applied sciences

MDPI

Article

Impact of Minutiae Errors in Latent Fingerprint Identification: Assessment and Prediction

Octavio Loyola-González [1], Emilio Francisco Ferreira Mehnert [2], Aythami Morales [3], Julian Fierrez [3], Miguel Angel Medina-Pérez [2,*] and Raúl Monroy [2]

[1] Altair Management Consultants Corp., 303 Wyman St., Suite 300, Waltham, MA 02451, USA; olg@altair.consulting
[2] Tecnologico de Monterrey, Carretera al Lago de Guadalupe, Km. 3.5, Atizapán, Estado de Mexico 52926, Mexico; A01020938@exatec.tec.mx (E.F.F.M.); raulm@tec.mx (R.M.)
[3] BiDA-Lab, Universidad Autonoma de Madrid, Ciudad Universitaria de Cantoblanco, 28049 Madrid, Spain; aythami.morales@uam.es (A.M.); julian.fierrez@uam.es (J.F.)
* Correspondence: migue@tec.mx

Abstract: We study the impact of minutiae errors in the performance of latent fingerprint identification systems. We perform several experiments in which we remove ground-truth minutiae from latent fingerprints and evaluate the effects on matching score and rank-*n* identification using two different matchers and the popular NIST SD27 dataset. We observe how missing even one minutia from a fingerprint can have a significant negative impact on the identification performance. Our experimental results show that a fingerprint which has a top rank can be demoted to a bottom rank when two or more minutiae are missed. From our experimental results, we have noticed that some minutiae are more critical than others to correctly identify a latent fingerprint. Based on this finding, we have created a dataset to train several machine learning models trying to predict the impact of each minutia in the matching score of a fingerprint identification system. Finally, our best-trained model can successfully predict if a minutia will increase or decrease the matching score of a latent fingerprint.

Keywords: latent fingerprint; identification; minutiae; biometric quality; human error; performance evaluation

check for updates

Citation: Loyola-González, O.; Ferreira Mehnert, E.F.; Morales, A.; Fierrez, J.; Medina-Pérez, M.A.; Monroy, R. Impact of Minutiae Errors in Latent Fingerprint Identification: Assessment and Prediction. *Appl. Sci.* **2021**, *11*, 4187. https://doi.org/10.3390/app11094187

Academic Editors: Larbi Boubchir, Elhadj Benkhelifa and Boubaker Daachi

Received: 30 March 2021
Accepted: 24 April 2021
Published: 4 May 2021

1. Introduction

In the last two decades, machine learning has attracted increasing interest in the research community, eager to automatize several processes in different application areas [1,2]. One of these areas is Biometrics [3–9], which aims to use several unique characteristics of the human body to automatically verify or identify people. From the several physiological traits of the human body, fingerprints hold the label of being the most reliable due to its uniqueness, permanence, acceptability, and collectability [2,3,5,10,11]. Fingerprints are considered genetically unique; up to now, there have been no reports of two individuals having the same fingerprint. Therefore, this biometric feature is widely used in several application fields, such as criminology, banking, and healthcare [2,12–15].

Fingerprints can be classified into impressions and latent fingerprints [6,7,16,17]. Fingerprint impressions are acquired under controlled conditions and have high quality. By contrast, latent fingerprints are unintentionally left by someone when manipulating objects and have a low quality [18] (see Figure 1). Similarly, the methodologies for comparing fingerprints have been clustered into two groups. On the one hand, fingerprint verification, which aims to verify an individual's identity from two given impressions in a fully automatized process. On the other hand, fingerprint identification, which aims to search a background database for impressions that are the most similar to a given latent fingerprint query usually related to forensic applications [12,19–22].

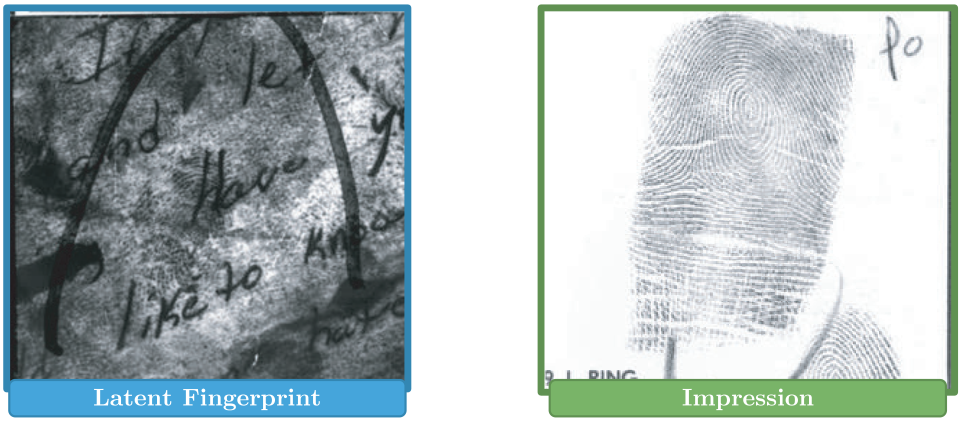


Figure 1. Example of a latent fingerprint and its corresponding impression, taken from the database NIST SD27 [23]. Notice how the latent fingerprint is a low-quality image, containing background noise that interrupts ridge flow. On the contrary, the impression is a clear and high-quality image taken under controlled conditions.

In 2006, in response to a misidentification of a latent fingerprint in a high profile case, the Federal Bureau of Investigation commissioned a review committee to evaluate the current state of forensic latent fingerprint identification technologies and processes and to better understand the bases of this discipline [24]. Their results showed that there are scientific areas where improvements in the practice can be made, particularly regarding validation, the analysis, comparison, evaluation, and verification (ACE-V) process, and data collection.

Fingerprint verification technologies based on digital impressions are dominated by fully automatic systems (e.g., smartphone authentication sensors). However, forensic latent fingerprint identification is usually performed through semi-automatic processes where human participation is still critical (e.g., minutiae labeling). Latent fingerprints are important evidence in thousands of real prosecutions all around the world. Together with DNA, the latent fingerprint is the most important biometric identification trait in these prosecutions. The main stages of latent fingerprint analysis are (a) reveal; (b) capture; (c) feature extraction, and (d) identification or matching. In nowadays forensic analysis, stages a to c are usually performed by human experts [25] while d is performed by automatic algorithms. These semi-automatic processes are error-prone; errors may originate either from a human or an algorithm. The analysis of these errors is critical to understand the performance of these systems. There are studies analyzing the likelihood of human errors in the stages a to c and showing these errors are habitual [26–29]. Nevertheless, there are not studies evaluating how these errors affect the identification stage, (d).

Minutiae extraction is a critical stage for any latent fingerprint identification system [13]. Usually, Automated Fingerprint Identification Systems (AFIS) work adequately for extracting minutiae from impressions but not for latent fingerprints. As a result, human fingerprint examiners are needed for extracting minutiae from latent fingerprints [21,22]. However, failing at marking minutiae or marking spurious minutiae can lead to misidentifying latent fingerprints, releasing criminals, or, even worse, yielding the apprehension of innocent people [21]. Recent studies [21,30] have shown that automatic fingerprint identification methods based on minutiae are often readily applicable and commonly outperform other types of methods. However, latent fingerprint identification rates are as low as 71.32% for Rank-1 when using medium-size databases (100,000 fingerprints) [30]. Consequently, latent fingerprint identification is an area of constant evolution, which aims to find new methods that help obtain better identification rates.

Based on the above discussion, three main research questions arise:

- What is the impact of human errors in the performance of Automatic Fingerprint Identification Systems?

- Are there minutiae having a higher impact on the identification performance when missed?
- If so, is there any feature of a minutia that can help determine its importance?

Aiming to develop methods that can help latent fingerprint examiners make better decisions with automatic methods as well as respond to the research questions mentioned above, in this paper, we propose to study how human error during minutiae extraction can affect the identification of latent fingerprints. By understanding the effect these mistakes have on matcher performance, we can identify research areas related to developing methods that seek to aid the latent fingerprint examiners.

The main contribution of this paper are summarized as follows:

- To the best of our knowledge, this is the first study related to the matching algorithms' performance when minutiae are missed from latent fingerprints.
- We quantify and discuss the impact of missing minutiae in the latent fingerprint on two latent fingerprint matching algorithms' performance by removing manually marked minutiae from latent fingerprints and calculating their matching score and rank, and comparing them to the original ground-truth latent fingerprints.

By removing minutiae from latent fingerprints, we simulate human mistakes. We show that even a single mistake could be fatal to the process. The variation in matching score when removing different minutiae leads us to believe that some minutiae are more important than others when it comes to latent fingerprint identification [13]. If we were able to determine the specific features of minutia that have a high impact on matching score, we could develop methods to aid latent fingerprint examiners by marking regions [31] where a mistake in feature selection would have a high negative impact in matching, in a kind of fingerprint quality map [18,32].

The remainder of this paper is organized as follows. In Section 2, we analyze previous works. After, in Section 3, we state the role of human errors in the forensic fingerprint analysis. Next, in Section 4, we define all our experimental setup. Then, in Section 5, we evaluate the impact of minutiae errors in latent fingerprint identification. Then, in Section 6, we experiment on predicting the utility of given minutiae for latent fingerprint identification. Finally, in Section 7, we present our conclusions and future work.

2. Previous Works

This section gives an overview of previous research that is closely related to ours. This includes the work done related to human performance in latent fingerprint minutiae extraction and matching, as well as the work related to the performance of fingerprint matching algorithms when the input is modified or distorted.

2.1. Research on the Performance of Experts in Latent Fingerprint Analysis

In this sub-section, we present works that study the performance of human latent fingerprint examiners when marking or matching latent fingerprints. These works are intended to show that even experts can make mistakes and serve as the motivation for our research on the effects of mistakes in this area.

In 2011, Ulery et al. studied the accuracy and reliability of forensic latent fingerprint decisions by using empirical approaches [26]. In particular, they studied how the quantity and quality of image features relate to the level of consensus among examiners and their decisions. The study of Ulery et al. was focused on determining the frequency of false-positive and false-negative errors, the extent of consensus among examiners, and factors contributing to variability in results. In such a study, 169 latent print examiners participated, who were generally highly experienced (83% of the participants were certified as latent print examiners). The data included 356 latent fingerprints, from 165 distinct fingers from 21 people, and 484 impressions combined finally making up 744 distinct latent-impression image pairs. Ulery et al. balanced the number of fingerprint pairs used in their study and the number of examiners assigned to each pair. As a result, 100 image pairs from the 744 image pairs were assigned to each participant examiner.

The results of Ulery et al. showed that, on the one hand, the false positive rate error (FPR) was 0.1%, and never two examiners committed an error on the same comparison. These results indicate that blind verification (between two examiners) should be highly effective at detecting this type of error, which demonstrates the potential of information fusion approaches in this problem [33,34]. On the other hand, the false-negative error was much more frequent (7.5% of mated comparisons). An in-depth analysis detected that 85% of the examiners committed at least one false-negative error. Using a blind verification would detect most of the false-negative errors; however, this blind verification is not generally practiced in operational procedures. After studying the quality of the latent fingerprints (quantity of features, distortion, background, among others) [18,35], this study could not identify the prints' features associated with false positive or false negative errors.

Later on, in 2015, Ulery et al. analyzed the changes in latent fingerprint examiners' markup [27]. The authors collected 320 (231 mated and 89 nonmated) image pairs of fingerprints constructed from 301 latent fingerprints and 319 impressions. Each one of the 170 volunteer latent print examiners was randomly assigned to analyze 22 pairs of fingerprints. From the 170 participants of this study, 89% were qualified as latent print examiners.

The experiments executed by Ulery et al. showed that from 41,774 minutiae labeled, 87% were retained, 6% were moved, 7% deleted, and 17% were added, see Figure 2. From these reports, the authors concluded that the comparison rates for inclusion or exclusion of minutiae ranged from 14% to 54%.

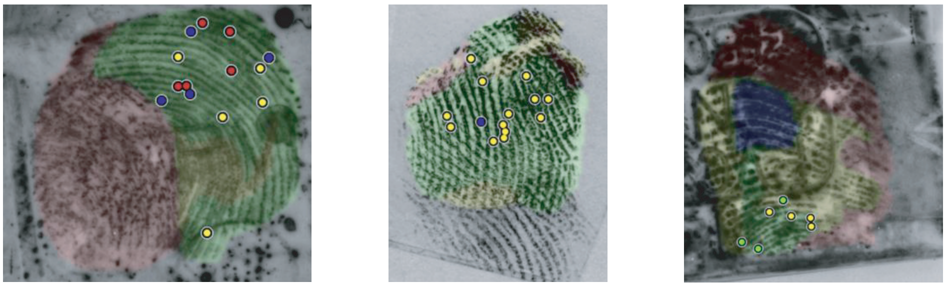


Figure 2. Example markups of latent fingerprints taken from Ulery et al. [27]. On each latent fingerprint image, the retained minutiae are in yellow, moved in blue, deleted in red, and added in green.

A detailed report of Ulery et al. showed that most of the latent fingerprint examiners (86%) included or excluded minutiae in the majority of their comparisons. When examiners were individualized (without checking by using double examiners), they changed their markup of minutiae in most comparisons. In addition, examiners included minutiae less frequently when the fingerprint image pair was nonmated than mated, being a possible explanation that the comparison with a mated exemplar draws attention to additional corresponding features in the latent. The authors claimed that the high variation in rates could be due to participants' unfamiliarity with the tested tools as well as the instructions and bringing casework habits. Next, in 2016, Ulery et al. analyzed the interexaminer variation of minutia markup on latent fingerprints [28]. Similar to [27], Ulery et al. [28] used 170 latent print examiners from which 89% got the qualification of latent print examiners. The dataset collected 320 fingerprint image pairs, 231 mated (from the same finger and person), and 89 nonmated (from different fingers or individuals). The image pairs were made with 301 latent fingerprints and 319 impressions. Each examiner was randomly assigned 17 mated fingerprint image pairs and 5 nonmated fingerprint image pairs. Their results were based on the analysis of 3730 fingerprint image pair, in total, among all the 170 latent print examiners, with a median of 12 examiners assigned to each fingerprint image pair.

Ulery et al. [28] also proposed to analyze whether examiners agree on the inclusion or exclusion of minutiae by measuring the minor variations in minutia location. For doing that, they used the Density-Based Spatial Clustering of Applications with Noise (DBSCAN) [36] to group minutiae such that more than two examiners agreed they are the same on the latent fingerprint. In this way, as shown in Figure 3, clusters are labeled as a singleton (marked by only one examiner), minority (<50% of examiners), majority (50–90%), and supermajority (≥90%).

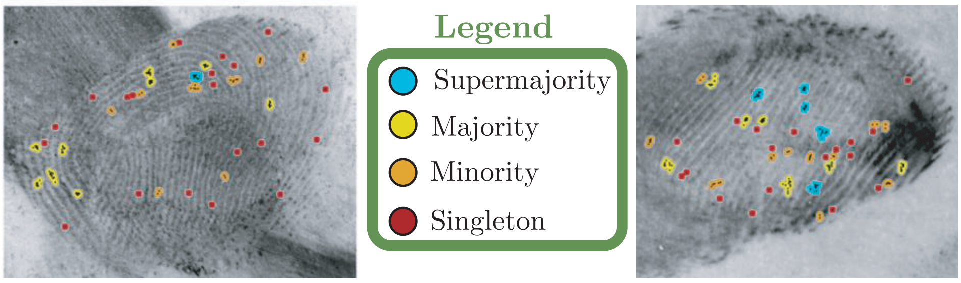


Figure 3. Two examples of latent fingerprints marked by several examiners, taken from [28]. Marked minutiae are shown as small black dots inside color-coded clusters. Singleton (marked by only one examiner), minority (<50% of examiners), majority (50–90%), and supermajority (≥90%).

The results of Ulery et al. showed that 66% of minutiae were reproduced by most examiners, 67% of the singleton clusters were in unclear areas of the fingerprints, and 98% of supermajorities were clear areas. After an analysis, the authors identified several factors that affect that several examiners can reproduce the same minutia in a fingerprint: clarity, region of interest, feature type, and location. Authors also claimed that a difference in minutiae markup could be due merely to a difference in how an interpretation is documented by an examiner.

Recently, in 2020, Kukucka et al. studied the impact of evidence lineups on fingerprint expert decisions. Their experiment involved the participation of 43 latent fingerprint examiners, at an average age of 44 years, most of them affiliated to a large laboratory. In the experiment, each examiner viewed four fingerprints, some of which belonged to a suspect. Fingerprints came from a crime scene, visited by the examiners, as the underlying hypothesis of Kukucka et al. is that an examiner could associate each latent fingerprint to a crime scene. Their results have shown that examiners made a positive identification of 37.8% for displayed images; by contrast, 25.6% images were classified as inconclusive. The main drawback of [29] is that examiners were aware of being part of a monitored study. This may explain why the study output an unusually high rate of inconclusive judgments attributed to suspicion of examiners aware they were under assessment. The study proposed by Kukucka et al. is more for the implementation of evidence lineups than for analyzing the fingerprint from a dactyloscopy point of view. As a consequence, fingerprint features such as minutiae, pore, core, among others, were not analyzed.

In summary, existing research has focused on studying human errors during the latent fingerprint markup. However, it has not considered the impact of missing minutiae on the score of matching algorithms or on the ranking results.

2.2. *Impact of Fingerprint Variations in Automatic Fingerprint Recognition*

In this section, we present an analysis on the performance of fingerprint identification systems in the presence of different distortions.

Studying the impact of fingerprint variations on fingerprint identification has attracted some attention in the last two decades, including position variability [35] and other distortions [10].

The most up-to-date and comprehensive work in this regard may be Grosz et al. [37], who performed a white-box evaluation of three fingerprint matchers so as to assess how different perturbations in fingerprints affect the matchers' scores. Of these algorithms, one, called SourceAFIS, was open-source and the other two were unnamed, minutiae-based commercial-off-the-shelf (COTS) matchers. Authors evaluated the robustness of these matchers against controlled perturbations of the fingerprints, specifically perturbations of minutiae sets. The fingerprint dataset used in this experimentation consists of fingerprint impressions, synthetically generated through SFinGe [38]. It is composed of 5000 different "master" fingerprints, each of which was used to generate two different impressions. For performance evaluation, Grosz et al. also generated a ground-truth minutiae set for each fingerprint.

Authors ran experiments where fingerprint impressions involved the following perturbations: (i) moving and rotating minutiae; (ii) adding spurious minutiae and removing ground-truth minutiae; (iii) considering a non-linear distortion of the minutiae sets; and (iv) combining the displacement and rotation of minutiae with the addition of spurious minutiae and removal of ground truth minutiae. The first two perturbations were generated by using a multivariate Gaussian Distribution model, which had parameters the researchers considered to model real possible perturbations. The non-linear perturbations were generated by using a non-linear distortion model learned from distorted fingerprints. Using these distortions, the authors performed two different experiments: (a) an analysis of uncertainty resulting from realistic amounts of perturbation and distortion; and (b) an evaluation of the recognition performance of each minutia-based matcher on increasing levels of perturbation and distortion.

To perform the uncertainty analysis, Grosz et al. generated 100 perturbations per perturbation type, per generated fingerprint. They obtained similarity scores and used them to calculate a global uncertainty score relating to each perturbation type. When performing the second experiment, the authors increased the perturbation parameters throughout eight iterations. The results of this experiment are reported as true acceptance rate at a fixed false acceptance rate of 0.01%. They also calculated impostor scores for each perturbation type, on each iteration. The authors found out that the non-linear distortion is the perturbation that reduced the mean of the similarity scores the greatest, followed by the combined perturbation, and after that, the removal of ground truth minutiae. The experiments suggested that the fingerprint identification algorithms are robust to elevate percentages of missing minutiae. The large number of minutiae in these experiments allows to maintain a competitive identification performance after missing minutiae.

3. Forensic Fingerprint Analysis: Role of Human Errors

This section introduces the main errors a human may incur in before and during the entire fingerprint identification process, possibly yielding misidentifications (see Figure 4).

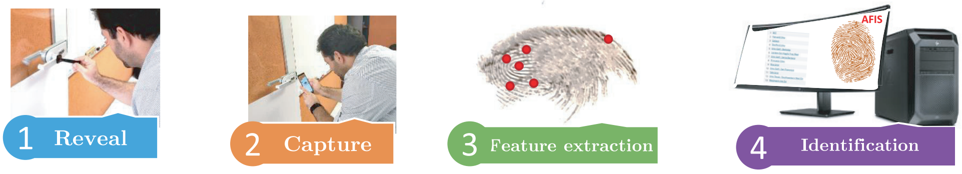


Figure 4. Four stages before and during the fingerprint identification where the human errors could produce misidentification.

Latent fingerprint identification is composed of four main stages, namely: reveal, capture, feature extraction, and identification. The more common errors typically observed at each one of these stages are as follows [16]:

Reveal: in this stage, an expert should use specific powders, based on the surface and shape of the object, to reveal the latent fingerprint. The errors one may incur at this stage are:

- Using a revealing powder that does not correspond to the surface or shape of the object where the latent fingerprint is, which could wrongly reveal the ridges of the latent fingerprints.

- Using more revealing powder than necessary, creating a filling among the fingerprint ridges, and consequently, making it hard to be of use on the next stages.

Capture: in this stage, an expert must be careful at capturing the latent fingerprint under the best possible conditions. Errors that are typically observed at this stage are:

- While lifting the latent fingerprint, deformations might be created in the ridges creating false bifurcations or false ends on the ridges. As a result, errors are induced that may severely affect the feature extraction stage.
- Output an out of focus or low-resolution photo of the latent fingerprint.
- Lack of use of a rule next to the latent fingerprint that may enable one to estimate the real scale of the fingerprint.

Feature extraction: during this stage, the examiners will extract all features necessary for the identification stage. The more common flaws one may experience at this stage are:

- False features can be added from errors originated at the capture stage.
- Actual features could be missed by examiners.
- The position or angle of some features could be shifted due to human perception.

Identification: any flaw committed at previous stages will affect identification performance. However, the main errors that may show up at this stage are:

- The ranking provides the corresponding impression, but the experts obviate this matching.
- The ranking does not provide the corresponding impression due to human errors issued at the previous stages.
- The expert issues a true positive identification when really it is a false positive.

All the human errors previously described above negatively affect the identification rate. One of the most important features for fingerprint identification is minutiae. A minutia is a minute detail on the ridges of a fingerprint, often ridge ending or bifurcation. Minutiae are one of the most used features for fingerprint identification [5,21,22]. Hence, we will analyze minutiae's impact on fingerprint identification and the matching algorithms upon the possible appearance of human errors.

4. Materials and Methods

This section describes the database used and its characteristics. After, the two tested matching algorithms are presented. Finally, our experimental setup is presented.

We used the database NIST SD27 [23], which is a public database widely used in latent fingerprint studies [13,39]. NIST SD27 contains images of 258 latent crime scene fingerprints with their manually marked minutiae, as well as their matched tenprint impressions with their extracted minutiae. The average number of minutiae in latent fingerprint images in NIST SD27 is 20, while the average number of minutiae in the corresponding impressions is 106.

Additionally, for some experiments, we used the NIST SD4 [40] as a background database. This database contains images of 2000 rolled fingerprints.

For determining the impact of our study on fingerprint identification, we used two matching algorithms that have demonstrated highly competitive performance in latent fingerprint identification:

- Minutia Cylinder-Code (MCC) [41]: Matching algorithm based on a three-dimensional representation constructed using basic minutiae features such as angles and distances to other minutiae.
- Deformable Minutiae Clustering using Cylinder-Codes (DMCCC) [19]: A matching algorithm independent of minutiae descriptors based on the use of clustering to improve robustness to non-linear transformations. In this case, we use Minutia Cylinder-Code as the minutiae descriptor.

We used CMC [42] curves as an evaluation measure adopting the norm ISO/IEC 19795-1, which indicates that CMC curves should be used for closed-set identification. As numerical measures of the CMC curve, we use from Rank-1 to Rank-100 identification rates. Notice that these ranks quantify the ratio of correct identifications in the first place and among the 100 first ranks, respectively, returned by an identification algorithm.

Our protocol consisted of *three sets of experiments* in which we removed minutiae from fingerprints and evaluated the impact of such minutiae removal on the two selected matching algorithms *plus a final prediction experiment*:

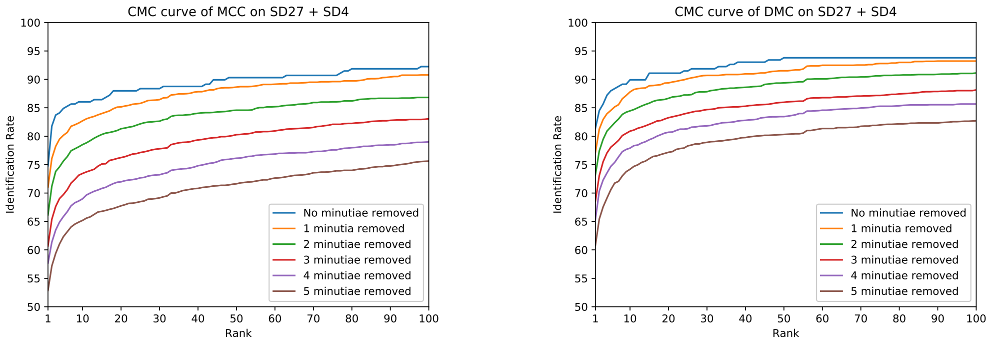
1. The first set of experiments consists of randomly removing minutiae from latent fingerprints in the database and comparing the resulting CMC curves in a closed set comparison. We ran 35 experiments; the first 20 experiments consisted of removing a fixed number of minutiae from each latent fingerprint, from 1 to 20. The next 15 experiments consisted of removing a percent of minutiae from each latent fingerprint, from 0.1% to 0.75%. Each experiment was run 10 times with different randomly-selected removed minutiae, and the results of the 10 experiments are then averaged.
2. The second set of experiments aims to measure the matching algorithms' negative impact when minutiae are removed. We remove every possible combination of one, two, and three minutiae from every fingerprint (more than 1,100,000 combinations for all fingerprints in the NIST SD27) for this set of experiments. Every new fingerprint (with the removed minutiae) was tested with the two selected matching algorithms to obtain their matching score and compared with the matching score obtained from the original fingerprints (without removed minutiae).
3. The third set of experiments consists of determining the set of minutiae that less decreased the score and those that decreased the most the score. Using our second experiment results, we selected six combinations of minutiae for each fingerprint and each matching algorithm to see how the change in score is reflected in the CMC curve and the rank-100 identification. The three combinations which lowered the score the most are considered the "lower" class. The three combinations which lowered the score the least are considered the "higher" class.
4. Finally, we perform one last experiment aimed to determine if it is possible to predict if removing a minutia will have a positive or negative effect on the matching score.

It is important to highlight that, for all experiments, the minutiae were not removed from fingerprints if a fingerprint was to be left with less than six minutiae, based on what INTERPOL recommends as a minimum for an AFIS [43].

5. Evaluating the Impact of Minutiae Errors

This section shows the experimental results obtained when removing fixed and variable numbers of random minutiae from each latent fingerprint.

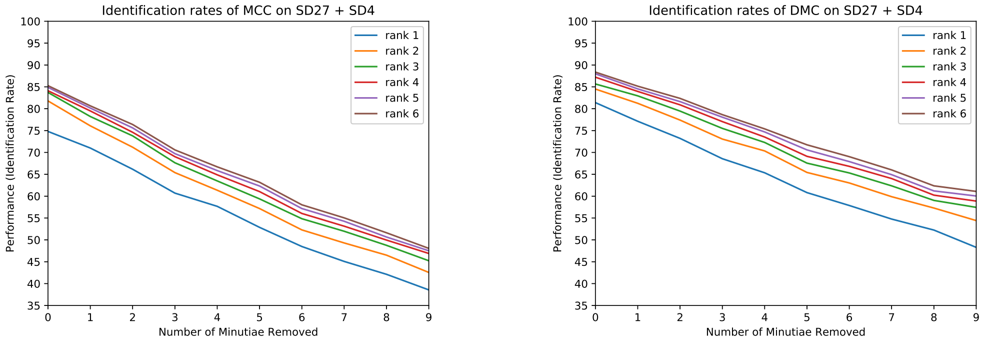
For our first set of experiments, Figure 5 shows CMC curves for random fixed number removal of minutiae using both MCC and DMC as matching algorithms. From this figure, we can see how both matching algorithms degrade for the increasing number of minutiae removed. In addition, notice that MCC obtains worse identification rates than DMC regarding each CMC curve plotted. From these results, we can see that no matter the matching algorithm used, the identification rate is affected when minutiae are randomly removed from latent fingerprints. The drop of performance varies depending on the matching algorithm, but it is consistently high with rank-n identification degradation higher than 5% for each minutia removed.



(**a**) (**b**)

Figure 5. CMC curves for random fixed number removal of minutiae using both MCC and DMC as matching algorithms. (**a**) CMC curves for random fixed number removal of minutiae using MCC as matching algorithm. (**b**) CMC curves for random fixed number removal of minutiae using DMC as matching algorithm.

Figure 6 shows the same results from Figure 5 in a different representation. From Figure 6, we notice that the identification rate decay proportionally to the number of minutiae removed. We can also see that rank one is more affected when minutiae are removed than the remaining ranks (from 2 to 6). In addition, we can notice that MCC's identification rates are more affected than those of DMC regarding the number of minutiae removed and the ranks analyzed.

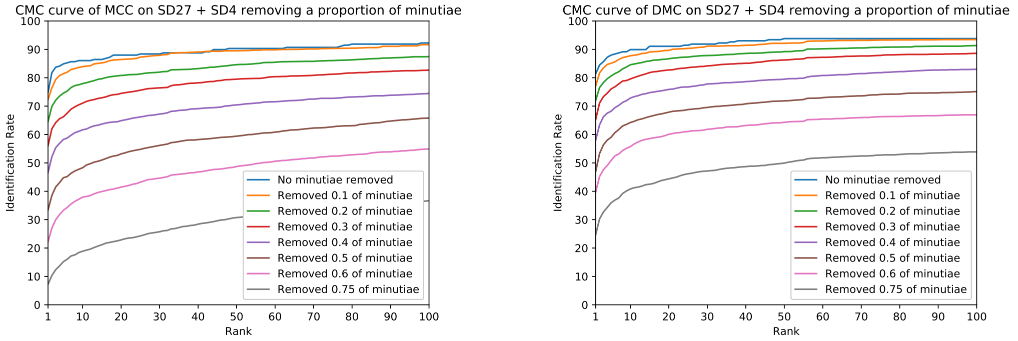


(**a**) (**b**)

Figure 6. Curves showing the identification rates of both MCC and DMC matching algorithms when a random number of minutiae are removed. (**a**) Curves showing the MCC matching algorithm's identification rates when a random number of minutiae is removed. (**b**) Curves showing the DMC matching algorithm's identification rates when a random number of minutiae is removed.

From our first set of experiments, we noted that the identification rate depends on both the number of removed minutiae and the total number of minutiae. Consequently, another essential experiment is to test removing a percentage of minutiae from each latent fingerprint.

For our second set of experiments, Figure 7 shows CMC curves for random proportion removal of minutiae using both MCC and DMC as matching algorithms. From this figure, notice that the identification rate decays very fast, with rank-n identification rate differences of 12% for a ratio of 0.2 missed minutiae. In addition, from Figure 7, we can see that the identification rate obtained by MCC (Figure 7a) is worse than the identification rate obtained by DMC (Figure 7b). These results suggest that the characteristics of the matching algorithm can serve to alleviate this drop in performance partially.



(**a**) (**b**)

Figure 7. CMC curves for random proportion removal of minutiae using both MCC and DMC as matching algorithms. (**a**) CMC curves for random proportion removal of minutiae using MCC as matching algorithm. (**b**) CMC curves for random proportion removal of minutiae using DMC as matching algorithm.

From our second set of experiments, we noted that some minutiae affected the matching scores differently than others. In addition, on the one hand, 2/3 of the minutiae lowered the matching score when removed. On the other hand, 1/3 of the minutiae have a null effect or even a small improvement of the matching score when removed when compared to the base score (no minutiae removed).

From the results obtained in our second set of experiments, we concluded that some minutiae are more critical for identification, but we still do not know why they are more important than others. The next experiment is performed to characterize minutiae that lower the matching score and compare them to the remaining minutiae to determine the reasons for this negative impact.

Using the results of our second set of experiments, we selected the 6 minutiae combinations of sizes one, two, and three that had the largest impact in matching score for each latent fingerprint and each matching algorithm to see how the change in scores reflected in the CMC curve and from the rank-1 to rank-100 identification.

The six combinations for each fingerprint and matching algorithm were determined by taking the three combinations of minutiae that lowered the score the most ("lower" class) and the three combinations of minutiae that raised the most ("higher" class). Figure 8 shows a latent fingerprint taken from NIST SD27 [23], which contains the minutiae labeled as "higher" class in green color, those labeled as "lower" class in red color, and the remaining minutiae in blue color. From this figure, we can see that those minutiae labeled as "lower" class are well separated from those labeled as "higher" class. In addition, we can notice that the sum of the score of all "lower" class minutiae (−0.1728) affects more negatively the identification score than the sum of the score of all "higher" class minutiae (0.0665).

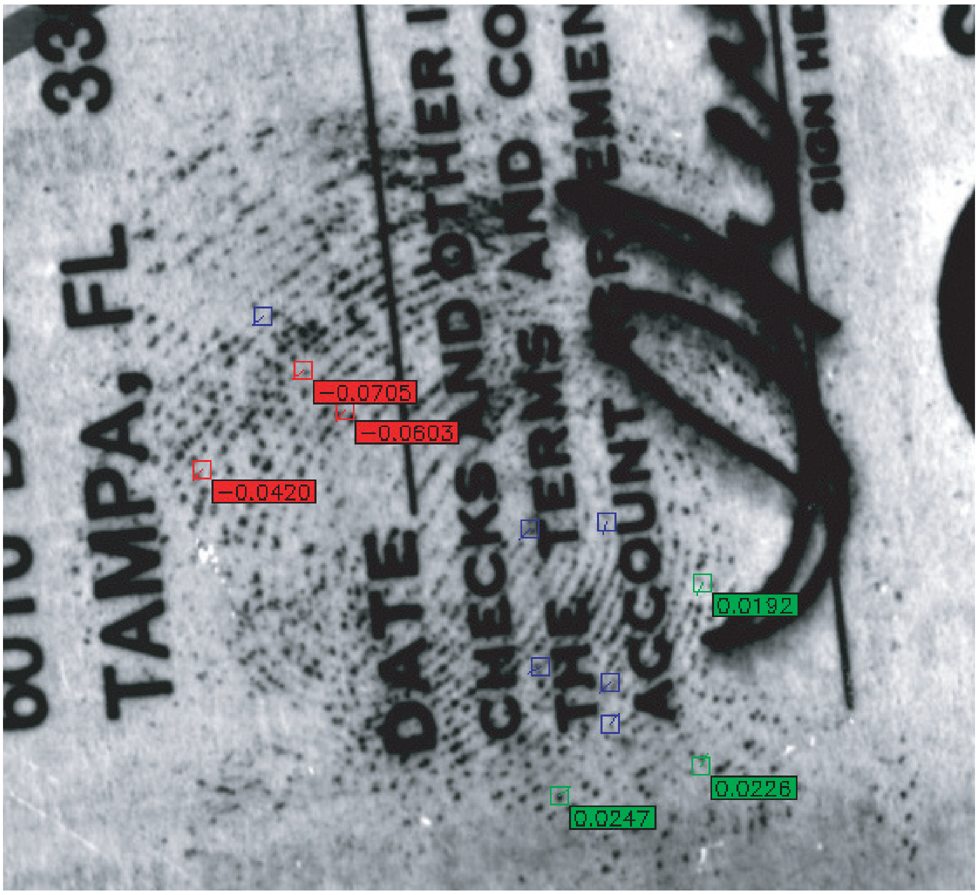


Figure 8. Example of a latent fingerprint taken from NIST SD27 [23]. Minutiae labeled as "higher" class are in green color, those labeled as "lower" class are in red color, and the remaining minutiae are in blue color. In both "higher" and "lower" classes, the minutiae contain the score difference that they introduce to the final score when that particular minutia is removed.

Table 1 shows percentages in which there was a rank drop considering only those minutiae labeled as "higher" class. Table 2 shows percentages in which there was a rank drop taking into account only those minutiae labeled as "lower" class. Notice that for both tables, MCC obtained worse identification rates than DMC. In addition, in Table 2, the identification rates were most affected when those minutiae labeled as "lower" class were removed.

Table 1. Percentages in which there was a rank drop taking into account only those minutiae labeled with the class "higher."

Num. Minutiae Removed	#MCC	#DMCCC
1	−5.53%	−3.37%
2	−3.86%	−0.69%
3	−3.86%	−0.57%

Table 2. Percentages in which there was a rank drop taking into account only those minutiae labeled with the class "lower."

Num. Minutiae Removed	#MCC	#DMCCC
1	−35.63%	−27.67%
2	−48.76%	−42.84%
3	−60.80%	−55.65%

Our third set of experiments shows how the identification rate is affected when those minutiae labeled as "lower" class are removed.

Figure 9 shows a histogram of rank loss of MCC when removing the minutiae of the "lower" class. From this figure, we can notice how removing minutiae labeled as "lower" class can affect the MCC rank value with variations up to 2000 positions in a ranked list. It means that a fingerprint ranked in the top 50 positions can easily drop to top 1000. These results demonstrate the high impact of these errors in the performance of fingerprint identification systems. In this figure, we can see, as expected, that the more minutiae are removed, the higher the rank loss. Notice that when only two or three minutiae are missed, the drop is severe for a large number of fingerprints.

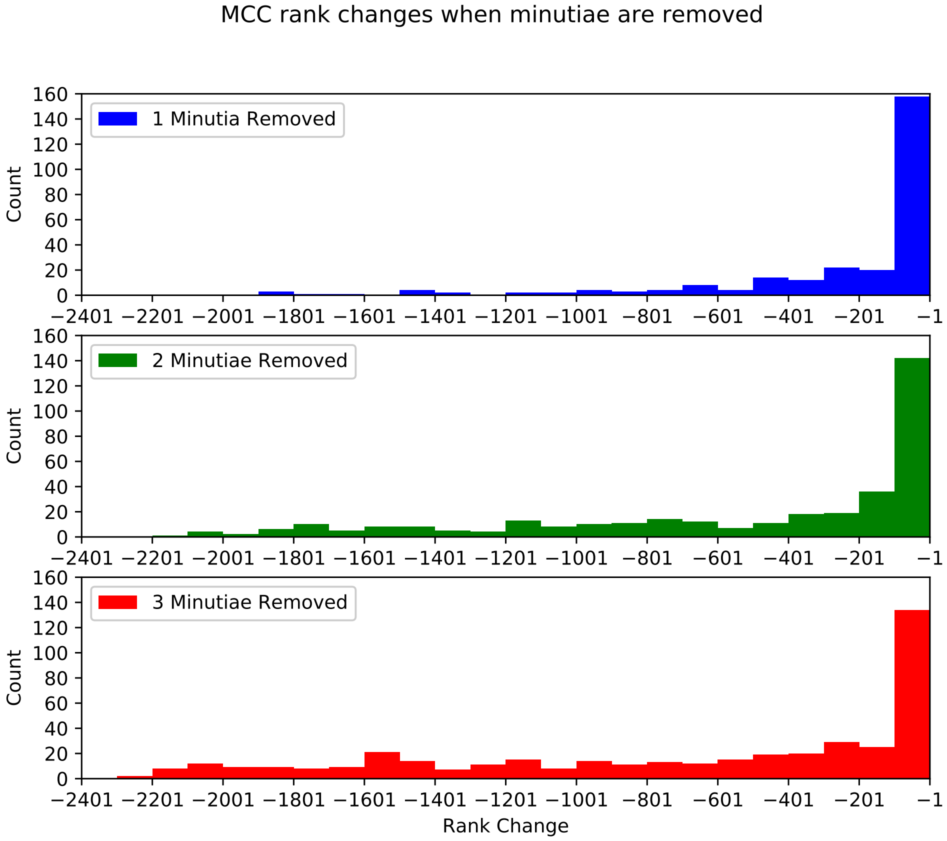


Figure 9. Histogram of rank loss for "lower" class regarding MCC.

Figure 10 shows a histogram of rank loss regarding DMC when "lower" class minutiae are removed. Contrasting the results obtained by Figures 9 and 10, we can see that the matching algorithm DMC is less affected than MCC when minutiae labeled as "lower" class are removed. However, notice that when two or three minutiae are removed the histogram is still highly affected.

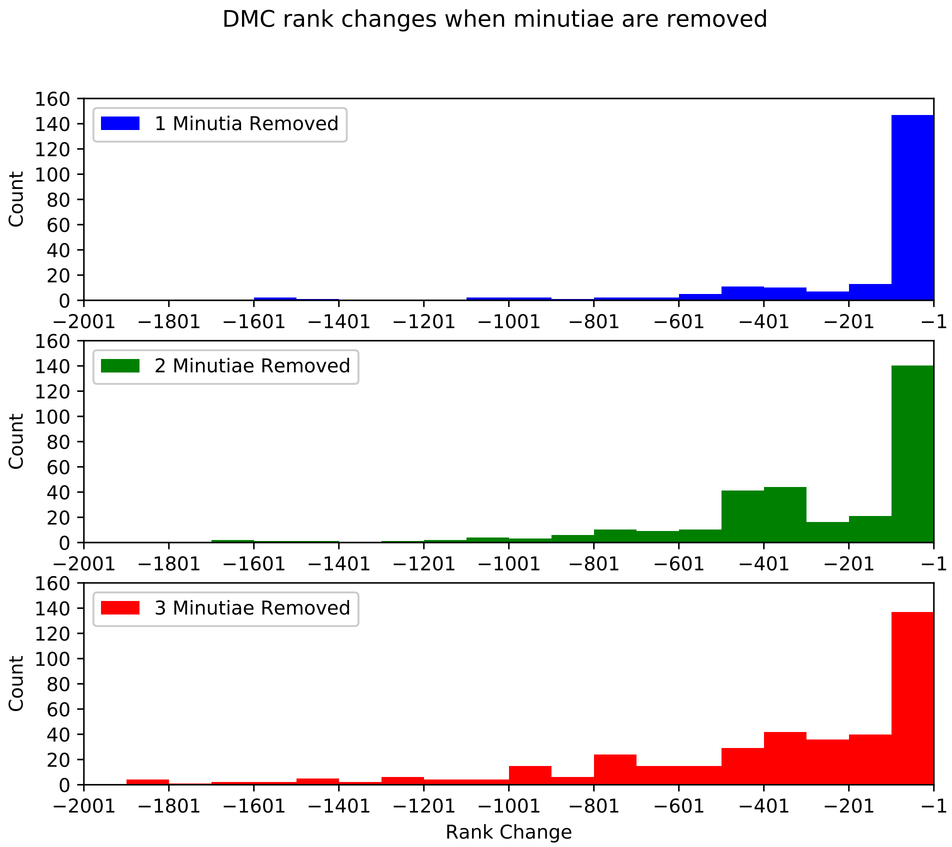


Figure 10. Histogram of rank loss for "lower" class regarding DMC.

6. Predicting the Impact of Minutiae Errors

In the previous section, we showed that removing minutiae can decrease or increase the score of fingerprint matching algorithms. If we could automatically predict the impact of the minutiae in the score before performing latent fingerprint identification, we could: (1) help the forensics experts to improve their minutiae labeling process to maximize the probability that they find minutiae that lead to successful latent fingerprint identification [16], and (2) improve automated algorithms for latent fingerprint processing and recognition using quality-based processing [44] and quality-based information fusion [45–47]. With these goals in mind, we developed a framework to determine if it is possible to predict if a given minutia will have a positive or negative effect on the score of fingerprint matching. Thus, we could develop tools for forensics examiners to automatically classify regions by its impact on the performance of the identification algorithm, or quality-based algorithms for latent fingerprint processing [45,46].

This framework was created by using the results of removing every possible combination of one minutia from a fingerprint, as described in the previous section for the DMC matcher. We created features based on the location of each minutia and the distances of neighboring minutiae. We designed two different types of features: (1) the first type counts the number of minutiae in a radius neighboring the specified minutia, and (2) the second type is the distance from the specified minutia to the n closest minutia. Finally, the class values *positive* and *negative* were used for minutiae that, after being removed, increased or decreased the matching score, respectively. In the end, each datum point in the created dataset has the following information:

- d[1–6]: Each of these features has the distance from the minutia to the closest minutia (d[1]), to the second closest minutia (d[2]), and so on.
- r[15, 30, 45, 60, 75, 90]: Each of these features counts how many minutiae there are in a radius (of 15 pixels, 30 pixels, and so on) around the specified minutia.

- class: Either a positive or negative impact on the matching score.

In total, this dataset has 12 features and a class feature. It contains 5215 instances, of which 1991 are positive examples (minutiae that increase the matching score when removed) and 3224 are negative examples (minutiae that lower the matching score when removed).

We tested eight different supervised classifiers. We selected popular classifiers of different types to get varied results. For each algorithm, we did five-fold distribution balanced stratified cross-validation [48], which is used for imbalanced class problems. We evaluated each algorithm with the area under the receiver operating characteristic curve (AUC) [49]. The AUC is calculated as:

$$\frac{1 + \mathrm{TPR} - \mathrm{FPR}}{2} \tag{1}$$

where TPR is true positive rate and FPR is false positive rate.

The eight supervised classifiers that we used were:

- Fisher's Linear Discriminant (LDA).
- Quadratic Discriminant Analysis (QDA).
- PBC4cip [50].
- Random Forest [51].
- Bagging [52].
- Logistic Regression [53].
- Multilayer Perceptron.
- Support Vector Machines (SVM) [54].

Figure 11 shows a bar graph comparing the average AUC of each supervised classifier when using five-fold distribution balanced stratified cross-validation. From Figure 11, we can see that PBC4cip [50] has the best performance with an AUC of .608, closely followed by FLDA and Random Forest [51]. The accuracy is still low, but these results suggest the existence of certain information that can be exploited to predict if a minutia will increase or decrease the matching score of a fingerprint with a better than random AUC.

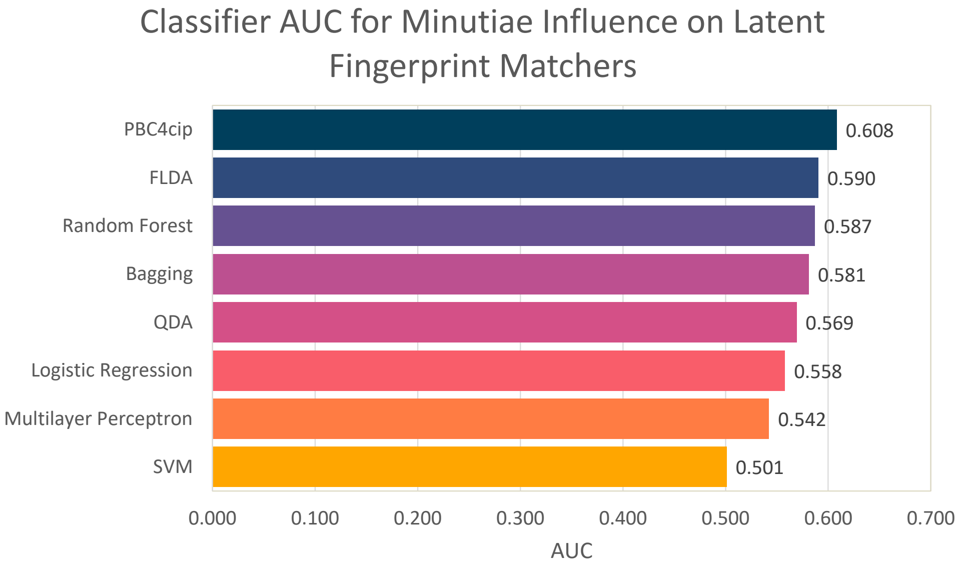


Figure 11. Average AUC for eight different classifiers tested on our minutiae dataset.

These results open a new research line related to creating automatic algorithms that help forensics experts to improve the minutiae labeling process in latent fingerprints.

7. Conclusions and Future Work

Aiming to develop automatic methods that can help latent fingerprint examiners make better decisions and can enable quality-based fingerprint processing, we carried out a study of how minutiae errors can affect the identification of latent fingerprints. Both human experts [28] and automatic algorithms [13] commit errors when labeling latent fingerprint minutiae. There is some knowledge already in the literature about the source and factors that originate those errors in both cases: human experts [26–28] and algorithms [13,21], but there is a lack of understanding of how those errors impact fingerprint identification systems. The present work is a step forward in understanding the impact of those minutiae errors.

From our experimental results, we can conclude that missing even one minutia from a fingerprint can have a very high negative impact on identification performance. In addition, some minutiae are more important than others to identify a latent fingerprint correctly. We also conclude that a result in the first places of the rank could be demoted to the last places of the rank when two or more minutiae (labeled as "lower" class) are removed. This fact of varying minutiae utility, or minutiae quality in terms of biometric utility [18], can enable specific processing for different minutiae [13] in quality-based conditional processing [44] or quality-based information fusion schemes [45–47].

In future work, we plan to deepen our study on what features make a minutia or a minutiae combination more important for identification performance. In addition, ongoing work is around determining critical areas of a latent fingerprint image in which missing a minutia could make the matching algorithms fail to identify a fingerprint correctly.

Author Contributions: O.L.-G., M.A.M.-P.: methodology, formal analysis, and writing—original draft. M.A.M.-P., E.F.F.M.: investigation, formal analysis, and software. A.M., J.F., M.A.M.-P., R.M., E.F.F.M.: investigation, writing—review and editing. A.M., J.F., M.A.M.-P., R.M.: supervision. R.M.: funding acquisition. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partly supported by the National Council of Science and Technology of Mexico under the scholarship grants 717345 and 005438. Authors J.F. and A.M. are funded by project BIBECA (RTI2018-101248-B-I00 MINECO/FEDER) and TRESPASS-ETN (MSCA-ITN-2019-860813).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Loyola-González, O. Black-Box vs. White-Box: Understanding Their Advantages and Weaknesses From a Practical Point of View. *IEEE Access* **2019**, *7*, 154096–154113. [CrossRef]
2. Gupta, R.; Khari, M.; Gupta, D.; Crespo, R.G. Fingerprint image enhancement and reconstruction using the orientation and phase reconstruction. *Inf. Sci.* **2020**, *530*, 201–218. [CrossRef]
3. Alonso-Fernandez, F.; Bigun, J.; Fierrez, J.; Fronthaler, H.; Kollreider, K.; Ortega-Garcia, J. Fingerprint Recognition. In *Guide to Biometric Reference Systems and Performance Evaluation*; Petrovska-Delacretaz, D., Chollet, G., Dorizzi, B., Eds.; Springer: Berlin/Heidelberg, Germany, 2009.
4. Jain, A.K.; Flynn, P.; Ross, A.A. *Handbook of Biometrics*, 1st ed.; Springer: Berlin/Heidelberg, Germany, 2010.
5. Alonso-Fernandez, F.; Fierrez, J. Fingerprint Databases and Evaluation. In *Encyclopedia of Biometrics*; Li, S.Z., Jain, A.K., Eds.; Springer: Berlin/Heidelberg, Germany, 2015; pp. 599–606. [CrossRef]
6. Zabala-Blanco, D.; Mora, M.; Barrientos, R.J.; Hernández-García, R.; Naranjo-Torres, J. Fingerprint Classification through Standard and Weighted Extreme Learning Machines. *Appl. Sci.* **2020**, *10*, 4125. [CrossRef]
7. Chen, J.; Zhao, H.; Cao, Z.; Guo, F.; Pang, L. A Customized Semantic Segmentation Network for the Fingerprint Singular Point Detection. *Appl. Sci.* **2020**, *10*, 3868. [CrossRef]
8. Wang, Y.; Gao, J.; Li, Z.; Zhao, L. Robust and Accurate Wi-Fi Fingerprint Location Recognition Method Based on Deep Neural Network. *Appl. Sci.* **2020**, *10*, 321. [CrossRef]

9. Pititheeraphab, Y.; Thongpance, N.; Aoyama, H.; Pintavirooj, C. Vein Pattern Verification and Identification Based on Local Geometric Invariants Constructed from Minutia Points and Augmented with Barcoded Local Feature. *Appl. Sci.* **2020**, *10*, 3192. [CrossRef]
10. Maltoni, D.; Maio, D.; Jain, A.K.; Prabhakar, S. *Handbook of Fingerprint Recognition*, 2nd ed.; Springer: Berlin/Heidelberg, Germany, 2009.
11. Ramírez-Sáyago, E.; Loyola-González, O.; Medina-Pérez, M.A. Towards Inpainting and Denoising Latent Fingerprints: A Study on the Impact in Latent Fingerprint Identification. In *Pattern Recognition*; Figueroa Mora, K.M., Anzurez Marín, J., Cerda, J., Carrasco-Ochoa, J.A., Martínez-Trinidad, J.F., Olvera-López, J.A., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 76–86.
12. Gonzalez-Rodriguez, J.; Fierrez-Aguilar, J.; Ramos-Castro, D.; Ortega-Garcia, J. Bayesian analysis of fingerprint, face and signature evidences with automatic biometric systems. *Forensic Sci. Int.* **2005**, *155*, 126–140. [CrossRef] [PubMed]
13. Krish, R.P.; Fierrez, J.; Ramos, D.; Alonso-Fernandez, F.; Bigun, J. Improving Automated Latent Fingerprint Identification using Extended Minutia Types. *Inf. Fusion* **2019**, *50*, 9–19. [CrossRef]
14. Nedjah, N.; Wyant, R.S.; Mourelle, L.M.; Gupta, B.B. Efficient fingerprint matching on smart cards for high security and privacy in smart systems. *Inf. Sci.* **2019**, *479*, 622–639. [CrossRef]
15. Lan, S.; Guo, Z.; You, J. Pre-registration of translated/distorted fingerprints based on correlation and the orientation field. *Inf. Sci.* **2020**, *520*, 292–304. [CrossRef]
16. Champod, C.; Lennard, C.; Margot, P.; Stoilovic, M. *Fingerprints and Other Ridge Skin Impressions*, 2nd ed.; CRC Press: Boca Raton, FL, USA, 2016.
17. Tistarelli, M.; Champod, C. *Handbook of Biometrics for Forensic Science*; Springer: Berlin/Heidelberg, Germany, 2017.
18. Alonso-Fernandez, F.; Fierrez, J.; Ortega-Garcia, J.; Gonzalez-Rodriguez, J.; Fronthaler, H.; Kollreider, K.; Bigun, J. A comparative study of fingerprint image-quality estimation methods. *IEEE Trans. Inf. Forensics Secur.* **2007**, *2*, 734–743. [CrossRef]
19. Medina-Pérez, M.A.; Moreno, A.M.; Ballester, M.Á.F.; García-Borroto, M.; Loyola-González, O.; Altamirano-Robles, L. Latent fingerprint identification using deformable minutiae clustering. *Neurocomputing* **2016**, *175*, 851–865. [CrossRef]
20. Ramos, D.; Krish, R.P.; Fierrez, J.; Meuwly, D. From Biometric Scores to Forensic Likelihood Ratios. In *Handbook of Biometrics for Forensic Science*; Tistarelli, M., Champod, C., Eds.; Springer: Berlin/Heidelberg, Germany, 2017; pp. 305–327. [CrossRef]
21. Valdes-Ramirez, D.; Medina-Pérez, M.A.; Monroy, R.; Loyola-González, O.; Rodríguez, J.; Morales, A.; Herrera, F. A Review of Fingerprint Feature Representations and Their Applications for Latent Fingerprint Identification: Trends and Evaluation. *IEEE Access* **2019**, *7*, 48484–48499. [CrossRef]
22. Rodríguez-Ruiz, J.; Medina-Pérez, M.A.; Monroy, R.; Loyola-González, O. A survey on minutiae-based palmprint feature representations, and a full analysis of palmprint feature representation role in latent identification performance. *Expert Syst. Appl.* **2019**, *131*, 30–44. [CrossRef]
23. Garris, M.D. *NIST Special Database 27: Fingerprint Minutiae from Latent and Matching Tenprint Images*; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2000.
24. Budowle, B.; Buscaglia, J.; Perlman, R.S. Review of the scientific basis for friction ridge comparisons as a means of identification: Committee findings and recommendations. *Forensic Sci. Commun.* **2006**, *8*. Available online: https://go.gale.com/ps/anonymous?id=GALE|A144388747 (accessed on 24 April 2021).
25. Morales, A.; Morocho, D.; Fierrez, J.; Vera-Rodriguez, R. Signature Authentication based on Human Intervention: Performance and Complementarity with Automatic Systems. *IET Biom.* **2017**, *6*, 307–315. [CrossRef]
26. Ulery, B.T.; Hicklin, R.A.; Buscaglia, J.; Roberts, M.A. Accuracy and reliability of forensic latent fingerprint decisions. *Proc. Natl. Acad. Sci. USA* **2011**, *108*, 7733–7738. [CrossRef]
27. Ulery, B.T.; Hicklin, R.A.; Roberts, M.A.; Buscaglia, J. Changes in latent fingerprint examiners' markup between analysis and comparison. *Forensic Sci. Int.* **2015**, *247*, 54–61. [CrossRef]
28. Ulery, B.T.; Hicklin, R.A.; Roberts, M.A.; Buscaglia, J. Interexaminer variation of minutia markup on latent fingerprints. *Forensic. Sci. Int.* **2016**, *264*, 89–99. [CrossRef]
29. Kukucka, J.; Dror, I.E.; Yu, M.; Hall, L.; Morgan, R.M. The impact of evidence lineups on fingerprint expert decisions. *Appl. Cogn. Psychol.* **2020**, *35*, 1143–1153. [CrossRef]
30. Valdes-Ramirez, D.; Medina-Pérez, M.A.; Monroy, R. An ensemble of fingerprint matching algorithms based on cylinder codes and mtriplets for latent fingerprint identification. *Pattern Anal. Appl.* **2020**, 1–12. [CrossRef]
31. Alonso-Fernandez, F.; Fierrez-Aguilar, J.; Ortega-Garcia, J. An enhanced Gabor filter-based segmentation algorithm for fingerprint recognition systems. In Proceedings of the IEEE International Symposium on Image and Signal Processing and Analysis, ISPA, Special Session on Signal and Image Processing for Biometrics, Zagreb, Croatia, 15–17 September 2005; pp. 239–244.
32. Alonso-Fernandez, F.; Fierrez, J.; Ortega-Garcia, J. Quality Measures in Biometric Systems. *IEEE Secur. Priv.* **2012**, *10*, 52–62. [CrossRef]
33. Fierrez-Aguilar, J.; Nanni, L.; Ortega-Garcia, J.; Cappelli, R.; Maltoni, D. Combining multiple matchers for fingerprint verification: A case study in FVC2004. In Proceedings of the 13th IAPR International Conference on Image Analysis and Processing, Cagliari, Italy, 6–8 September 2005; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3617, pp. 1035–1042.
34. Fierrez, J.; Morales, A.; Vera-Rodriguez, R.; Camacho, D. Multiple Classifiers in Biometrics. Part 1: Fundamentals and Review. *Inf. Fusion* **2018**, *44*, 57–64. [CrossRef]

35. Simon-Zorita, D.; Ortega-Garcia, J.; Fierrez-Aguilar, J.; Gonzalez-Rodriguez, J. Image quality and position variability assessment in minutiae-based fingerprint verification. *IEE Proc. Vision Image Signal Process.* **2003**, *150*, 402–408. [CrossRef]
36. Ester, M.; Kriegel, H.P.; Sander, J.; Xu, X.; others. A density-based algorithm for discovering clusters in large spatial databases with noise. In Proceedings of the International Conference on Knowledge Discovery and Data Mining (KDD-96), AAAI, Portland, OR, USA, 2–6 August 1996; Volume 96, pp. 226–231.
37. Grosz, S.A.; Engelsma, J.J., Jr.; Paulter, N.G.; Jain, A.K. White-box evaluation of fingerprint matchers: Robustness to minutiae perturbations. *arXiv* **2019**, arXiv:1909.00799.
38. Cappelli, R.; Maio, D.; Maltoni, D. SFinGe: An approach to synthetic fingerprint generation. In Proceedings of the International Workshop on Biometric Technologies (BT2004), Calgary, AB, Canada, 22–23 June 2004; pp. 147–154.
39. Krish, R.; Fierrez, J.; Ramos, D.; Ortega-Garcia, J.; Bigun, J. Pre-Registration of Latent Fingerprints based on Orientation Field. *IET Biom.* **2015**, *4*, 42–52. [CrossRef]
40. Watson, C.I.; Wilson, C.L. *NIST Special Database 4*; Technical report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 1992.
41. Cappelli, R.; Ferrara, M.; Maltoni, D. Minutia Cylinder-Code: A New Representation and Matching Technique for Fingerprint Recognition. *IEEE Trans. Pattern Anal. Mach. Intell.* **2010**, *32*, 2128–2141. [CrossRef] [PubMed]
42. Grother, P.; Micheals, R.J.; Phillips, P.J. Face Recognition Vendor Test 2002 Performance Metrics. In *Audio- and Video-Based Biometric Person Authentication*; Kittler, J., Nixon, M.S., Eds.; Springer: Berlin/Heidelberg, Germany, 2003; pp. 937–945.
43. INTERPOL. *Guidelines concerning transmission of Fingerprint Crime Scene Marks*; INTERPOL: Lyon, France, 2012.
44. Alonso-Fernandez, F.; Fierrez, J.; Ramos, D.; Gonzalez-Rodriguez, J. Quality-Based Conditional Processing in Multi-Biometrics: Application to Sensor Interoperability. *IEEE Trans. Syst. Man Cybern. Part A* **2010**, *40*, 1168–1179. [CrossRef]
45. Fierrez-Aguilar, J.; Chen, Y.; Ortega-Garcia, J.; Jain, A.K. Incorporating image quality in multi-algorithm fingerprint verification. In Proceedings of the IAPR International Conference on Biometrics, ICB, LNCS, New Delhi, India, 29 March 2006; Volume 3832, pp. 213–220.
46. Fronthaler, H.; Kollreider, K.; Bigun, J.; Fierrez, J.; Alonso-Fernandez, F.; Ortega-Garcia, J.; Gonzalez-Rodriguez, J. Fingerprint Image Quality Estimation and its Application to Multi-Algorithm Verification. *IEEE Trans. Inf. Forensics Secur.* **2008**, *3*, 331–338. [CrossRef]
47. Fierrez, J.; Morales, A.; Vera-Rodriguez, R.; Camacho, D. Multiple Classifiers in Biometrics. Part 2: Trends and Challenges. *Inf. Fusion* **2018**, *44*, 103–112. [CrossRef]
48. Moreno-Torres, J.G.; Sáez, J.A.; Herrera, F. Study on the impact of partition-induced dataset shift on *k*-fold cross-validation. *IEEE Trans. Neural Netw. Learn. Syst.* **2012**, *23*, 1304–1312. [CrossRef] [PubMed]
49. Fawcett, T. Introduction to ROC analysis. *Pattern Recognit. Lett.* **2006**, *27*, 861–874. [CrossRef]
50. Loyola-González, O.; Medina-Pérez, M.A.; Martínez-Trinidad, J.F.; Carrasco-Ochoa, J.A.; Monroy, R.; García-Borroto, M. PBC4cip: A new contrast pattern-based classifier for class imbalance problems. *Knowl. Based Syst.* **2017**, *115*, 100–109. [CrossRef]
51. Breiman, L. Random forests. *Mach. Learn.* **2001**, *45*, 5–32. [CrossRef]
52. Breiman, L. Bagging predictors. *Mach. Learn.* **1996**, *24*, 123–140. [CrossRef]
53. le Cessie, S.; van Houwelingen, J. Ridge Estimators in Logistic Regression. *Appl. Stat.* **1992**, *41*, 191–201. [CrossRef]
54. Cortes, C.; Vapnik, V. Support-vector networks. *Mach. Learn.* **1995**, *20*, 273–297. [CrossRef]

Short Biography of Authors

Octavio Loyola-González received his Ph.D. degree in Computer Science from the National Institute for Astrophysics, Optics, and Electronics, Mexico, in 2017. He has won several awards from different institutions due to his research work on applied projects; consequently, he is a Member of the National System of Researchers in Mexico (Rank1). He worked as a distinguished professor and researcher at Tecnologico de Monterrey, Campus Puebla, for undergraduate and graduate programs of Computer Sciences. Currently, he is responsible for running Machine Learning and Artificial Intelligence practice inside Altair Management Consultants Corp., where he is involved in the development and implementation using analytics and data mining in the Altair Compass department. He has outstanding experience in the fields of big data and pattern recognition, cloud computing, IoT, and analytical tools to apply them in sectors where he has worked for as Banking and Insurance, Retail, Oil and Gas, Agriculture, Cybersecurity, Biotechnology, and Dactyloscopy. From these applied projects, Dr. Loyola-González has published several books and papers in well-known journals, and he has several ongoing patents as a manager and researcher in Altair Compass.

Emilio Francisco Ferreira Mehnert obtained his Bachelor's of Engineering degree in Software Engineering from Tecnológico de Monterrey, Campus Santa Fe in 2017. He received his Master of Science degree in Computer Science from Tecnológico de Monterrey, Campus Estado de México in 2020. His interests include machine learning, deep learning, and software development.

Aythami Morales Moreno received his M.Sc. (Electronical Engineering) and Ph.D. (Artificial Intelligence) degrees from Universidad de Las Palmas de Gran Canaria in 2006 and 2011, respectively. Since 2017, he is an Associate Professor with the Universidad Autonoma de Madrid. He has conducted research stays at Michigan State University, Hong Kong Polytechnic University, University of Bologna, and the Schepens Eye Research Institute. He has authored over 100 scientific articles in topics related to machine learning, trustworthy AI, and biometric signal processing.

Julian Fierrez (Member, IEEE) received his M.Sc. and the Ph.D. degrees in Telecommunications Engineering from Universidad Politecnica de Madrid, Spain, in 2001 and 2006, respectively. Since 2004, he is at Universidad Autonoma de Madrid, where he is an Associate Professor since 2010. His research is on signal and image processing, AI fundamentals and applications, HCI, forensics, and biometrics for security and human behavior analysis. He is actively involved in large EU projects in these topics (e.g., BIOSECURE, TABULA RASA and BEAT in the past; now IDEA-FAST, PRIMA, and TRESPASS-ETN). Since 2016, he is an Associate Editor for Elsevier's Information Fusion and IEEE Trans. on Information Forensics and Security, and since 2018 also for IEEE Trans. on Image Processing. He has been a General Chair of IAPR CIARP 2018 and IAPR IbPRIA 2019. Since 2020, he is member of the ELLIS Society. Prof. Fierrez has received best papers awards at AVBPA, ICB, IJCB, ICPR, ICPRS, and Pattern Recognition Letters. He is also a recipient of several world-class research distinctions, including: EBF European Biometric Industry Award 2006; EURASIP Best Ph.D. Award 2012; Miguel Catalan Award to the Best Researcher under 40 in the Community of Madrid in the general area of Science and Technology; and IAPR Young Biometrics Investigator Award 2017, given to a single researcher worldwide every two years under the age of 40 whose research has had a major impact in biometrics.

Miguel Angel Medina-Pérez received a Ph.D. in Computer Science from the National Institute of Astrophysics, Optics, and Electronics, Mexico, in 2014. He is currently a Research Professor with the Tecnologico de Monterrey, Campus Estado de Mexico, where he is also a member of the GIEE-ML (Machine Learning) Research Group. He has rank 1 in the Mexican Research System. His research interests include pattern recognition, data visualization, explainable artificial intelligence, fingerprint recognition, and palmprint recognition. He has published tens of papers in referenced journals, such as "Information Fusion," "IEEE Transactions on Affective Computing," "Pattern Recognition," "IEEE Transactions on Information Forensics and Security," "Knowledge-Based Systems," "Information Sciences," and "Expert Systems with Applications." He has extensive experience developing software to solve pattern recognition problems. A successful example is a fingerprint and palmprint recognition framework which has more than 1.3 million visits and 135 thousand downloads.

Raúl Monroy obtained a Ph.D. degree in Artificial Intelligence from Edinburgh University, in 1998, under the supervision of Prof. Alan Bundy. He has been in Computing at Tecnologico de Monterrey, Campus Estado de México, since 1985. In 2010, he was promoted to (full) Professor in Computer Science. Since 1998, he is a member of the CONACYT-SNI National Research System, rank three. Together with his students and members of his group, Machine Learning Models (GIEE – MAC), Prof. Monroy studies the discovery and application of novel model machine learning models, which he often applies to cybersecurity problems. At Tecnologico de Monterrey, he is also the Head of the graduate program in computing, at region CDMX.