MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems

Aditi Roy, *Student Member, IEEE*, Nasir Memon, *Fellow, IEEE*, and Arun Ross, *Senior Member, IEEE*

***Abstract*— This paper investigates the security of partial fingerprint-based authentication systems, especially when multiple fingerprints of a user are enrolled. A number of consumer electronic devices, such as smartphones, are beginning to incorporate fingerprint sensors for user authentication. The sensors embedded in these devices are generally small and the resulting images are, therefore, limited in size. To compensate for the limited size, these devices often acquire multiple partial impressions of a single finger during enrollment to ensure that at least one of them will successfully match with the image obtained from the user during authentication. Furthermore, in some cases, the user is allowed to enroll multiple fingers, and the impressions pertaining to multiple partial fingers are associated with the same identity (i.e., one user). A user is said to be successfully authenticated if the partial fingerprint obtained during authentication matches any one of the stored templates. This paper investigates the possibility of generating a "MasterPrint," a synthetic or real partial fingerprint that serendipitously matches one or more of the stored templates for a significant number of users. Our preliminary results on an optical fingerprint data set and a capacitive fingerprint data set indicate that it is indeed possible to locate or generate partial fingerprints that can be used to impersonate a large number of users. In this regard, we expose a potential vulnerability of partial fingerprint-based authentication systems, especially when multiple impressions are enrolled per finger.**

***Index Terms*— Authentication, biometrics, computer security, dictionary attack, fingerprint recognition, hill climbing, mobile applications, mobile device authentication, partial fingerprint.**

I. Introduction

FINGERPRINTS are one of the oldest and most widely employed biometric traits used by forensics and law enforcement agencies worldwide [19]. Their use for human *identification* is based on two premises: (i) permanence or persistence, and (ii) uniqueness or distinctiveness. In recent times, there has been a remarkable growth in the utilization of fingerprints for biometric *verification* in various applications.

Manuscript received August 1, 2016; revised December 6, 2016 and February 7, 2017; accepted March 13, 2017. Date of publication April 6, 2017; date of current version June 14, 2017. This work was supported by the National Science Foundation under Grant 1618750 and Grant 1617466. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Julien Bringer. *(Corresponding author: Aditi Roy.)*

A. Roy and N. Memon are with the Department of Computer Science and Engineering, New York University Tandon School of Engineering, Brooklyn, NY 11201 USA (e-mail: ar3824@nyu.edu; memon@nyu.edu).

A. Ross is with the Department of Computer Science and Engineering, Michigan State University, East Lansing, MI 48824 USA (e-mail: rossarun@cse.msu.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2017.2691658

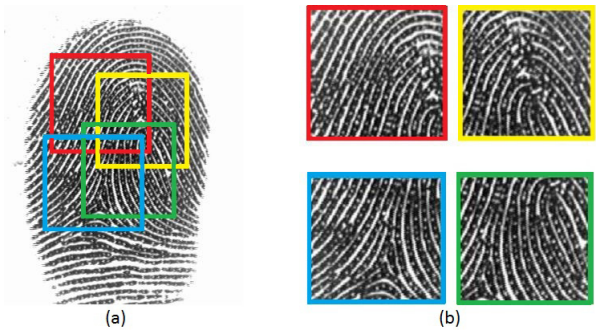

Fig. 1. A set of partial fingerprints (b) extracted from the full fingerprint (a).

Companies such as Apple and Samsung have introduced fingerprint sensors for authenticating users on smartphones. The European Association for Biometrics considers the release of the iPhone 5s in September 2013 as heralding a paradigm shift [3]. This shift is now fueling a second emerging trend in user authentication that uses fingerprints for payments and other financial transactions. In addition to mobile payment services by Apple, Samsung and others, a credit card with a fingerprint scanner has been developed by Zwipe and MasterCard.

Although, from a usability point of view, fingerprint authentication is being touted as a much awaited and welcome replacement for "what you know" (e.g. PINs), and "what you have" (e.g. ID cards) based systems, their security has not been well studied in the context of the following:

- Smartphones and other small form factor mobile devices typically employ small sensors which capture only a limited portion of the full fingerprint (see Figure 1 (a)) [15].
- Since only a partial fingerprint is captured in any single sensing instance, multiple partial fingerprints are captured for the same finger during enrollment, and a collection of these partial fingerprint impressions is stored (see Figure 1(b)).
- To enhance usability of the system, a user is permitted to enroll multiple fingers.
- Since authentication is done in an unsupervised manner, the verification system does not know which finger or which part of the finger is being sensed. Hence, in some cases, authentication is declared successful if the sensed partial fingerprint matches with any of the stored impressions; that is, any partial fingerprint of any enrolled finger.

In the specific case of the Apple Touch ID, it has been claimed that the system has a one in 50,000 chance for a

false match [1]. Hence, the system is assumed to be more secure than the fallback (minimum 4 digit) PIN that a user is requested to enter after 5 unsuccessful tries [1] or a restart. However, irrespective of the specifics of a system, the security of an authentication system is not merely measured by the chance that a random attempt will succeed, but is based on the probability that an attacker, with some knowledge about the distribution of the input data, will succeed in a given number of attempts to guess the right input. So, for example, in a PIN-based authentication system, an attacker who guesses "1234" has a 4.3% [8] chance of success. The same question could be asked of partial fingerprint-based user authentication systems.

Is there a partial fingerprint that can fortuitously match with the fingerprint data of an arbitrary user with high probability? We define a MasterPrint as a fingerprint that serendipitously matches a certain proportion of the fingerprint population. This is akin to discovering a password or passcode that can unlock many accounts. Considering PIN-based authentication on mobile phones as [8], the existence of MasterPrints that match with 4.3% of the population would have strong security implications. A MasterPrint could be either a full print or a partial print. For brevity sake, we use the term MasterPrint for both situations with the context indicating the specific case being discussed. The objective of this paper is to study the security of fingerprint-based verification systems against such attacks:

- Is it possible to find MasterPrints that match with a large number of fingerprints originating from different users?
- Alternatively, is it possible to generate such a MasterPrint synthetically and, if so, how?

Our results indicate that the answer to the above questions may be "yes", thereby exposing a potential vulnerability of partial fingerprint-based authentication systems.

II. Prior Work

The security of biometric systems has been extensively studied in the past two decades. It is well known that in spite of its numerous advantages, a fingerprint-based biometric system is potentially vulnerable to a variety of attacks [36]. Ratha *et al.* [28] identified eight points of attack in a biometric system that can be grouped into four categories, namely, (i) attacks at the user interface (input level), (ii) attacks at the interfaces between modules, (iii) attacks on the modules, and (iv) attacks on the database. Among these, type 1 attacks which involve the presentation of fingerprint spoofs have proven to be quite successful [22]. Since this attack only needs a fake biometric without any knowledge of the matcher, image specifications or database access privileges, its vulnerability is higher compared to the other attacks. Moreover, since it operates in the analog domain, digital protection mechanisms like encryption, digital signature, hashing etc. may not be easily applicable. Therefore, this type of attack represents a realistic threat for fingerprint verification systems used in mobile devices.

A spoof attack can be launched by (a) lifting the residual fingerprint of a user from the phone or any other surface, (b) creating a dummy finger from the lifted impression; and (c) placing the dummy finger on the fingerprint sensor [34]. Such attacks have been demonstrated against the Apple iPhone 5S as well as the Samsung Galaxy S5 [2]. Another type of attack involves the reconstruction of a fingerprint image from a minutiae template which can be achieved, for example, by using amplitude and frequency modulated (AM-FM) functions [31]. Consequently, if an attacker steals a database of minutiae templates from a server or cloud storage, it is possible - in principle - to reconstruct the corresponding fingerprint images and generate spoof fingers using the reconstructed images.

A. Brute Force Attack

When none of the aforementioned attacks are feasible, a crude brute force attack with a large number of input fingerprints can be used. Ratha *et al.* [28] established the relationship between the number of brute force attack attempts and the number of minutiae that is expected to match. They showed that the search space for guessing the fingerprint to be matched can be prohibitively large. However, for a mobile device, where only a portion of the full fingerprint is used, this search space would be much smaller.

B. Dictionary Based Guessing Attack

In contrast to a brute force attack, a dictionary attack tries only those possibilities which are deemed most likely to succeed. For example, a study on the RockYou! database [12] shows if an attacker tries to gain access to a password-protected system by trying the 10 most common passwords in that database and using a listing of known accounts, he could be expected to succeed within 25 accounts, costing only 250 guesses [13]. Analyses on dictionary attacks report that the percentage of rightly guessed text passwords can vary between 17% and 24% [23], [35], depending on the dataset and dictionary size.

To quantify the resistance to dictionary attacks, proper metrics are needed. In the context of PIN, text or pattern based passwords, a number of measures have been proposed. A traditional measure is *Shannon entropy* [33], which is mathematically unsuited to measuring guessing difficulty. A more sound measure is *Guessing entropy* [7] that computes the average number of guesses that the optimal attack needs in order to find the correct password. However, according to [8], both of these measures are influenced by rare events significantly enough to make them misleading for security analysis. A preferable alternative is *Marginal guesswork*, μ_α, which measures the expected number of guesses required to succeed with probability α [8]:

$$\mu_\alpha = min\{j \in [1, N] | \sum_{i=1}^{j} p_i > \alpha\}, \tag{1}$$

where the password x_i in a database $\mathcal{X}$ of N passwords has probability of occurrence p_i and $p_1 \geq p_2 \geq \ldots \geq p_N$. In the case of a fingerprint-based verification system, attackers are almost always externally limited in the number of guesses that are allowed. Then, the best metric is the *Marginal success rate* λ_β, the probability that an attacker can correctly guess an

unknown password x in β attempts:

$$\lambda_\beta = \sum_{i=1}^{\beta} p_i. \tag{2}$$

However, the Marginal success rate cannot be used in biometric authentication as multiple biometric passwords can be jointly accepted with a probability corresponding to the False Match Rate (FMR) of the matcher. So, we used the Imposter Match Rate, described later, for this purpose.

Although dictionary attacks have been extensively studied and analyzed for traditional password-based authentication systems, they have not been systematically considered by the research community in the context of fingerprint verification. To perform a guessing attack with fingerprints, the question arises as to whether there are some fingerprints that are more likely to match a target than the others? It has been observed in the previous literature, that different users have different performance characteristics based on their fingerprint. Doddington *et al.* [14] pointed out in the context of speaker recognition that some users contribute disproportionately to high a FMR and False Non-Match Rate (FNMR). They introduced the concept of the "biometric menagerie", which characterized users into four different groups based on their genuine scores and imposter scores, namely, sheep, goat, lamb, and wolf. While Doddington *et al.* considered genuine scores and imposter scores separately, Yager *et al.* [39] took the relationship between genuine and imposter scores into account, and introduced a new menagerie consisting of dove (users with high genuine scores and low imposter scores), chameleons (high genuine scores and high imposter scores, thus are easy to match with everyone, including themselves), phantom (hard to match with most of the users), and worm (hard to match with themselves but easy to match with others). Previous studies [27], [39] have identified the existence of chameleons in datasets of full fingerprints.

There are two research topics in the literature that are closely related to the current work on MasterPrints: "wolf attack" [16], [38] and evidential value analysis [24]. The work presented in [16], [38] introduced a security measure called "Wolf Attack Probability (WAP)" to estimate the strength of a biometric authentication system against impersonation attacks. In that work, a wolf is defined to be any input sample, including non-biometric samples such as physical artifacts, that can incorrectly match with multiple biometric templates. The focus of the previous work is primarily on defining a measure for security. In our work, the focus is on locating and generating MasterPrints. There are two major differences between [16], [38] and our proposed work. First, we present specific approaches to generate MasterPrint unlike [16], [38]. Second, we show that the probability of detecting a MasterPrint and the attack accuracy increases when partial fingerprints are used, thereby exposing the vulnerability of fingerprint systems that use partial prints for authentication. Such an analysis has not been undertaken in the previous work.

The other related research work deals with evidential value analysis [24] of latent fingerprints. The study shows that if the surface area of the latent fingerprint is small or if there are fewer minutiae points, then the evidential value of the print is also low resulting in a higher probability of matching error. Based on this observation, we hypothesize that the probability of finding MasterPrints that incorrectly match with a large number of templates is higher in a partial print dataset.

III. MasterPrints: Do They Exist?

While it is widely accepted in the fingerprint literature that partial fingerprints are more prone to generate a false match due to loss in "information entropy", an analytical evaluation of the probability of false matches using such partial fingerprints of variable sizes is hard to perform. Existing work has only modeled the observed minutiae feature distribution statistically to compute the Probability of Random Correspondence (PRC), which is actually the false match rate, for a full fingerprint dataset [25]. Investigation of how PRCs change with the size of a fingerprint image has not been done, to the best of our knowledge.

In the absence of such analytical models, in this section we explore statistical evidence that supports the intuition that an increase in false match rate in a partial fingerprint dataset leads to a higher chance of finding MasterPrints.

A. MasterPrint Existence Hypothesis

We hypothesize that the probability of finding MasterPrints is higher in partial print dataset than full print dataset. Consider a population of N subjects with J fingers, with each finger having K impressions. Let this dataset be denoted as $\mathcal{F} = \{F^i_{jk} | i \in \{1, \ldots, N\}, j \in \{1, \ldots, J\}, k \in \{1, \ldots, K\}\}$. Let the size of each print F^i_{jk} be $W \times H$. There are N_G $(= J \cdot K)$ full prints per identity and the total number of full prints is N_T $(= N \cdot N_G)$.

Fingerprints obtained using small sensors generally capture only a partial print. Let a single full fingerprint be tessellated into L partial prints each of size $w \times h$ ($w < W$ and $h < H$). The L fold increase in the number of partial fingerprints (PF^i_{jkl}) results in a dataset $\mathcal{F}' = \{PF^i_{jkl} | i \in \{1, \ldots, N\}, j \in \{1, \ldots, J\}, k \in \{1, \ldots, K\}, l \in \{1, \ldots, L\}\}$. This in turn results in an increase in the number of genuine scores and impostor scores for each subject in an all-to-all match test using a symmetric matcher, which consequently may increase the probability of observing chameleons having high imposter scores that lead to false matches.

1) Hypothesis: Let, the probability of finding MP in partial print dataset $\mathcal{F}'$ be $P(MP \subset \mathcal{F}')$ and the probability of finding it in full print dataset $\mathcal{F}$ be $P(MP \subset \mathcal{F})$. Then, our null hypothesis is:

$$H_0 : P(MP \subset \mathcal{F}) \geq P(MP \subset \mathcal{F}'). \tag{3}$$

For our hypothesis to hold, H_0 has to be rejected.

B. Hypothesis Test

To test the MasterPrint existence hypothesis, experiments were conducted on the standard FVC 2002 dataset DB1-A [40] that contains 8 fingerprints of 100 subjects, for a total of 800 fingerprints. We created partial prints of size $w \times h$

by cropping the full prints using an overlapping window that moved from top-to-bottom and left-to-right with a 50% overlap between adjacent windows. To create similar sized partial fingerprints as used by Apple Touch ID, a window size of 150×150 was used (See Appendix for a justification of the window size). The sampling was done uniformly from the foreground area of the full fingerprints. On an average, 10 partial prints were extracted from each of the 800 full prints, creating a total of 8220 partial prints.[1]

The commercial fingerprint verification software Verifinger 6.1 SDK was used for matching fingerprints. When using full fingerprints in the DB1-A dataset, the average FMR was found to be 0.1% while the average True Match Rate (TMR) was 99.18%. When comparing the full as well as partial prints, only pairs of prints having at least 10 minutiae were considered. Those partial or full fingerprints that matched with at least 4% of partial or full prints of other subjects were selected as candidate MasterPrints. 1 out of 800 full fingerprints and 1203 out of 8220 partial fingerprints were detected as MasterPrints.

Next, the t-test was applied to test our hypothesis in Eq. (3) based on these results. We found $X^2 = 185.42$, degree of freedom $= (2-1)*(2-1) = 1$, and p-value $< 2.2e{-}16$. Our desired confidence level was $\alpha = 0.05$. Since the p-value $\ll 0.05$, the null hypothesis H_0 can be rejected in favor of the alternative hypothesis that the proportion of MasterPrints is indeed much higher in a partial print dataset.

1) Robustness Check on Hypothesis Testing: The traditional hypothesis testing approach described above uses the entire sample set for evaluation. However, Perols *et al.* [26] pointed out that it is important to consider the robustness of results across different subsamples of the original data. They proposed the Multi-subset Observation Undersampling (OU) [10] method to check the robustness of traditional hypothesis testing. This approach addresses the imbalance between the low number of full fingerprint data compared to the number of partial fingerprint data by creating multiple subsets of the original dataset. Each subset contains all the samples from the "full" fingerprint data and multiple random subsamples of the "partial" fingerprint data.

We created 12 subsets where each subset included 800 full fingerprints and a random sample of 800 partial fingerprints from the pool of 8220 partial fingerprints. MasterPrints were then located on each of these subsets. On an average, 92 MasterPrints were detected from each partial print subset. Each subset was then used in the hypothesis testing framework. The p-value was $<<$ 0.05 in all of the 12 cases. These results suggest that OU yields similar results as the traditional hypothesis testing analysis, i.e., the null hypothesis, H_0, is rejected in the OU analysis. However, the OU results are generally more conservative. For example, the p-values from the OU results are numerically higher than the traditional approach. Thus, the OU subsample analysis indicates that our hypothesis testing is robust and that the probability of finding MasterPrints from the partial fingerprint dataset is higher than the full fingerprint dataset. Additional comparative analysis in Section V will show that the accuracy of an attack is also higher in the case of the partial fingerprint dataset.

[1]The dataset can be downloaded from https://wp.nyu.edu/memon/the-master-print/

IV. MasterPrint Generation

Next, we investigate methods for generating MasterPrints. We explore two approaches: one where the print is selected from an existing dataset of real fingerprints, and another where the print is generated synthetically. For the first approach, a fixed dataset is used as the training dataset from which the MasterPrint is sampled. These MasterPrints selected directly from a dataset are termed as "Sampled MasterPrints" or "SAMPs". The synthetically created MasterPrints in the second approach are termed as "Synthetic MasterPrints" or "SYMPs". Both approaches are designed for a minutiae-based fingerprint authentication system and a detailed description of them is presented below.

A. Sampled MasterPrint Generation

Generating MasterPrints by sampling a fingerprint dataset (training set) is rather straightforward. The "Imposter Match Rate" (IMR) - which is the number of false matches when a fingerprint is compared against images of other fingers (impostors) - is computed for all candidate prints. If $S((\chi),(i,j,k,l))$ represents the match score between fingerprint χ and F^i_{jkl}, and θ represents the matching threshold, then $IMR(\chi)$ is formally defined as follows:

$$IMR(\chi) = \frac{1}{(N-1)\cdot L\cdot N_G}\sum_{\forall i,j,k,l}\phi((\chi),(i,j,k,l)),$$

where

$$\phi((\chi),(i,j,k,l)) = \begin{cases} 1, & \text{if } S((\chi),(i,j,k,l)) > \theta \\ 0, & \text{otherwise.} \end{cases} \quad (4)$$

The prints with maximum IMRs are selected from the dataset. However, since these SAMPs are identified from an existing dataset, properties such as image size, degree of fingerprint variability, noise, etc, might affect the IMR of these SAMPs when used in various other datasets, i.e., their imitating power may be low. Moreover, it may not be always possible to find a MasterPrint in a selected dataset. To improve the IMR of MasterPrint, we also explore the possibility of creating a synthetic MasterPrint by altering a SAMP.

B. Synthetic MasterPrint Generation

Here, our objective is to generate improved MasterPrints synthetically by maximizing their IMR over a training dataset. Let Σ be the space of all MasterPrints. If ω is a candidate MasterPrint in Σ, it implies that ω at least matches with 4% of the fingerprints. The goal is to find SYMP ω' in the space Σ of all possible MasterPrints that maximizes the following objective function:

$$\omega' = \arg\max_{\omega\in\Sigma}\{IMR(\omega)\}. \quad (5)$$

Since searching over the entire space is intractable, local search can be applied to find a solution.

Algorithm 1 Synthetic MasterPrint Generation Algorithm

Parameters:
F_{best} = Best synthetic template
F_{curr} = Current synthetic template
F_{temp} = Candidate template
SAMP = Sampled template used as seed
IMR_{best} = Imposter match rate of F_{best}
IMR_{curr} = Imposter match rate of F_{curr}
IMR_{temp} = Imposter match rate of F_{temp}
IMR_{SAMP} = Imposter match rate of SAMP
i_{max} = Maximum iteration
M_{min} = Minimum number of minutiae in a template
IMR_{max} = Maximum Imposter match rate
Input: SAMP, IMR_{SAMP}, i_{max}, M_{min}
Output: F_{best}
Initialization:
$F_{best} \leftarrow F_{curr} \leftarrow$ SAMP,
$IMR_{best} \leftarrow IMR_{curr} \leftarrow IMR_{SAMP}$
Begin
while $i < i_{max}$ & $IMR_{best} < IMR_{max}$ **do**
  $F_{temp} \leftarrow F_{curr}$
  Perform one of the following four operations on F_{temp} and then calculate IMR_{temp}:
    (a) Change an existing minutia of F_{temp} by moving it to an adjacent cell or by changing its orientation to the previous/next angle quantum with equal probability.
    (b) Add a randomly generated minutia to F_{temp}.
    (c) Replace an existing minutia of F_{temp} with a new minutia by randomly selecting a minutia, deleting it and then adding a randomly generated minutia.
    (d) Delete an existing minutia of F_{temp} randomly if the number of minutiae $> M_{min}$.
  If $IMR_{temp} > IMR_{curr}$, then $IMR_{curr} \leftarrow IMR_{temp}$ and $F_{curr} \leftarrow F_{temp}$
  If $IMR_{curr} > IMR_{best}$, then $IMR_{best} \leftarrow IMR_{curr}$ and $F_{best} \leftarrow F_{curr}$
  $i = i + 1$;
end while
End

A number of approaches have been proposed in the literature to generate synthetic fingerprints for launching indirect attacks against fingerprint systems. Attacks based on hill climbing [36] have been found to be highly effective in generating synthetic impressions that are falsely accepted by the matcher [21]. We adopt a similar approach in our work. The SAMPs found from the training dataset are used as the initial seed in the hill climbing process.

In hill climbing, a randomly generated synthetic minutiae template is presented to the matcher and, based on the output score, it is iteratively modified until a specific criteria is fulfilled. Here, minutiae are defined by their position and orientation. At first, image-level matching is performed on the training dataset to select a sampled MasterPrint (SAMP) with high IMR (IMR_{SAMP}). The seed fingerprint is then divided into multiple cells each covering one inter-ridge distance (9 pixels for a 500 dpi image) to prevent adding minutiae points that are in close proximity to each other (details below). Thus, each cell of size 9×9 pixels can only contain one minutia in the center of the cell, apart from the already existing minutiae in the initial SAMP. Also, the minutia orientation range $[0,2\pi)$ is quantized into 16 equally spaced intervals. Next, a hill climbing method is applied on this fingerprint as described in Algorithm 1.

The algorithm modifies the SAMP such that the number of minutiae is increased or decreased, or the positions and orientations of existing minutiae points are changed. The value of IMR is used to guide this process. However, the average number of minutiae in partial prints is generally low. To prevent the situation where the number of minutiae in SYMP is further lowered by the deletion operation to the extent that it cannot be reliably used for matching, a lower bound on the number of minutiae is set. After each iteration, if the IMR improves, the current template (IMR_{curr}) is replaced with the new template (IMR_{temp}). Hence, the algorithm "hill climbs" to increase the IMR. The SAMP is modified until the maximum number of iterations is reached or the IMR attains a predefined maximum value.

V. Experimental Results

To investigate whether the generated MasterPrints successfully match with a large number of fingerprint impressions pertaining to multiple subjects, several experiments were conducted. In addition to determining the maximum value of

ϕ for which MasterPrints could be found, we also explored the scenario where an authentication system would permit a user to offer their fingerprints multiple times in the case of a failed authentication attempt. In the latter case, multiple MasterPrints are identified, and a successful authentication is claimed when any one of them incorrectly matches with the target subject. The questions of interest in this scenario are: What set of MasterPrints one would choose to increase the probability of success? What part of the fingers do MasterPrints typically come from? To address these questions, a collection of MasterPrints were identified from publicly available fingerprint datasets. Experiments on a capacitive fingerprint dataset, similar to the one used by Apple TouchID, showed that it is possible to break 6.88% of users' account in 5 attempts if the FMR setting of the matching algorithm (Verifinger 6.1 SDK) was set to 0.01% and each subject was enrolled with one finger and 12 partial impressions per finger. This is significantly higher than what has been estimated for PINs and passwords. Further, with higher FMR settings (lower security), it was possible to perform successful attacks on an even higher subject population. The rest of this section presents detailed results for not only a capacitive dataset but also with an optical dataset, thereby ensuring variation in quality as well as nature of partial prints.

The FingerPass DB7 dataset [18] consisting of images from a capacitive sensor and FVC 2002 DB1-A dataset consisting of images from an optical sensor were used in our experiments. The capacitive dataset comprises 8640 fingerprints of size 144 $\times$ 144 pixels and 500 dpi resolution from 720 fingers, each having 12 impressions. The data was collected using Authentec AES3400 sensor. The fingerprints from this dataset were used without any modifications, as these fingerprints were already partial in nature. It is assumed that there are substantial differences among the partial fingerprints captured from the same finger. From the optical dataset, partial fingerprints of size 150 $\times$ 150 pixels were created from the 800 full prints, as mentioned in Section III. To create the training and test datasets, each dataset was divided into two disjoint sets each containing data corresponding to 50% of the fingers. In the case of FVC dataset, both the training and test datasets consisted of 50 fingers with a total of 400 impressions each. Similarly, for the FingerPass dataset, the training and test sets each had 360 fingers resulting in a total of 4320 impressions in each set. The training sets were used to generate the MasterPrints based on the two techniques described in Section IV, while the test sets were used in the dictionary attack. This partitioning of each dataset into finger-disjoint training and test sets was done 5 times, resulting in 5 different estimates for dictionary attack success.

Using the Verifinger 6.1 SDK, first "all-to-all" matching was performed on the training sets of both the capacitive and optical fingerprints to determine the thresholds to be used for assessing the success of the dictionary attack. In all our experiments, we assume that the minutiae are defined by their position and orientation. The thresholds corresponding to three FMR values, i.e., 1%, 0.1% and 0.01%, were used in our experiments to observe how the MasterPrints perform under different security settings (lower FMR increases the system security). Table I shows the thresholds and the TMR values corresponding to these three FMR values. Since the capacitive dataset itself is partial in nature, the TMR was lower than the optical dataset.

TABLE I

THRESHOLD SELECTION CORRESPONDING TO DIFFERENT FMR SETTINGS OF THE MATCHING ALGORITHM

	Capacitive Dataset			Optical Dataset		
	1% FMR	0.1% FMR	0.01% FMR	1% FMR	0.1% FMR	0.01% FMR
Threshold	35	50	65	18	30	40
TMR (%)	80.85	71.28	62.42	99.29	99.18	99.04

TABLE II

THE PERCENTAGE OF IMAGES IN THE PARTIAL FINGERPRINT POPULATION THAT MATCHED WITH THE TOP 5 INDEPENDENT SAMPS ARE SHOWN IN TERMS OF IMPOSTER MATCH RATE (%). CAPACITIVE SAMPS PERFORMED BETTER THAN THE OPTICAL SAMPS AT LOWER SECURITY SETTINGS (HIGHER FMR)

Rank	Capacitive Dataset			Optical Dataset		
	1% FMR	0.1% FMR	0.01% FMR	1% FMR	0.1% FMR	0.01% FMR
1	6.77%	1.31%	0.36%	3.51%	1.31%	0.56%
2	6.45%	1.12%	0.31%	3.31%	1.11%	0.50%
3	5.95%	1.08%	0.27%	3.13%	0.97%	0.45%
4	5.87%	1.03%	0.27%	2.97%	0.85%	0.40%
5	5.64%	0.98%	0.25%	2.94%	0.80%	0.38%

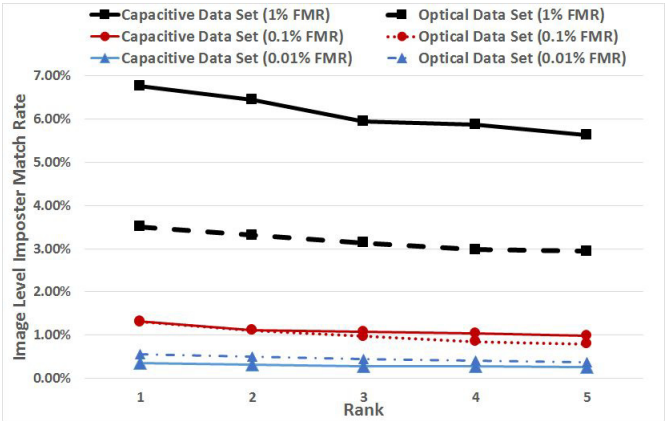

Fig. 2. Image-level Imposter Match Rate (%) using top 5 independent SAMPs corresponding to table II.

The experiments were performed in two phases: "*image-level comparison*" phase, where best SAMPs were identified by an "all-to-all" matching and "*finger-level comparison*" phase, where the selected SAMPs and the SYMPs generated from them were used to attack the subjects in the test set. Since the subjects in the two datasets used for our experimentation had impressions from only one finger, the term "subject" and "finger" will be used interchangeably in the rest of the paper.[2] The attack accuracy of a MasterPrint was measured in terms of IMR. Image-level comparison assesses the number of *images* against which a MasterPrint is successfully matched; while finger-level comparison assesses number of *fingers* against

[2]Note that the term "subject" is synonymous with "user" in this article.

Fig. 3. Minutiae location of top 5 partial fingerprints that were selected as MasterPrints from the FingerPass DB7 dataset.

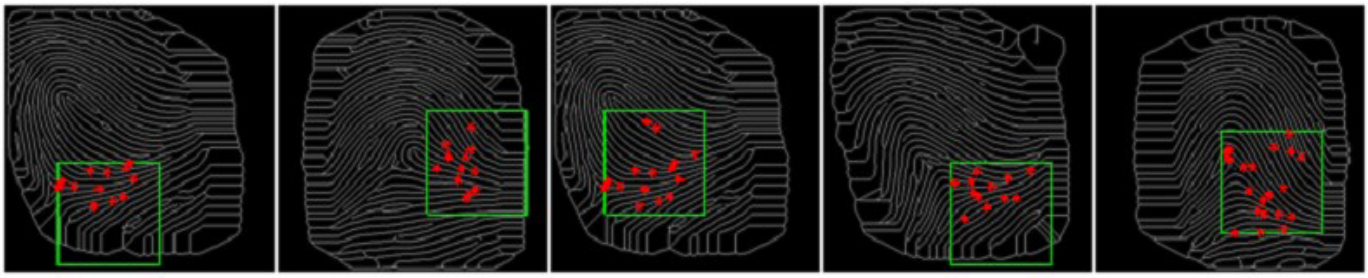

Fig. 4. Minutiae location of top 5 partial fingerprints that were selected as MasterPrints from the FVC 2002 DB1-A dataset.

which a MasterPrint is successfully matched. Consider a dataset of 50 fingerprint images corresponding to 5 different fingers with 10 impressions per finger. If a MasterPrint matches with 25 images corresponding to 3 fingers, then the result of image-level comparison would be 25 and finger-level comparison would be 3.

A. Image-Level Comparison

In a dictionary attack, an attacker will try out a pre-defined set of fixed fingerprints to access the system. In this regard, we create a fingerprint dictionary consisting of MasterPrints that sequentially increase the probability of matching a large number of target prints.

1) Independent SAMP Selection: In FingerPass DB7 dataset, each of the 4320 fingerprints corresponding to 360 subjects were compared with all fingerprints of the other 359 subjects. The partial prints corresponding to the 5 highest IMRs were chosen as the Sampled MasterPrints. The IMRs were computed for each of the three FMR settings in 5 cross-validation trials giving different sets of SAMPs for different trials. Table II summarizes these results. Figure 2 shows the drop in IMR when the FMR is decreased, i.e., when the security of the authentication system is increased.

The top 5 SAMPs from the FingerPass dataset are shown in Figure 3. It can be observed that the fingerprint patterns and the spatial distribution of the minutiae of these automatically selected SAMPs are quite different. For example, the third SAMP covers the right side of the core while the fourth SAMP covers the left side of the core. Together, these 5 SAMPs span over different portions of the full fingerprint, which in turn increases the probability of matching with a large number of imposter partial fingerprints irrespective of their spatial location.

Similarly, from the FVC 2002 DB1-A dataset, the SAMPs were identified from the partial prints generated from 50 fingers. It can be observed from Table II that the IMR decreases at lower FMRs (as expected).

The full fingerprint images from which the top 5 SAMPs were extracted are shown in Figure 4. The minutiae locations corresponding to only these SAMPs are shown here. It can be observed that the SAMPs are mostly located in the lower regions of the full prints, and dense distribution of minutiae usually occurred near the core and delta regions of the fingerprints. This observation is consistent with the previous work of Cao *et al.* [9] who pointed out that low discriminative minutiae configurations usually exist in these regions. Further, they found that these spatial minutiae configurations lead to high FMR with higher probability. Their observation is supported by our experimental results.

If the SAMPs from capacitive and optical datasets are compared, it can be noticed that the optical SAMPs are more diverse in terms of their position within the corresponding full fingerprints. The inherent nature of the source of the partial fingerprints in the two datasets is the reason behind such diversity. Since the partial fingerprints of the capacitive dataset were obtained directly from the sensor, where the users tend to position the center of their fingertip on the sensor, almost all of the captured partial fingerprints contained the core (when present). On the other hand, the partial fingerprints extracted from the images in the optical dataset are more uniformly distributed over the full fingerprint. Therefore, the SAMPs also show more diversity in the optical dataset in terms of their position in the fingertip.

2) Sequential SAMP Selection: Here, we assume that the attacker can launch multiple attempts to break into the system. Therefore, we determine the SAMPs (5 attempts) that can sequentially increase the probability of forcing an impostor

TABLE III

PERCENTAGE OF IMAGES IN THE PARTIAL FINGERPRINT POPULATION THAT MATCHED WITH THE TOP 5 SEQUENTIAL SAMPS ARE SHOWN HERE. AS IN THE CASE OF INDEPENDENT SAMPS, CAPACITIVE SAMPS PERFORMED BETTER THAN THE OPTICAL SAMPS AT HIGHER FMR VALUES

Rank	Capacitive Dataset			Optical Dataset		
	1% FMR	0.1% FMR	0.01% FMR	1% FMR	0.1% FMR	0.01% FMR
1	6.77%	1.31%	0.36%	3.51%	1.31%	0.56%
2	5.06%	1.06%	0.31%	2.81%	0.73%	0.44%
3	4.11%	0.91%	0.26%	2.10%	0.68%	0.40%
4	3.38%	0.83%	0.25%	1.65%	0.57%	0.33%
5	2.87%	0.77%	0.22%	1.59%	0.52%	0.28%
Total	22.19%	4.89%	1.40%	11.67%	3.81%	2.01%

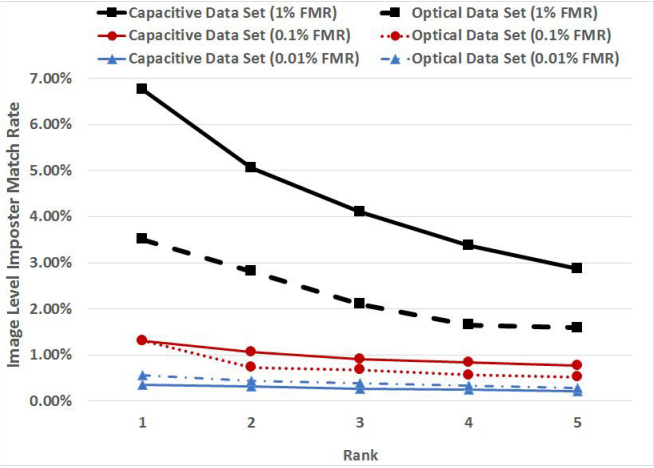

Fig. 5. Image-level Imposter Match Rate (%) when using the top 5 sequential SAMPs corresponding to table III.

match.

In this case, the top 5 SAMPs were selected sequentially. At first, the IMRs of all the partial fingerprints in the training dataset were computed and the print with the highest IMR was selected. The selected partial print and all the partial fingerprints that matched with it were excluded from the training set. Then, the IMRs of the remainder of the partial prints in the reduced training set were computed in order to select the next partial print. This process was repeated until there were 5 partial prints selected. Table III shows the average image-level IMRs of the top 5 sequential SAMPs obtained over 5 different trials. Sequentially, these 5 SAMPs matched with 1.40-22.19% of the fingerprint population of the FingerPass dataset. Figure 5 shows the variation in IMR when using different ranked MasterPrints. In case of the FVC dataset, these 5 SAMPs matched with 2.01-11.67% of the 4110 partial fingerprints. Thus, image-level probability of matching was found to be in the range of 1.40-22.19% for FingerPass and 2.01-11.67% for FVC, when the MasterPrints were used to match the fingerprints in the training dataset.

B. Finger-Level Comparison

In finger-level comparison, we replicate the situation of a dictionary attack on a fingerprint dataset that is unknown to the attacker. Here, if any one of the imposter match scores generated when comparing a MasterPrint with the multiple partial or full print templates corresponding to a finger is higher than a specified threshold, a match is declared. To explore whether MasterPrints can also be used for full fingerprint attack, we computed full fingerprint based MasterPrints and compared their performance with partial fingerprint based MasterPrints. Detailed results with sampled as well as synthetic MasterPrints are described below. For finger-level matching, the test datasets created in each of the 5 trials were used.

It must be noted that, during evaluation, the size of the FVC2002 DB1-A dataset used for the full fingerprints (400) is less than that of the partial fingerprints ($\approx$ 4110). There are two common data imbalance compensation methods, (i) over-sampling and (ii) under-sampling. Over-sampling can be done in two ways: by duplicating the existing fingerprint impressions or by generating them synthetically. While the duplication approach can easily lead to over-fitting due to the lack of new information in the sampled dataset, the use of synthetic dataset may cause over-generalization. Moreover, the quality of the synthetic fingerprint may also affect the results. Further, it has been shown that the under-sampling method can delete crucial data [6], [11], which may adversely impact the performance. Therefore, in subsequent experiments, we avoided using any data imbalance compensation techniques and employed the original datasets for testing the attack accuracy using MasterPrints.

1) Results With Sampled MasterPrints: Finger-level matching is performed on the test dataset with the independent SAMPs as well as the sequential SAMPs. While the top SAMP was compared with all the impressions of the available subjects,[3] successive SAMPs were matched with only those impressions corresponding to the subjects that were not already matched by the higher ranked SAMPs. Thus, the finger-level IMR represents the percentage of subjects in the population matched by the 5 SAMPs sequentially.

The finger-level IMR was calculated at different FMR values for each set of 5 SAMPs corresponding to the 5 test trials. The combined average finger-level IMR is, therefore, the average IMR over these 5 trials. Further, the combined average finger-level IMR was computed as a function of the number of fingerprint impressions per finger. As the number of impressions per finger is increased, it is expected that the chance of matching the MasterPrint with any one of them will also increase. Thus, the IMR will gradually improve with increasing number of impressions per finger. Here, we assume that the partial fingerprints corresponding to a finger are sufficiently dissimilar to each other. Otherwise, increasing the number of impressions per finger will not favorably affect the IMR. Next, we present experimental results to support this hypothesis.

a) Attack against full fingerprints: Since the fingerprints in the FingerPass DB7 dataset are already partial in nature, we used the FVC2002 DB1-A dataset that has full fingerprints. The sequential and independent SAMPs were identified by

[3]We use the terms "subject" and "finger" interchangeably since every subject has samples corresponding to only a single finger.

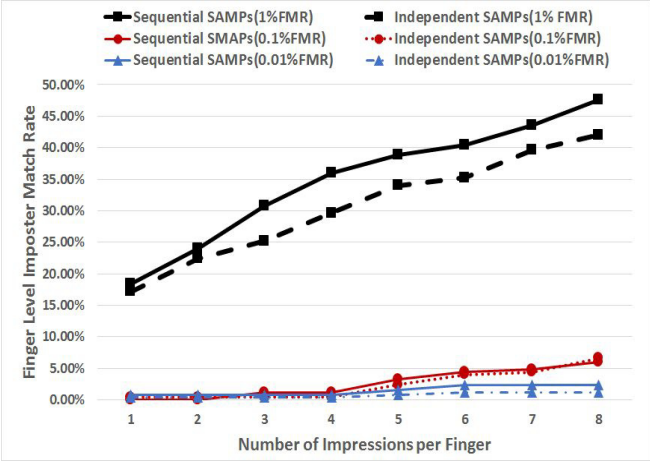

Fig. 6. Finger-level Imposter Match Rate variation as a function of the number of impressions per finger using the top 5 full fingerprint based SAMPs from the FVC 2002 DB1-A dataset. At the 0.1% and 0.01% FMR security settings, both the sequential as well as independent SAMPs exhibited very low IMR.

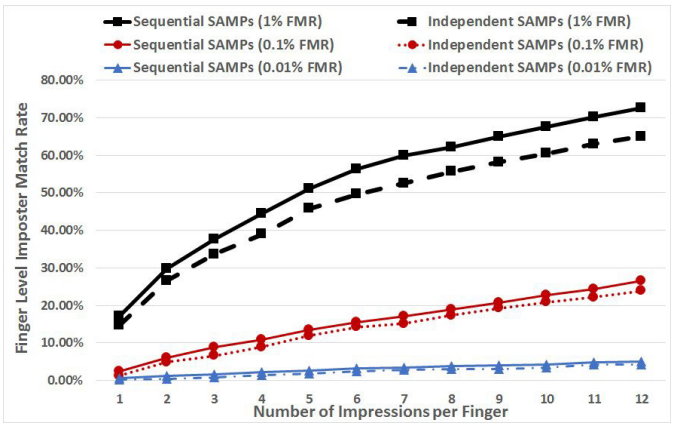

Fig. 7. Finger-level Imposter Match Rate variation as a function of the number of impressions per finger using the top 5 SAMPs from the FingerPass DB7 dataset. When the number of impressions per finger is increased, IMR increases gradually.

performing image-level comparison as described in the previous section. Every SAMP was compared with 400 unseen full fingerprints corresponding to 50 subjects in the test dataset. Figure 6 shows the variation in the combined average finger-level IMR when the number of full fingerprints per finger was increased from 1 to 8. Even when using the 5 top SAMPs together, the probability of matching is observed to be quite low at the 0.1% and 0.01% FMR security settings.

b) Attack against partial fingerprints: Now, we present the performance of partial fingerprint based SAMPs from both the capacitive as well as optical datasets. In case of the FingerPass DB7 dataset, the number of partial fingerprints was varied from 1 to 12. Figure 7 shows the variation in the combined average finger-level IMR when increasing the number of impressions per finger. For example, at an FMR of 0.1%, the IMR increased from 1.32% to 23.9% when the number of impressions per finger was increased from 1 to 12 using independent SAMPs.

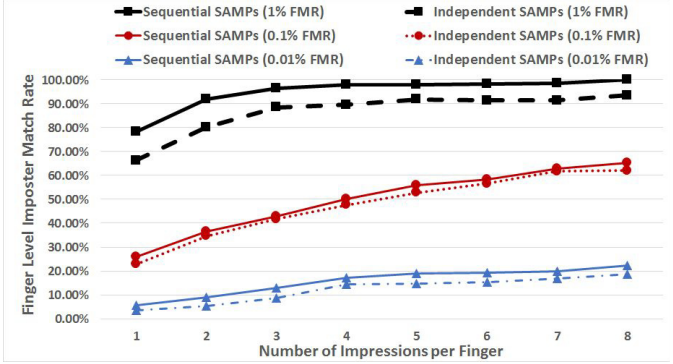

Fig. 8. Finger-level Imposter Match Rate variation as a function of the number of impressions per finger (each impression of a finger having ≈ 10 partial fingerprints) using the top 5 partial fingerprint based SAMPs from the FVC 2002 DB1-A dataset. Further, the partial fingerprint based SAMPs performed much better than that of the full fingerprint based SAMPs (see Figure 6).

Further, it can be observed that the sequential SAMPs performed marginally better than the independent SAMPs irrespective of the number of impressions per finger. The IMR using sequential SAMPs at an FMR of 0.1% increased from 2.4% to 26.5% when the number of impressions per finger was increased from 1 to 12.

Similar experiments were also performed on the partial fingerprints of FVC 2002 DB1-A dataset. Figure 8 shows the variation in the combined average finger-level IMR when the number of full fingerprints per finger was increased from 1 to 8. At a 0.1% FMR, the IMR of the independent SAMPs ranged from 22.8% − 62.0% with 1 - 8 impressions per finger, while the IMR of sequential SAMPs ranged from 26.0% − 65.2% IMR. Therefore, in the experiments below we only consider the 5 sequential SAMPs.

When these results are compared with the corresponding FingerPass dataset results, it can be observed that the optical SAMPs performed far better than the capacitive SAMPs in terms of IMR. There could be multiple reasons behind this. First, the difference in sensor type causes differences in image quality. Second, as pointed out in Section V.A.1, the diverseness in optical SAMPs is more than that in capacitive SAMPs. This in turn can increase the probability of matching with a large number of imposter partial fingerprints irrespective of their capture location. Thirdly, the nature of partial fingerprints in the two datasets are quite different. Since almost all the partial fingerprints in the capacitive dataset contained the core region, the imposter match probability was lower compared to that of partial fingerprints from the optical dataset, which were uniformly cropped from a full fingerprint.

Further, the partial fingerprint based SAMPs show much better performance than that of the full fingerprint based SAMPs. Specifically, at strong security settings (0.1% − 0.01% FMR), the IMR of the full fingerprint based sequential SAMPs was low (6.6% − 2.4%) compared to the partial fingerprint based sequential SAMPs (65.2% − 22.2%). These results confirm that not only is the proportion of MasterPrints much higher in the partial fingerprint dataset, but that these MasterPrints perform much better than the corresponding full fingerprint based MasterPrints.

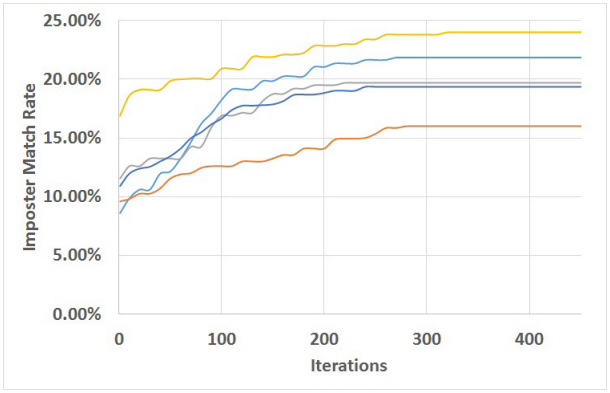

Fig. 9. Improvement in Imposter Match Rate of the top 5 sequential SAMPs with increasing number of iterations in the hill-climbing method.

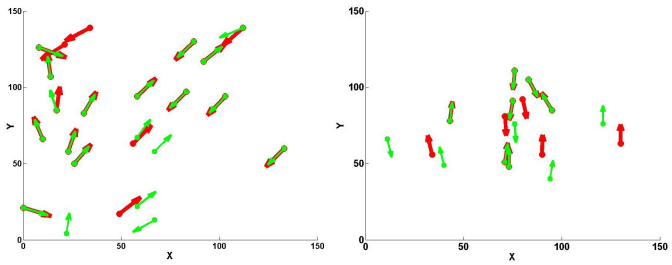

Fig. 10. Minutiae location in two MasterPrint templates. The red minutiae are the original ones in the seed template and the green minutiae are the updated ones in the corresponding synthetic template.

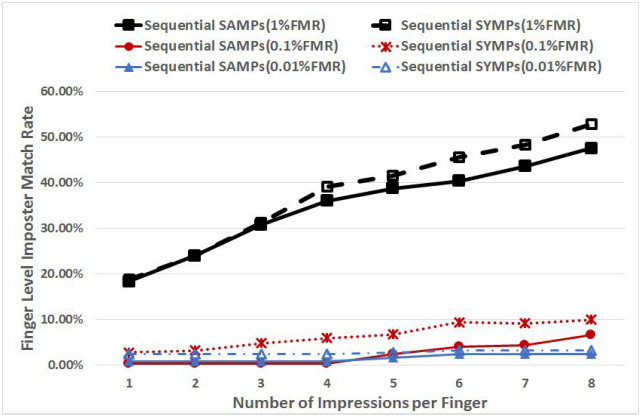

Fig. 11. Finger-level Imposter Match Rate using full fingerprint based SAMPs and SYMPs on the FVC 2002 DB1-A dataset. The IMR of SYMPs was observed to be better than that of SAMPs by $\approx 2\%$.

If the finger-level matching results on the two datasets are compared against that of the image-level matching results in Tables II and III, it can be observed that although the optical MasterPrints matched with lower number of partial *fingerprint impressions* than the capacitive MasterPrints, they matched with higher number of *fingers* than the capacitive ones. Thus, although the optical MasterPrints seem to be weaker based on the image-level comparison results, they turn out to be stronger than the capacitive MasterPrints based on the finger-level comparison. The difference in the number of partial fingerprints corresponding to a finger in the two datasets could be the reason behind this. The number of partial fingerprint impressions per finger in the optical dataset is 8×10 (average) ≈ 80, whereas in the capacitive dataset there are 12 impressions per finger. During finger-level matching, a match is declared if the Masterprint matches with any 1 of the 80 partial fingerprints in the optical dataset. Since the number of partial prints per finger is higher in the optical dataset, the probability of finger-level matching is also higher compared to the capacitive dataset.

2) Results With Synthetic MasterPrints: In this section, the results of finger-level matching using the synthetically generated MasterPrints, SYMPs, are presented. The SYMPs were generated from the training datasets by applying the hill-climbing method (described in Section IV) on the top 5 sequential SAMPs. The SAMPs are modified until the IMR is stabilized. If the IMR remains unchanged for a predefined number of iterations, it is assumed that the performance has been stabilized. Figure 9 shows the change in IMR values as a function of the number of iterations, for the top 5 sequential SAMPs. The hill-climbing process is terminated if the IMR values remain fixed over 100 iterations. As can be seen from the figure, the IMR is steadied after 350 iterations. Figure 10 shows the change in minutiae configuration after applying the hill-climbing method. The original positions of the minutiae in the SAMPs are shown in red. The updated minutiae in the corresponding SYMPs are shown in green. It should be noted that reconstruction of the actual fingerprint image corresponding to the synthetic "template" has not been done here.

Next, these SYMPs were used to launch a dictionary attack on the test datasets. The finger-level IMR for each set of 5 SYMPs was computed at different FMR values and over 5 different trials. As in the previous subsection, the combined finger-level IMR was computed as the summation of all the finger-level IMRs obtained by the 5 sequential SYMPs. Then, the final combined average finger-level IMR was computed by averaging over the 5 trials (cross-validation). Like before, the combined average finger-level IMR was computed as a function of the number of fingerprint impressions per finger.

a) Attack against full fingerprints: The SYMPs created from the corresponding full fingerprint based SAMPs were now used to attack the full fingerprints in the FVC 2002 DB1-A dataset. Figure 11 shows the variation in the combined average finger-level IMR when the number of full fingerprints per finger was increased from 1 to 8. The SYMPs were observed to perform better than the corresponding SAMPs. At 0.1% FMR, the IMR increased from 0.4% to 2.8% when only one impression per finger was used. When 8 impressions per finger were used, the IMR increased from 6.6% to 10.0%.

b) Attack against partial fingerprints: Next, performance of the synthetic MasterPrints obtained from the partial fingerprint datasets is presented. Figure 12 shows the IMR results of the SYMPs and the corresponding SAMPs on the FingerPass DB7 dataset. Here too the SYMPs are observed to perform better than the corresponding SAMPs. For example, at a 0.1% FMR, the IMR increased from 2.4% to 3.7% when only one impression per finger was used. When 12 impressions per finger were used, the IMR increased from 26.4% to 30.8%.

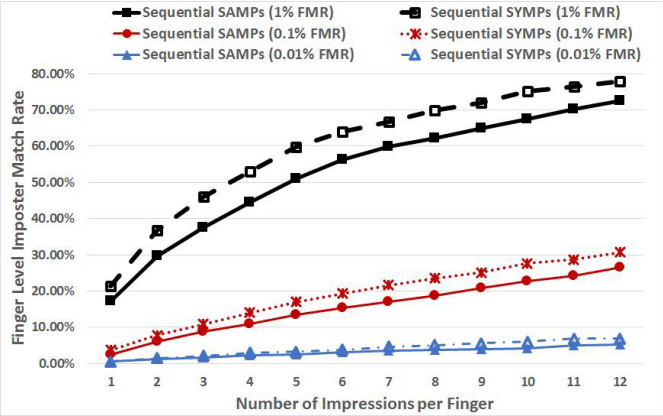

Fig. 12. Finger-level Imposter Match Rate using SAMPs and SYMPs on the FingerPass DB7 dataset. Using the SYMPs, the average improvement over the SAMPs in all settings was $\approx 4\%$. At a higher FMR, the improvement was more pronounced compared to a lower FMR setting. Further, with increasing number of impressions per finger, the margin of improvement also increased.

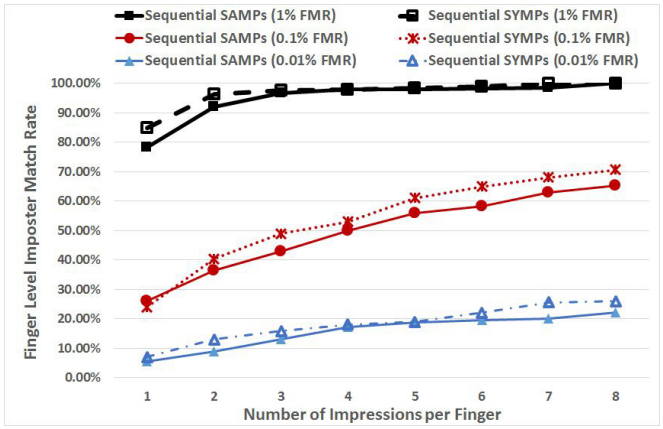

Fig. 13. Finger-level Imposter Match Rate using the partial fingerprint based SAMPs and SYMPs on the FVC 2002 DB1-A dataset. There were ≈ 10 partial fingerprints corresponding to each impression of a finger. The IMR of SYMPs is observed to be better than that of SAMPS by $\approx 3\%$. Overall, the partial fingerprint based SYMPs continued to perform better than the full fingerprint based SYMPs shown in Figure 11.

Finger-level Imposter Match Rate using the partial fingerprint based SAMPs and SYMPs on the FVC 2002 DB1-A dataset. There were ≈ 10 partial fingerprints corresponding to each impression of a finger.

Figure 13 shows comparative IMR results on the partial fingerprints of the FVC 2002 DB1-A dataset. Like before, the SYMPs are observed to result in better performance than the SAMPS. The results also indicate the importance of the *number* of prints and the *type* of prints that are stored for each user in a partial fingerprint based authentication system.

Performance comparison of the partial fingerprint based SYMPs with the full fingerprint based SYMPs suggests that partial fingerprint based SYMPs continue to exhibit higher accuracy in terms of IMR. Moreover, the degree of improvement of partial fingerprint based SYMPs over the corresponding SAMPs is more than that of the full fingerprint based SYMPs. These results further strengthen our hypothesis that the probability of finding MasterPrints with high accuracy is greater in a partial print dataset than a full print dataset.

VI. Discussion and Future Work

This work exposes a vulnerability of fingerprint authentication systems that use partial fingerprints for user recognition. Specifically, we discussed the generation of a MasterPrint that could be used to launch a dictionary attack. Experiments were carried out using a commercial fingerprint verification software on two different fingerprint datasets, viz., the FVC2002 DB1-A optical dataset and the FingerPass DB7 capacitive dataset. Two approaches to generate MasterPrints were presented in this paper. The efficacy of both approaches were tested on the two datasets. The main findings of this work are as follows:

1) The work establishes the fact that it is indeed possible to perform a dictionary attack on a fingerprint dataset with substantial accuracy using a set of carefully chosen MasterPrints. The MasterPrints can be either full or partial fingerprints sampled from a dataset or designed synthetically using a hill climbing method. However, the probability of finding MasterPrints from a partial fingerprint dataset and the accuracy of the ensuing attack are much higher than that of a full fingerprint dataset.
2) With a dictionary of 5 partial fingerprint based MasterPrints, and assuming a maximum of 5 attempts to be authenticated, it was possible to attack 26.46% users (each having 12 impressions per finger) in the FingerPass DB7 capacitive fingerprint dataset and 65.20% users (each having 8×10 (average) ≈ 80 partial impressions per finger) in the FVC optical fingerprint at a FMR of 0.1%. The attack accuracy varied greatly with the FMR value and the number of impressions per finger (for details refer to Section V.B.1).
3) It was observed that the synthetic MasterPrints, generated by a simple first-order hill climbing algorithm, are able to improve the attack accuracy over the sampled MasterPrints. On the capacitive dataset, the average improvement over all FMR settings was $\approx 4\%$ whereas on the optical dataset it was $\approx 3\%$ (for details refer to Section V.B.2). Thus, it can be concluded that properly designed synthetic MasterPrints can be used to perform dictionary attack with higher accuracy.
4) The minutiae distribution of the selected MasterPrints reveals that regions of high minutiae activity usually occurred in the upper delta point of the fingerprints. According to Cao *et al.* [9], these minutiae generally have lower discriminative power, which may lead to a higher imposter match rate.
5) Detailed analysis of the results reveals that even if a MasterPrint matches with a small number of partial fingerprints, the percentage of subjects that it matches against can be quite high. This is because, for each subject, multiple partial prints may be stored. For example, at a 0.1% FMR, a single MasterPrint (from the capacitive dataset) matched only 1.4% of the partial fingerprints, but this corresponded to 10.6% of the subjects owing to the fact that every subject had 12 impressions. It is clear that this risk would increase

if multiple fingers are enrolled for each subject. This observation indicates that the number as well as the type of partial fingerprint impressions to be stored for each finger should be judiciously chosen such that the chance of matching with an arbitrary finger is minimized as suggested in [37].

Together, these results illustrate the effectiveness of MasterPrints in launching a dictionary attack on partial fingerprint-based authentication systems. The work presented in this paper opens up several avenues for future research. Firstly, the impact of the distribution of the location of partial fingerprints on attack accuracy must be explored. Secondly, the process of generating synthetic MasterPrints can be improved. In this article, a rather simple (but effective) scheme was discussed. Thirdly, the synthetic MasterPrint generation technique discussed here modified an existing partial fingerprint at the "template-level" by minutiae manipulation. Such a modification can also be done at the "image-level" in order to construct a digital artifact, which can be potentially transferred to a physical artifact for launching a spoof-attack [20].

The results of this work must be used to better address the broader problem of designing trustworthy user authentication systems that utilize partial fingerprints. This could entail developing effective anti-spoofing schemes [20]; carefully selecting the number and nature of partial impressions of a user during enrollment [37]; improving the resolution of the small-sized sensors to facilitate extraction of more discriminative features [17]; developing matchers that utilize both minutiae and texture information [30]; and designing more effective fusion schemes to combine the information presented by multiple partial impressions of a user [29], [32].

APPENDIX

The size of the window was decided to approximately match the size of the fingerprint image captured by the Apple Touch ID sensor which is composed of an 8×8 millimeter ($0.3" \times 0.3"$) capacitive sensor of 500 dpi resolution [5]. But, average finger dimension is $0.5" \times 0.7"$ [4]. Thus, Apple Touch ID captures only a part of fingerprint of image size 150×150 ($500*0.3 = 150$). To create similar sized partial fingerprints from FVC2002 DB1-A dataset having image resolution 500 dpi, the window size is chosen to be 150×150.

REFERENCES

[1] *About Touch ID Security on iPhone and iPad*, accessed on Jan. 2016. [Online]. Available: https://support.apple.com/en-us/HT204587

[2] *Chaos Computer Club Breaks Apple TouchID*, accessed on Jan. 2016. [Online]. Available: http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid

[3] European Association for Biometrics. *iPhone 5S: Heralding a Paradigm Shift?* accessed on Jan. 2016. [Online]. Available: http://perma.cc/U5H6-WTF5

[4] *A Technical Evaluation of Fingerprint Scanners*, accessed on Jan. 2016. [Online]. Available: http://www.biometrika.it/eng/wp_scfing.html

[5] *The Trouble With Apple's Touch ID Fingerprint Reader*, accessed on Jan. 2016. [Online]. Available: http://www.wired.com/2013/12/touch-id-issues-and-fixes/

[6] R. Akbani, S. Kwek, and N. Japkowicz, "Applying support vector machines to imbalanced datasets," in *Proc. Eur. Conf. Mach. Learn.*, 2004, pp. 39–50.

[7] J. Bonneau, "The science of guessing: Analyzing an anonymized corpus of 70 million passwords," in *Proc. IEEE Symp. Secur. Privacy*, May 2012, pp. 538–552.

[8] J. Bonneau, S. Preibusch, and R. Anderson, "A birthday present every eleven wallets? The security of customer-chosen banking pins," in *Financial Cryptography and Data Security*. Berlin, Germany: Springer-Verlag, 2012, pp. 25–40.

[9] K. Cao, E. Liu, L. Pang, J. Liang, and J. Tian, "Fingerprint matching by incorporating minutiae discriminability," in *Proc. Int. Joint Conf. Biometrics (IJCB)*, 2011, pp. 1–6.

[10] P. K. Chan and S. J. Stolfo, "Toward scalable learning with non-uniform class and cost distributions: A case study in credit card fraud detection," in *Proc. KDD*, 1998, pp. 164–168.

[11] D. Chetchotsak, S. Pattanapairoj, and B. Arnonkijpanich, "Integrating new data balancing technique with committee networks for imbalanced data: Grsom approach," *Cognit. Neurodyn.*, vol. 9, no. 6, pp. 627–638, 2015.

[12] N. Cubrilovic. (2009). *RockYou Hack: From Bad to Worse*, accessed on Jan. 2016. [Online]. Available: http://techcrunch.com/2009/12/14/rockyou-hack-security-myspace-facebook-passwords

[13] M. M. Devillers, "Analyzing password strength," Dept. Comput. Sci., Radboud Univ., Nijmegen, The Netherlands, Tech. Rep. 2, Jul. 2010.

[14] G. Doddington, W. Liggett, A. Martin, M. Przybocki, and D. Reynolds, "SHEEP, GOATS, LAMBS and WOLVES: A statistical analysis of speaker performance in the NIST 1998 speaker recognition evaluation," in *Proc. IEEE Int. Conf. Lang. Speech Process.*, Jan. 1998, pp. 1351–1354.

[15] B. B. Han, C. A. Marciniak, and W. C. Westerman, "Fingerprint sensing and enrollment," U.S. Patent 14/244 143, Apr. 3, 2014.

[16] M. Inuma, A. Otsuka, and H. Imai, "Theoretical framework for constructing matching algorithms in biometric authentication systems," in *Proc. Int. Conf. Biometrics*, 2009, pp. 806–815.

[17] A. K. Jain, Y. Chen, and M. Demirkus, "Pores and ridges: High-resolution fingerprint matching using level 3 features," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 1, pp. 15–27, Jan. 2007.

[18] X. Jia, X. Yang, Y. Zang, N. Zhang, and J. Tian, "A cross-device matching fingerprint database from multi-type sensors," in *Proc. 21st Int. Conf. Pattern Recognit. (ICPR)*, 2012, pp. 3001–3004.

[19] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. London, U.K.: Springer-Verlag, 2009.

[20] E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems," *ACM Comput. Surv.*, vol. 47, no. 2, p. 28, 2015.

[21] M. Martinez-Diaz, J. Fierrez, J. Galbally, and J. Ortega-Garcia, "An evaluation of indirect attacks and countermeasures in fingerprint verification systems," *Pattern Recognit. Lett.*, vol. 32, no. 12, pp. 1643–1651, 2011.

[22] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial 'gummy' fingers on fingerprint systems," *Proc. SPIE*, vol. 4677, pp. 275–289, Apr. 2002.

[23] R. Morris and K. Thompson, "Password security: A case history," *Commun. ACM*, vol. 22, no. 11, pp. 594–597, 1979.

[24] A. Nagar, H. Choi, and A. K. Jain, "Evidential value of automated latent fingerprint comparison: An empirical approach," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1752–1765, Dec. 2012.

[25] S. Pankanti, S. Prabhakar, and A. K. Jain, "On the individuality of fingerprints," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 24, no. 8, pp. 1010–1025, Aug. 2002.

[26] J. L. Perols, R. M. Bowen, C. Zimmermann, and B. Samba, "Finding needles in a haystack: Using data analytics to improve fraud prediction," *Accounting Rev.*, vol. 92, no. 2, pp. 221–245, 2016.

[27] N. Poh and J. Kittler, "A methodology for separating sheep from goats for controlled enrollment and multimodal fusion," in *Proc. Biometrics Symp.*, 2008, pp. 17–22.

[28] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *Audio- and Video-Based Biometric Person Authentication*. London, U.K.: Springer-Verlag, 2001, pp. 223–228.

[29] A. Ross, "Information fusion in fingerprint authentication," Ph.D. dissertation, Dept. Comput. Sci. Eng., Michigan State Univ., East Lansing, MI, USA, 2003.

[30] A. Ross, A. Jain, and J. Reisman, "A hybrid fingerprint matcher," *Pattern Recognit.*, vol. 36, no. 7, pp. 1661–1673, Jul. 2003.

[31] A. Ross, J. Shah, and A. K. Jain, "From template to image: Reconstructing fingerprints from minutiae points," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 544–560, Apr. 2007.

[32] A. Ross, S. Shah, and J. Shah, "Image versus feature mosaicing: A case study in fingerprints," *Proc. SPIE*, vol. 6202, pp. 620208-1–620208-12, Apr. 2006.

[33] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 5, no. 1, pp. 3–55, 2001.

[34] C. Sousedik and C. Busch, "Presentation attack detection methods for fingerprint recognition systems: A survey," *IET Biometrics*, vol. 3, no. 4, pp. 219–233, 2014.
[35] E. H. Spafford, "Observing reusable password choices," Dept. Comput. Sci., West Lafayette, IN, USA, Purdue Univ., Tech. Rep. 92-049, 1992.
[36] U. Uludag and A. K. Jain, "Attacks on biometric systems: A case study in fingerprints," *Proc. SPIE*, vol. 5306, pp. 622–633, Jun. 2004.
[37] U. Uludag, A. Ross, and A. Jain, "Biometric template selection and update: A case study in fingerprints," *Pattern Recognit.*, vol. 37, no. 7, pp. 1533–1542, 2004.
[38] M. Une, A. Otsuka, and H. Imai, "Wolf attack probability: A new security measure in biometric authentication systems," in *Proc. Int. Conf. Biometrics*, 2007, pp. 396–406.
[39] N. Yager and T. Dunstone, "The biometric menagerie," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 32, no. 2, pp. 220–230, Feb. 2010.
[40] *Fvc2002 Database*. Accessed Apr. 2017. [Online]. Available: http://bias.csr.unibo.it/fvc2002/databases.asp

Aditi Roy received the B.Tech. degree (Hons.) in electronics and instrumentation engineering from the West Bengal University of Technology, India, and the M.S. and Ph.D. degrees in computer science and engineering from IIT Kharagpur, India. She is currently a Post-Doctoral Fellow with the Department of Computer Science and Engineering, New York University Tandon School of Engineering. Her research interests lie in the area of biometrics, authentication, image and video processing, pattern recognition, and human–computer interaction.

Nasir Memon received the M.Sc. and Ph.D. degrees in computer science from the University of Nebraska. He is currently a Professor with the Department of Computer Science and Engineering, New York University (NYU) Tandon School of Engineering, the Director of the OSIRIS Laboratory, a Founding Member of the Center for Interdisciplinary Studies in Security and Privacy, and a Collaborative Multidisciplinary Initiative of several schools within NYU. He is also the Cofounder of Digital Assembly and Vivic Networks, two early stage startups in NYUs business incubators. He has authored over 250 articles in journals and conference proceedings and holds a dozen patents in image compression and security. His research interests include digital forensics, biometrics, data compression, network security, and usable security. He is a Distinguished Lecturer of the IEEE Signal Processing Society. He received several awards, including the Jacobs Excellence in Education Award and several best paper awards. He has been on the editorial boards of several journals and was the Editor-In-Chief of IEEE TRANSACTIONS ON INFORMATION SECURITY AND FORENSICS.

Arun Ross received the B.E. degree (Hons.) in computer science from the Birla Institute of Technology and Science, Pilani, India, and the M.S. and Ph.D. degrees in computer science and engineering from Michigan State University. He was with the Faculty of West Virginia University from 2003 to 2012. He is currently a Professor with the Department of Computer Science and Engineering, Michigan State University, and the Director of the i-PRoBe Laboratory. He has coauthored the textbook *Introduction to Biometrics* and the monograph *Handbook of Multibiometrics*. He was a recipient of the IAPR JK Aggarwal Prize, the IAPR Young Biometrics Investigator Award, and the NSF CAREER Award, and was designated a Kavli Frontier Fellow by the National Academy of Sciences in 2006. He was a recipient of the 2005 *Biennial Pattern Recognition Journal* Best Paper Award and the Five Year Highly Cited BTAS 2009 Paper Award.