Authentication Attacks on Projection-based Cancelable Biometric Schemes

Axel Durbet[1], Paul-Marie Grollemund[2], Pascal Lafourcade[1], Denis Migdal[1] and Kevin Thiry-Atighehchi[1]

[1]*Université Clermont-Auvergne, CNRS, Mines de Saint-Étienne, LIMOS, France*

[2]*Université Clermont-Auvergne, CNRS, LMBP, France*

Keywords: Cancelable Biometrics, Local-sensitive Hash, Sobel Filter, Reversibility Attacks, Biohash.

Abstract: Cancelable biometric schemes aim at generating secure biometric templates by combining user specific tokens, such as password, stored secret or salt, along with biometric data. This type of transformation is constructed as a composition of a biometric transformation with a feature extraction algorithm. The security requirements of cancelable biometric schemes concern the irreversibility, unlinkability and revocability of templates, without losing in accuracy of comparison. While several schemes were recently attacked regarding these requirements, full reversibility of such a composition in order to produce colliding biometric characteristics, and specifically presentation attacks, were never demonstrated to the best of our knowledge. In this paper, we formalize these attacks for a traditional cancelable scheme with the help of integer linear programming (ILP) and quadratically constrained quadratic programming (QCQP). Solving these optimization problems allows an adversary to slightly alter its fingerprint image in order to impersonate any individual. Moreover, in an even more severe scenario, it is possible to simultaneously impersonate several individuals.

1 INTRODUCTION

Biometric authentication is seeing widespread use due to the common integration of fingerprint sensors and cameras on many smart objects. Since biometrics is more convenient and quicker to use, and biometric characteristics cannot be lost or forgotten, biometric authentication solutions are in general preferred over their password or physical token counterparts. Despite their many advantages, biometric solutions are not exempt from vulnerabilities. As biometric-based technologies are deployed at a larger scale, centralized biometric databases and devices become natural targets in cyberattacks. These cyberattacks have the potential to be harmful on the long term if they lead to the theft of biometric data. Therefore, a biometric data may actually be vulnerable to impersonation attacks and privacy leakage.

Several criteria essential to biometric authentication systems have been identified in (ISO, 2011) and (ISO, 2018): irreversibility, unlinkability, revocability and performance preservation of templates. Fulfilling this set of criteria is now necessary to comply with the *privacy* principles of the GDPR.

Faced with the mentioned vulnerabilities and requirements, the community has proposed primitives dedicated to biometrics, so-called biometric template protection (BTP) schemes. In this paper, we focus on cancelable biometrics (CB) which is an example of BTP scheme claimed to meet the four criterias. For more details on BTP schemes, the reader is referred to two surveys (Nandakumar and Jain, 2015) and (Natgunanathan et al., 2016). In CB, a biometric template is computed through a process where the inputs are biometric data (*e.g.*, biometric image) of a user and a user specific token (*e.g.*, a random key, seed, salt, or password). A CB scheme generally consists of a sequence of processes (an extraction of features followed by a parameterized transformation) that produces the biometric templates, and a matcher to generate a matching score between the templates. With a CB scheme, templates can be revoked, changed, and renewed by changing user specific tokens. Cryptanalysis of CB schemes with strong adversarial models commonly assume that the attacker knows both the biometric template and token of the user. This assumption is plausible in practice because a user token may have low entropy (*e.g.*, a weak password), or it may just have been compromised by an attacker. This is the stolen-token scenario (Teoh et al., 2008).

In (Ratha et al., 2001), the first CB scheme was introduced in the case of face recognition. Since then, several CB schemes have been proposed, including the BioHash algorithm (Jin et al., 2004) applied on

Durbet, A., Grollemund, P., Lafourcade, P., Migdal, D. and Thiry-Atighehchi, K.
Authentication Attacks on Projection-based Cancelable Biometric Schemes.
DOI: 10.5220/0011277100003283
In *Proceedings of the 19th International Conference on Security and Cryptography (SECRYPT 2022)*, pages 568-573
ISBN: 978-989-758-590-6; ISSN: 2184-7711

many modalities. CB schemes offer several advantages such as efficient implementation, high matching accuracy, and revocability. However, several attacks on a variety of CB schemes have been proposed: attacks against privacy by approximating feature vectors or linking several templates of an individual, and authentication attacks by elevating the false acceptance rate (FAR). We refer the reader to (Nagar et al., 2010; Topcu et al., 2016) for attacks on BioHash type schemes, (Li and Hu, 2014) for attacks using the Attack via Record Multiplicity (ARM) technique, (Lacharme et al., 2013; Dong et al., 2019) for attacks using genetic algorithms, as well as attacks using constrained programming on CB schemes (Ghammam et al., 2020; Topcu et al., 2016).

Contributions. In this paper, we propose reversibility attacks against some projection-based CB schemes, such as the BioHash. The particularity of our attacks, as opposed to previous works, is that we reverse the complete sequence of treatments including the *feature extraction* algorithm. This allows us to construct impostor fingerprint images, thus enabling authentication (or presentation) attacks. In our authentication attacks, an adversary, who already has the knowledge of a user's specific token and has at least one fingerprint template of the same user, tries to alter her own fingerprint image such that the adversary can now use its own altered biometrics and the stolen token to be falsely authenticated as a legitimate user. The considered CB schemes are built upon uniform random projection (URP) and a kernel based feature extractor.To perform our attacks, we use Integer Linear Programming (ILP) as well as quadratically constrained quadratic programming (QCQP). We state our results as follows:

1) Simple Authentication Attacks. A complete reversal methodology of some projection-based CB schemes, including the BioHash algorithm, is proposed. The main ideas are to solve an integer linear program and a quadratically constrained quadratic program to reverse both the projection and the feature extraction. The solution provided by a solver is a fingerprint image of the attacker whose the amount of changes is minimized. Practical resolutions are provided for tiny synthetic images.

2) One Fingerprint Image for Several Impersonations. The first attack is extended to produce a single fingerprint image that impersonates the identity of several users. This fingerprint image, when combined with the distinct stolen tokens, produces templates that match exactly the stolen templates of the respective users. To reach this objective, the attack consists for the attacker to collect the pairs of (token, template) of the target users to enlarge the set of constraints of a QCQP program.

Outline. Some background information and the adversarial models are presented in Section 2. Section 3 provides our simple authentication attacks. Then, in Section 4, it is shown how to impersonate several users with different passwords. Finally, experimental evaluations and future works are discussed in Section 5 and Section 5 respectively.

2 BACKGROUND

Cancelable biometric schemes generate secure biometric templates by combining user specific tokens such as password with a biometric data to create templates in respect of the four aforementioned criteria. Biometric templates in CB schemes are constructed in two steps: (*i*) *Feature extraction*: A feature vector is derived from a biometric image; (*ii*) *Transformation*: A user specific token is used to transform the user's feature vector to a template.

In the following, we let $(\mathcal{M}_I, D_I)$, $(\mathcal{M}_F, D_F)$ and $(\mathcal{M}_T, D_T)$ be three metric spaces, where $\mathcal{M}_I$, $\mathcal{M}_F$ and $\mathcal{M}_T$ represent the fingerprint image space, the feature space and the template space, respectively; and D_I, D_F and D_T are the respective distance functions. Note that D_I and D_F are instantiated with the Euclidean distance, while D_T is instantiated with the Hamming distance.

2.1 Feature Extraction

Let $\mathcal{U}$ be the set of users of the biometric system. We identify a user with its biometric characteristic, and define a function $\mathcal{BC}(\cdot)$ that takes a biometric characteristic $usr \in \mathcal{U}$ as input, and outputs a digital representation of biometric data I; for instance, the scan image of a fingerprint. Note that for two different computations of $I = \mathcal{BC}(usr)$ and $I' = \mathcal{BC}(usr)$ (*e.g.*, at different times, or different devices), we may have $I \neq I'$ due to the inherent noise in the measurement of biometric data.

Definition 2.1. *A biometric feature extraction scheme is a pair of deterministic polynomial time algorithms* $\Pi := (E, V)$*, where:*

- *E is the feature extractor that takes biometric data I as input, and returns a feature vector $F \in \mathcal{M}_F$.*
- *V is the verifier that takes two feature vectors $F = E(I)$, $F' = E(I')$, and a threshold τ as input, and returns True if $D(F, F') \leq \tau$, and False otherwise.*

An example of feature extraction is Sobel filtering (Vincent and Folorunso, 2009). The resulting image is obtained by computing two convolutions given by the following matrices:

$$G_1 = \begin{pmatrix} 1 & 0 & -1 \\ 2 & 0 & -2 \\ 1 & 0 & -1 \end{pmatrix} \text{ and } G_2 = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{pmatrix}.$$

Let $*$ denote the operator of convolution and I the output matrix. Note that pixels at the edges of the image are ignored and, their values are set to 0 in the corresponding matrix I. The gradients, G_x and G_y, are computed as follows $G_x = G_1 * I$ and $G_y = G_2 * I$. Then, the matrix of the output image S is computed as $\|G_x + G_y\|_2$ where $\|\cdot\|_2$ denotes the Euclidean norm. However, the norm does not apply in the usual way. In this case, it is applied coordinate by coordinate.

2.2 Generation of Templates with URP

Definition 2.2. *Let $\mathcal{K}$ be the token (seed) space, representing the set of tokens to be assigned to users. A cancelable biometric scheme is a pair of deterministic polynomial time algorithms $\Xi := (\mathcal{T}, \mathcal{V})$, where:*

- *$\mathcal{T}$ is the transformation that takes a feature vector $F \in \mathcal{M}_F$ and the token parameter P as input, and returns a biometric template $T = \mathcal{T}(P,F) \in \mathcal{M}_T$.*
- *$\mathcal{V}$ is the verifier that takes two biometric templates $T = \mathcal{T}(P,F)$, $T' = \mathcal{T}(P',F')$, and a threshold τ_T as input; and returns True if $D_T(T,T') \leq \tau_T$, and returns False otherwise.*

The attacked CB instantiation, described in Algorithm 1, is based on a uniform random projection (*URP*). Such a projection serves as an embedding of a high-dimensional space into a space of much lower dimension while preserving approximately the distances between all pairs of points. Algorithm 1 assumes the second factor, *i.e.*, the token, is a password and outputs a *Biometric Compressed Vector* (BCV).

Remark 2.2.1. *BioHash instantiation is based on the same type of projection, except that an additional step of orthonormalization. This skipped step affects neither the accuracy nor the feasibility of the attacks.*

2.3 Attack Models and Objectives

The objective of our attack is to impersonate one or several users of a database. To perform this attack some information are needed: the password of our target and the original BioHash of the target. We show that anybody can perform a simple authentication attack or a one fingerprint image for several impersonations attack by building a template preimage if he knows the above information.

Algorithm 1: [URP-SOBEL].

Inputs : biometric data I; token parameter P
Output : BCV vector $T = (t_1, \ldots, t_m)$

1: Apply Sobel filter on I to produce an n-sized feature vector: $F = (f_1, \ldots, f_n)$.
2: Generate with the token P a family V of m pseudorandom vectors $V_1, \ldots, V_m$ of size n according to a uniform law $\mathcal{U}([-0.5, 0.5])$.
3: Arrange the family V as a matrix M of size $n \times m$.
4: Compute T as the matrix-vector product $F \times M$.
5: **for** t_i in T **do**
6: **if** $t_i < 0$ **then** $t_i = 0$ **else** $t_i = 1$
7: **end for**
8: **return** T

The informal definitions of (Ghammam et al., 2020) are tailored for the rest of the paper. Let $I \in \mathcal{M}_I$ be a fingerprint image, and let $T = \Xi.\mathcal{T}(P,E(I)) \in \mathcal{M}_T$ be the template generated from I and the secret parameter P. In our authentication attack, an adversary is given T, P, and a threshold value τ_T, and the adversary tries to find a fingerprint image $I^* \in \mathcal{M}_I$ such that for $T^* = \Xi.\mathcal{T}(P,E(x^*))$, T^* is exactly the same as T, or T^* is close to T with respect to the distance function over $\mathcal{M}_T$ and the threshold value τ_T. In this case, we say that I^* is a τ_T-nearby-template preimage of the template T.

A strategy for the adversary which have stolen the secret parameter P is to alter her fingerprint image I_A such that P along with her extracted feature vector F_A enable the generation of the exact template T. This motivates the notion of *template fingerprint preimage* defined below.

Definition 2.3 (Template Fingerprint Preimage)**.** *Let $I \in \mathcal{M}_I$ be a fingerprint image, and $T = \Xi.\mathcal{T}(P,\Pi.E(I)) \in \mathcal{M}_T$ a template for some secret parameter P. A template preimage of T with respect to P is a fingerprint image I^* such that $T = \Xi.\mathcal{T}(P,\Pi.E(I^*))$.*

Another authentication attack consists in generating a fingerprint image that yields the exact templates of several distinct users with their corresponding stolen tokens.

Definition 2.4 (n-template Fingerprint Preimage)**.** *Let $I_1, \ldots, I_n \in \mathcal{M}_I$ be n fingerprint images of distinct users, and n templates $T_i = \Xi.\mathcal{T}(P_i,\Pi.E(I_i)) \in \mathcal{M}_T$ for distinct secret parameters P_i $\forall i \in \{0, \ldots, n\}$. A n-template preimage of $(I_1, \ldots, I_n)$ with respect to $(P_1, \ldots, P_n)$ is a fingerprint image I^* such that:*

$$\forall i \in \{0, \ldots, n\}, T_i = \Xi.\mathcal{T}(P_i,\Pi.E(I^*)).$$

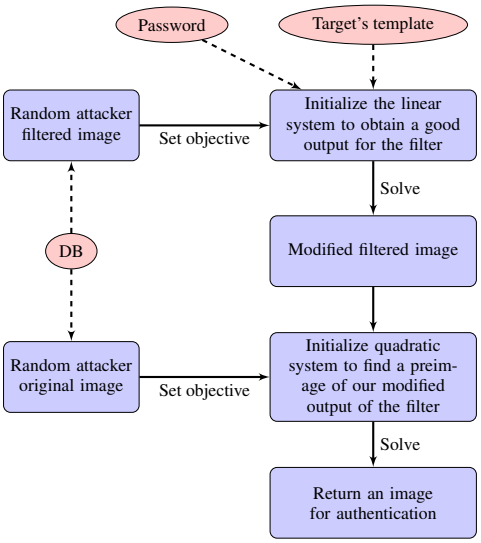

Figure 1: Principle of the attack's first approach.

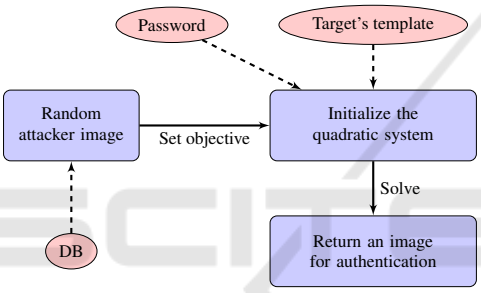

Figure 2: Principle of the attack's second approach.

3 SIMPLE AUTHENTICATION ATTACK

There are two ways of performing this attack. The first one includes two steps described in Section 3.1. First, given an attacker feature vector, we seek the slightest modification of it such that its transformation by Ξ yields exactly the template of the victim. Then, using the filter constraints of the convolution, we seek the slightest variation of the attacker's image such that the filtering of this variation produces exactly the modified feature vector. The second approach described in Section 3.2 consists in generating all constraints at once and directly generating the modified attacker's image.

3.1 Two-phase Approach Formulation

The attack takes as input: the target's password (P_t), the target's template (T_t) and the attacker's image (I_A). This attack computes and uses these intermediate information: the attacker's derivative features (F_A) and the modified attacker's features (F'_A). The output is a modified attacker's image X whose complete transformation using P_t matches exactly T_t.

First, the attacker ($\mathcal{A}$) uses I_A to compute the derivative F_A using the filter. Then, $\mathcal{A}$ computes her modified image's features F'_A whose derived template using P_t matches exactly the target template T_t. As described in Section 3.1.1, this is done by solving an under-constrained linear system and seeking the nearest modified features whose derived template using P_t matches exactly T_t. Next, using F'_A and I_A, $\mathcal{A}$ computes her modified image X whose image derivative by Sobel filter matches exactly the modified features F'_A. As described in Section 3.1.2, this is done by solving an under-constrained quadratic system and seeking the nearest modified image X whose Sobel derivative matches exactly the features F'_A. Figure 1 gives an overview of this first method step by step, where inputs are in circles and different steps in boxes.

3.1.1 Getting a Correct Output for the Filter

For this part, we assume that we are after the filter. We want to reverse target's template by using the password. To do that, let $X = (x_0, \ldots, x_n)$, M the projection matrix derivated from target's password and f the quantization function which takes XM to create a binary template.

We know the projection matrix and the template T. Thus, a pre-image of the projected vector can be find by solving a system under constraints. Notice that the proposed attack works for many projections system such as BioHash.

Let $\mathcal{K}_1$ be all indices where T is equal to 0 and $\mathcal{K}_2$ all other indices. So, we seek a solution to the following system:

$$\begin{cases} XM_i < 0, \forall i \in \mathcal{K}_1 \\ XM_i \geq 0, \forall j \in \mathcal{K}_2 \\ x_i \in \mathbb{R}^+, \forall i \in (\mathcal{K}_1 \cup \mathcal{K}_2) \end{cases}$$

With M_i the i-th column of M. We seek to minimize the distance between F and F_A. By doing so, the attacker can be authenticated by modifying the smallest number of information of her own biometric feature vector.

This part of the attack solves the following problem. By taking $F_A = (o_1, \ldots, o_n)$ the attacker's biometric features, M the projection matrix we have:

- Minimize: $\|X - F_A\|^2$
- Under the following constraints:

$$\begin{cases} XM_i < 0, \forall i \in \mathcal{K}_1 \\ XM_i \geq 0, \forall j \in \mathcal{K}_2 \\ x_i \in \mathbb{R}^+, \forall i \in (\mathcal{K}_1 \cup \mathcal{K}_2) \end{cases}$$

With M_i the i-th column of M.

3.1.2 Get a Preimage to Avoid Filter Effect

The filter leads to a loss of information. But we can write a quadratic system to create a collision and get a correct preimage. Let the image matrix be

$$I = \begin{bmatrix} o_{0,0} & \cdots & o_{0,\text{width-1}} \\ \vdots & \ddots & \vdots \\ o_{\text{length-1},0} & \cdots & o_{\text{length-1,width-1}} \end{bmatrix}$$

Applying the filter to that formal matrix yields a new matrix D which has quadratic components. But, we know that D must be equal to F_A. Thus, we can solve a quadratic system with (length $\times$ width) equations and (length $\times$ width) variables to find a preimage.

Let $I_A = (o_{i,j})$ denote the attacker's original image, $F_A = (a_{i,j})$ its modified features, $I' = (x'_{i,j})$ the modified original image and $X = (x_{i,j})$ its augmented form. We consider the augmented form as the original matrix where zeroes are added all around the matrix to compute the convolution without overflowing.

In the case of Sobel filter, we solve the following problem:

- Minimize: $\sum_{i,j}(o_{i,j} - x_{i,j})^2$
- Subject to the following constraints:

$$\begin{cases} \alpha_{i,j} = x_{(i-1,j-1)} + 2x_{(i,j-1)} + x_{(i+1,j-1)} \\ \qquad - x_{(i-1,j+1)} - 2x_{(i,j+1)} - x_{(i+1,j+1)} \\ \beta_{i,j} = x_{(i-1,j-1)} + 2x_{(i-1,j)} + x_{(i-1,j+1)} \\ \qquad - x_{(i+1,j-1)} - 2x_{(i+1,j)} - x_{(i+1,j+1)} \\ a^2_{i,j} = \alpha^2_{i,j} + \beta^2_{i,j}, \forall (i,j) \\ x_{i,j} = 0 \text{ if } i = 0 \text{ or } i = length + 1 \\ x_{i,j} = 0 \text{ if } j = 0 \text{ or } j = width + 1 \\ x_{i,j} \in [\![0, 255]\!], \forall (i,j) \end{cases}$$

3.2 Formulation as a Single Program

The attack takes as input the same parameters (P_t, T_t and I_A) and returns a modified attacker's image X whose complete transformation matches the target template. The main idea is to merge both steps described in Section 3.1. A unique constrained quadratic system is solved to find the nearest modified image whose complete transformation matches exactly the template (see Figure 2). Note that this single program avoids some problems such as having an intermediate feature vector which is not in the range of the filter function.

Assume that $I_A = (o_{i,j})_{n \times m}$ is the attacker's original image, $I' = (x'_{i,j})_{n \times m}$ the modified original image and $X = (x_{i,j})_{n \times m}$ its augmented form. Let $\mathcal{K}_1$ be all indices where the template is equal to 0 and $\mathcal{K}_2$ all other indices. Let $M = (a_{i,j})_{(n*m) \times \ell}$ be the projection matrix. Let Y_{flat} be the flattened form of the matrix Y where rows are concatenated in a single vector.

Thus, using the notations from the sections 3.1 and 3.2 we define the following problem for Sobel filter:

- Minimize: $\|X - I_A\|^2$
- Subject to the following constraints:

$$\begin{cases} Y^2 = \left[(G_1 * X)^2 + (G_2 * X)^2\right] \\ Y_{flat} M_i < 0, \forall i \in \mathcal{K}_1 \\ Y_{flat} M_j \geq 0, \forall j \in \mathcal{K}_2 \\ x_{i,j} \in [\![0, 255]\!], \forall (i,j) \end{cases}$$

Where the squaring stands for the coordinate by coordinate squaring and M_i the i-th column of M.

4 MULTIPLE COLLISIONS ATTACK

In this attack, the attacker knows the templates and passwords of the victims. Then, her goal is to use all these information to generate one image that allows her to impersonate all the victims using their own password. The attack takes as input: the target's templates $(T_t)_{i \in \mu}$, the attacker's image (I_A) and the target's passwords $(P)_{i \in \mu}$. The output is a modified attacker's image X which matches all templates for the corresponding password.

As in the single authentication attack, we define a quadratic system with more constraints and a function to minimize. Let M_i be the projection matrix for the i-th user. Assume that $(\mathcal{K}_1)_i$ is the list of all indices where $(T_t)_i$ is equal to 0 and $(\mathcal{K}_2)_i$ all other indices. The other notations are the same as in Section 3.2. The problem can be defined as:

- Minimize: $\|X - I_A\|^2$
- Under the following constraints where $(M_i)_j$ is the j-th column of M_i:

$$\begin{cases} Y^2 = \left[(G_1 * X)^2 + (G_2 * X)^2\right] \\ Y_{flat} (M_i)_j < 0, \forall i \in \mu, \forall j \in (\mathcal{K}_1)_i \\ Y_{flat} (M_i)_k \geq 0, \forall i \in \mu, \forall k \in (\mathcal{K}_2)_i \\ x_{i,j} \in [\![0, 255]\!], \forall (i,j) \end{cases}$$

As matrices M_i are fully random, the probability of them forming an indexed family of linearly dependent vectors is negligible, thus making the system solvable. Assume that $L(V_1, \ldots, V_k)$ is the event that $(V_1, \ldots, V_k)$ is an indexed family of linearly independent vectors, with n the size of vector and η the number of precision bits for our numbers. It can be shown that $P(L(V_1, \ldots, V_k)) = (\prod_{i=2}^{k} 2^{\eta(n-i+1)} -$

$1)/(\prod_{i=2}^{k} 2^{\eta(n-i+1)})$. Since this probability is near 1, the usurpation of $\lfloor n/w \rfloor$ persons with w the size of the template is a likely event.

5 EVALUATION AND CONCLUSION

We evaluate our attack (Section 3.2) through our Python implementation. Gurobi 9.1.2 is used to solve the quadratic non-convex programs, on a computer running on Debian 11, with an EPYC 7F72 dual processor (48 cores) and 256GB RAM. We have launched resolutions of the programs 50 times, each with a time limit of 150 seconds. Table 1 reports the running times for the different settings along with the amount of changes done in the attacker fingerprint, using Euclidian distance. With a 4×4-pixel image and a 50-bit template, 150 seconds starts to be insufficient to solve the system and optimize the criterion. In 500 seconds, we solve the system with a 10×10-pixel image for a better ratio amount of changes over image size. Thus, the experiments are encouraging for a NP-hard problem (Sahni, 1974).

Table 1: Summary of the experiments for a 50-bit template.

Image Size	Template Size	Mean Distance	Mean Time (s)
2×2	50	99	0.14
2×3		117	32.76
3×3		133	150.0
4×3		144	146.67
4×4		177	150.0

In this paper, we present several authentication attacks on a popular CB scheme consisting in a composition of a kernel-based filter with a projection-based transformation, in the stolen token scenario. Their particularity is to completely reverse a CB scheme to impersonate any or several users. To the best of our knowledge, this is the first time that attacks are conducted on a complete chain of treatments, including a non-linear filter. The proposed methodology is to formalize the attacks as constrained optimization problems. As long as the attacker has access to one or several templates with the corresponding passwords or not, our attacks can be performed. Future work will focus on finding optimizations and relaxations of the systems to ensure the scaling of our attacks.

ACKNOWLEDGEMENT

The authors acknowledges the support of the French Agence Nationale de la Recherche (ANR), under grant ANR-20-CE39-0005 (project PRIVABIO).

REFERENCES

(2011). ISO/IEC24745:2011: Information technology – Security techniques – Biometric information protection. Standard, International Organization for Standardization.

(2018). ISO/IEC30136:2018(E): Information technology – Performance testing of biometrictemplate protection scheme. Standard, International Organization for Standardization.

Dong, X., Jin, Z., and Jin, A. T. B. (2019). A genetic algorithm enabled similarity-based attack on cancellable biometrics. In *2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–8.

Ghammam, L., Karabina, K., Lacharme, P., and Thiry-Atighehchi, K. (2020). A cryptanalysis of two cancelable biometric schemes based on index-of-max hashing. *IEEE Transactions on Information Forensics and Security*, PP:1–12.

Jin, A. T. B., Ling, D. N. C., and Goh, A. (2004). Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition*, 37(11):2245–2255.

Lacharme, P., Cherrier, E., and Rosenberger, C. (2013). Preimage attack on biohashing. In *2013 International Conference on Security and Cryptography (SECRYPT)*, pages 1–8.

Li, C. and Hu, J. (2014). Attacks via record multiplicity on cancelable biometrics templates. *Concurrency Computation: Practice and Experience*, pages 1593–1605.

Nagar, A., Nandakumar, K., and Jain, A. K. (2010). Biometric template transformation: a security analysis. In Memon, N. D., Dittmann, J., Alattar, A. M., and Delp, E. J., editors, *Media Forensics and Security*, volume 7541 of *SPIE Proceedings*, page 75410O. SPIE.

Nandakumar, K. and Jain, A. K. (2015). Biometric template protection: Bridging the performance gap between theory and practice. *IEEE Signal Processing Magazine*, 32:88–100.

Natgunanathan, I., Mehmood, A., Xiang, Y., Beliakov, G., and Yearwood, J. (2016). Protection of privacy in biometric data. *IEEE Access*, 4:880–892.

Ratha, N. K., Connell, J. H., and Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication system. *IBM Systems J.*, 37(11):2245–2255.

Sahni, S. (1974). Computationally related problems. *SIAM Journal on Computing*, 3(4):262–279.

Teoh, A. B. J., Yip, W. K., and Lee, S. (2008). Cancellable biometrics and annotations on BioHash. *Pattern Recognition*, 41(6):2034–2044.

Topcu, B., Karabat, C., Azadmanesh, M., and Erdogan, H. (2016). Practical security and privacy attacks against biometric hashing using sparse recovery. *EURASIP Journal on Advances in Signal Processing*, 2016(1):100.

Vincent, O. and Folorunso, O. (2009). A descriptive algorithm for sobel image edge detection.