 60 for the first matcher and 48 for the second matcher

Across all evaluated mobile devices, namely Samsung **A25**, **A71**, and **S25** (see fingerprint images from these phones in Fig. 10), the system achieved perfect empirical separation between genuine and impostor comparisons. For both matchers and all devices, the observed false acceptance rate and false rejection rate were equal to zero. Although these results indicate excellent performance, it should be noted that the number of comparisons per device is limited, and therefore the statistical confidence of these estimates remains constrained.

Fig. 10. Sample images of the user 1, from left: Samsung A25, Samsung A71, Samsung S25, dactyloscopic card.

A detailed analysis of score distributions reveals consistent improvements due to DPI normalization. For the A25 device, the average genuine score increased substantially for both matchers compared to the 500 DPI baseline, while impostor scores remained close to zero. Similar trends were observed for the S25 device, where both the average and minimum genuine scores improved after DPI normalization. For the A71 device, improvements were also observed for one matcher, while the second matcher showed comparable performance to the baseline.

In all cases, the minimum genuine scores increased after DPI normalization, indicating improved robustness for lower-quality samples. At the same time, impostor score distributions remained well separated from genuine scores, preserving a clear decision boundary. These observations confirm that accurate DPI estimation and normalization positively influence matcher performance by restoring correct ridge frequency and spatial relationships.

The results further highlight the sensitivity of fingerprint matching to geometric scale. Even small deviations in DPI can distort ridge spacing and reduce similarity scores. By compensating for these distortions, the proposed approach improves both average performance and worst-case behavior.

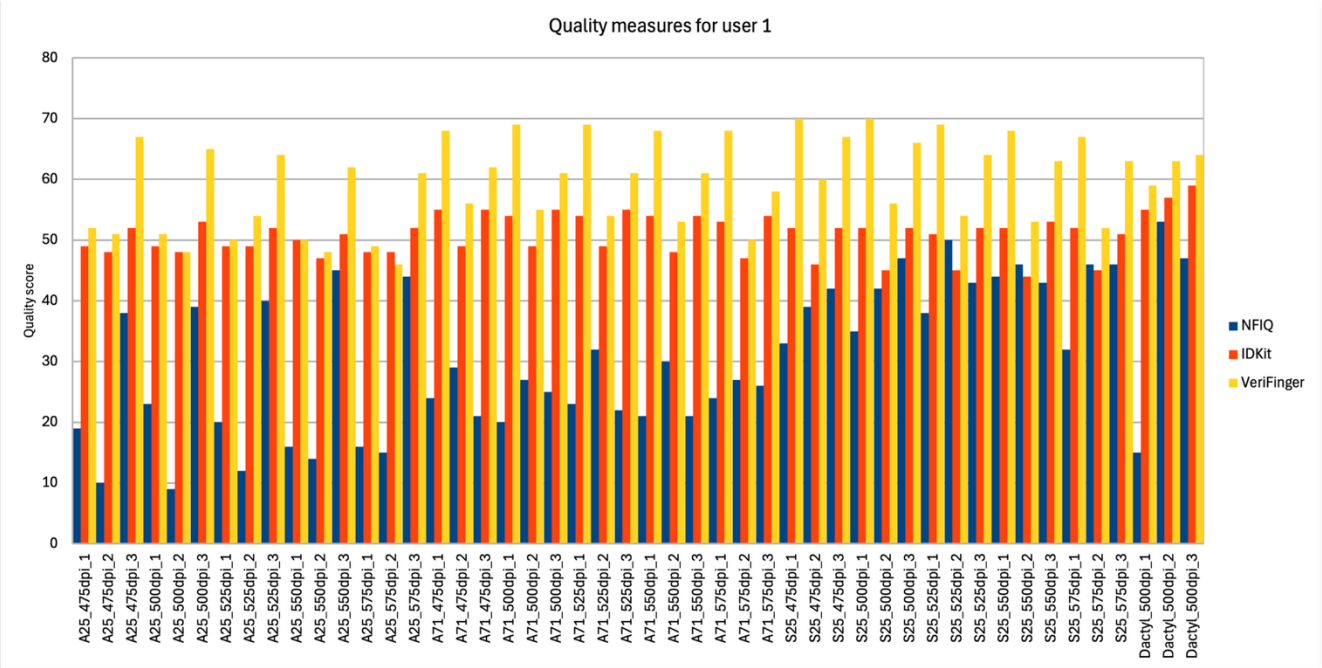

Fig. 11. Quality measures for user 1.

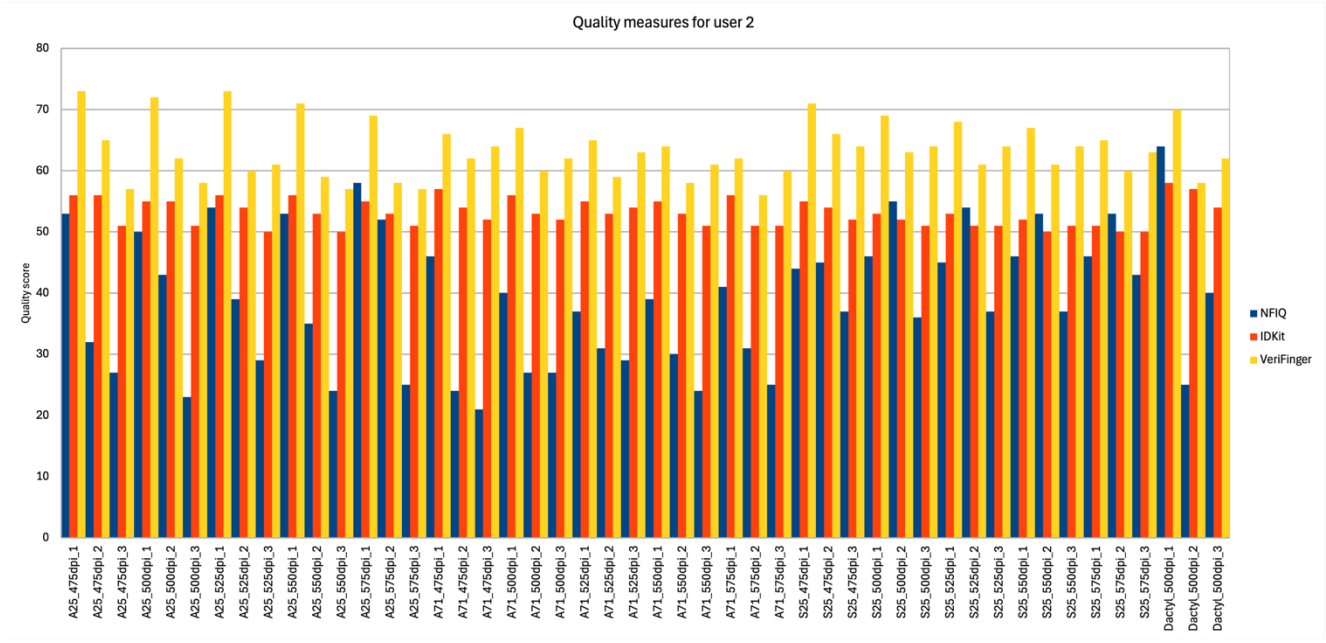

Fig. 12. Quality measures for user 2.

Quality Analysis

Image quality was evaluated using three complementary approaches (always last version were used): the NFIQ (NIST Fingerprint Image Quality) metric, together with matcher-specific quality scores produced by the Innovatrics IDKit and Neurotechnology VeriFinger recognition systems.

To further illustrate the quality characteristics of the evaluated samples, Figures 11 and 12 present representative quality measure distributions for two selected users. The figures 11 and 12 provide insight into the variability of image quality across samples and its relationship to matching performance. In particular, they highlight the consistency of quality estimates across rescaled variants and support the observed improvements in genuine matching scores.

Comparison Analysis

Fingerprint comparison was evaluated using two complementary approaches (always last version were used): matchers produced by the Innovatrics IDKit and Neurotechnology VeriFinger recognition systems.

Achieved results for FAR/FRR by phone model:

- Samsung A25
  - IDKit: *FAR*: 0.000000 (0/30); *FRR*: 0.000000 (0/6); *Genuine score*: min 216.0, avg 536.833, max 751.0; *Impostor score*: min 0.0, avg 0.0, max 0.0; *500 DPI genuine baseline*: min 197.0, avg 471.0, max 658.0.
  - VeriFinger: *FAR*: 0.000000 (0/30); *FRR*: 0.000000 (0/6); *Genuine score*: min 264.0, avg 589.167, max 906.0; *Impostor score*: min 0.0, avg 10.367, max 29.0; *500 DPI genuine baseline*: min 115.0, avg 379.833, max 685.0.
- Samsung A71
  - IDKit: *FAR*: 0.000000 (0/30); *FRR*: 0.000000 (0/6); *Genuine score*: min 395.0, avg 608.833, max 849.0; *Impostor score*: min 0.0, avg 0.0, max 0.0; *500 DPI genuine baseline*: min 279.0, avg 588.167, max 849.0.
  - VeriFinger: *FAR*: 0.000000 (0/30); *FRR*: 0.000000 (0/6); *Genuine score*: min 195.0, avg 818.500, max 1317.0; *Impostor score*: min 0.0, avg 10.600, max 31.0; *500 DPI genuine baseline*: min 94.0, avg 827.167, max 1317.0.
- Samsung S25
  - IDKit: *FAR*: 0.000000 (0/30); *FRR*: 0.000000 (0/6); *Genuine score*: min 121.0, avg 505.000, max 902.0; *Impostor score*: min 0.0, avg 0.0, max 0.0; *500 DPI genuine baseline*: min 56.0, avg 436.333, max 892.0
  - VeriFinger: *FAR*: 0.000000 (0/30); *FRR*: 0.000000 (0/6); *Genuine score*: min 265.0, avg 673.333, max 1052.0; *Impostor score*: min 0.0, avg 9.000, max 30.0; *500 DPI genuine baseline*: min 128.0, avg 438.0, max 857.0.

The presented results demonstrate that accurate estimation of physical scale is a critical factor in enabling reliable matching of contactless fingerprint images. The proposed pipeline effectively compensates for scale variability introduced during acquisition and significantly improves matching robustness. From a practical perspective, the placement of the reference object is essential; it should lie in the same physical plane as the finger surface to avoid perspective-induced errors. Deviations from this condition may introduce bias in the DPI estimate and degrade performance.

Despite the promising results, the evaluation is based on a relatively small dataset, and further validation on larger and more diverse datasets is necessary. Future work will focus on extending the evaluation protocol, improving robustness of reference detection, and exploring alternative calibration targets.

7. Conclusions

From a practical perspective, it is important to note that fingerprint recognition using mobile devices is already deployed in operational environments. For example, the Metropolitan Police Service (MPS) in the United Kingdom utilizes mobile fingerprinting solutions in the field. Although limited technical details of the system are publicly available, it is known that a dedicated INK application has been used since 2018 [11]. As of June 2023, approximately 750 devices – specifically iPhone SE smartphones – were in operation for this purpose [12]. These devices enable officers to capture fingerprints and compare them against national databases, such as IDENT1 (criminal records) and IABS (immigration records) [13].

Another relevant example is the case study "From Crime Scene to Identification in 3 Minutes," presented by Innovatrics at the "Advances in Forensics 2025" conference. This work demonstrates the practical capabilities of the Innovatrics ABIS multimodal biometric system, which integrates fingerprint, iris, and facial recognition technologies to support rapid identification processes [14].

At the same time, official reports, such as the 2024 biometric technology assessment issued by U.S. governmental authorities [15], highlight both the potential and current limitations of contactless biometric systems. While such technologies offer clear advantages in scenarios involving large populations or where hygienic considerations are critical, their widespread adoption is hindered by the lack of standardized interoperability between contactless and traditional contact-based fingerprints.

The analysis presented in this paper further demonstrates that, although mobile devices are technically capable of capturing fingerprint images, reliable and secure use requires careful consideration of multiple factors. These include acquisition conditions (e.g., lighting, background, and finger positioning), compliance with established standards (e.g., resolution requirements), and appropriate preprocessing to transform contactless images into a form suitable for comparison with existing databases.

A key contribution of this work is the proposed two-phase processing and evaluation pipeline, which addresses one of the fundamental challenges of contactless acquisition – the absence of known physical scale. By estimating image resolution (DPI) using reference objects and applying normalization, the method ensures consistency of ridge frequency and significantly improves matching performance. Experimental results demonstrate that such normalization leads to clear separation between genuine and impostor comparisons, achieving zero false acceptance and false rejection rates within the evaluated dataset. Although these results are promising, it should be noted that the dataset is limited, and further validation on larger and more diverse data is necessary.

From a cybersecurity perspective, the study highlights the high risk associated with presentation attacks, particularly the use of fingerprint presentation attack instruments. The unconstrained nature of mobile acquisition increases vulnerability to such attacks, as well as to other forms of manipulation, including scale distortion and environmental interference. The proposed framework contributes to mitigating these risks by incorporating mechanisms such as DPI consistency checks, multi-algorithm quality assessment (NFIQ, Innovatrics IDKit, and Neurotechnology VeriFinger), and cross-matcher validation. These elements provide a foundation for future integration of explicit presentation attack detection methods in accordance with ISO/IEC 30107.

In conclusion, mobile phones can be used for fingerprint acquisition; however, their reliable deployment in security-critical applications requires strictly controlled acquisition procedures, specialized software support, and adherence to standardized processing methods. Without these measures, the risk of errors and potential security vulnerabilities remains high. Future work should focus on improving robustness under unconstrained conditions, expanding experimental validation, and integrating advanced presentation attack detection techniques to ensure both performance and security in real-world applications.

Acknowledgements. The authors acknowledge the support of their respective institutions in enabling this research. We further thank Innovatrics for providing a complimentary license of the IDKit software, which was essential for the conducted experiments.

References

1. **Kleinman Z.** Politician's fingerprint 'cloned from photos' by hacker. BBC News, 2014, Available at: https://www.bbc.com/news/technology-30623611 [accessed on 2026-JAN-30].
2. **Geuss M.** Politician's fingerprint reproduced using photos of her hands. Ars technica, 2014, Available at: https://arstechnica.com/information-technology/2014/12/politicians-fingerprint-reproduced-using-photos-of-her-hands/ [accessed on 2026-JAN-15].
3. **Thomas J.** Fact-check: Can hackers steal fingerprints from selfies?. Euronews, 2024, Available at: https://www.euronews.com/my-europe/2024/04/29/fact-check-can-hackers-steal-fingerprints-from-selfies [accessed on 2026-JAN-30].

4. **Ganguli P.** The Hidden Danger in Your Victory Selfie: How Cybercriminals Can Exploit Your Fingerprints. LinkedIn, 2024, Available at: https://www.linkedin.com/pulse/hidden-danger-your-victory-selfie-how-cybercriminals-can-ganguli-yf6lc [accessed on 2026-JAN-12].
5. **Jain A.K., Chen Y., Demirkus M.** Pores and Ridges: High-Resolution Fingerprint Matching Using Level 3 Features. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pp. 15-27, 2007. ISSN 1939-3539 https://doi.org/10.1109/tpami.2007.250596.
6. **Orandi S., Libert J., Grantham J. et al.** Specification for Certification Testing of Contactless Fingerprint Acquisition Devices, ver. 1.0, NIST, p. 13, 2023, Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-339.pdf [accessed on 2026-JAN-30].
7. **Priesnitz J., Rathgeb C., Buchmann N. et al.** An overview of touchless 2D fingerprint recognition. *EURASIP Journal on Image and Video Processing*, 2021, https://doi.org/10.1186/s13640-021-00548-4.
8. **Priesnitz J., Huesmann R., Rathgeb C. et al.** Mobile Contactless Fingerprint Recognition: Implementation, Performance and Usability Aspects. *Sensors*, 2022, https://doi.org/10.3390/s22030792.
9. **Mucha V.** Převod otisků prstů nasnímaných mobilním zařízením do standardizovaného formátu – úpravy obrazu (Conversion of fingerprints captured by a mobile device into a standardized format – image processing). FEEC BUT, 2024, http://hdl.handle.net/11012/246465.
10. **Liu D., Yu J.** Otsu method and K-means. In: *9th International Conference on Hybrid Intelligent Systems*. IEEE, 2009. pp. 344-349, https://doi.org/10.1109/his.2009.74
11. **Say M.** Met Police develops mobile fingerprint device. UKAuthority. 2018, Available at: https://www.ukauthority.com/articles/met-police-develops-mobile-fingerprint-device/ [accessed on 2026-JAN-20].
12. Greater London Authority. Mobile Fingerprint Scanners. Available at: https://www.london.gov.uk/who-we-are/what-london-assembly-does/questions-mayor/find-an-answer/mobile-fingerprint-scanners-0 [accessed on 2026-JAN-20].
13. London Assembly. Use of Fingerprint Scanners in the Met. Available at: https://www.london.gov.uk/who-we-are/what-london-assembly-does/questions-mayor/find-an-answer/use-fingerprint-scanners-met-1 [accessed on 2026-MAR-26].
14. Innovatrics, Innovatrics ABIS. Available at: https://www.innovatrics.com/glossary/abis/ [accessed on 2026-FEB-03].
15. U.S. Department of Homeland Security, U.S. Department of Justice, White House Office of Science and Technology Policy. Biometric Technology Report, 2024, Available at: https://www.dhs.gov/sites/default/files/2024-12/24_1230_st_13e-Final-Report-2024-12-26.pdf [accessed on 2026-FEB-20].