

Interpretable security analysis of cancellable biometrics using constrained-optimized similarity-based attack

Hanrui Wang, Xingbo Dong, Zhe Jin
Monash University Malaysia
47500 Subang Jaya, Selangor, Malaysia

{hanrui.wang, xingbo.dong, jin.zhe}@monash.edu

Andrew Beng Jin Teoh
Yonsei University, South Korea
50 Yonsei-ro Seodaemun-gu, Seoul, South Korea

bjteoh@yonsei.ac.kr

Massimo Tistarelli
University of Sassari, Italy
Alghero, SS 07041, Italy

tista@uniss.it

Abstract

In cancellable biometrics (CB) schemes, template security is achieved by applying, mainly non-linear, transformations to the biometric template. The transformation is designed to preserve the template distance/similarity in the transformed domain. Despite its effectiveness, the security issues attributed to similarity preservation property of CB are underestimated. Dong et al. [BTAS'19], exploited the similarity preservation trait of CB and proposed a similarity-based attack with high successful attack rate. The similarity-based attack utilizes preimage that are generated from the protected biometric template for impersonation and perform cross matching. In this paper, we propose a constrained optimization similarity-based attack (CSA), which is improved upon Dong's genetic algorithm enabled similarity-based attack (GASA). The CSA applies algorithm-specific equality or inequality relations as constraints, to optimize preimage generation. We interpret the effectiveness of CSA from the supervised learning perspective. We identify such constraints then conduct extensive experiments to demonstrate CSA against CB with LFW face dataset. The results suggest that CSA is effective to breach IoM hashing and BioHashing security, and outperforms GASA significantly. Inferring from the above results, we further remark that, other than IoM and BioHashing, CSA is critical to other CB schemes as far as the constraints can be formulated. Furthermore, we reveal the correlation of hash code size and the attack performance of CSA.

1. Introduction

In the past decade, biometric technology has been widely deployed for identity management systems due to its usability. As a consequence, the proliferation of centralized biometric databases is unavoidable, thus increasing security and privacy concerns. Cancellable biometrics (CB) is devised to protect the biometric template. CB employs a parameterized, renewable, and irreversible but similarity preserving transformation to convert a biometric template into a protected instance. Due to the property of similarity preservation, templates comparison can be done in the transformed domain while prohibiting the comparison of templates between original and its transformed version [1]. Since CB was introduced, a large number of methods have been reported. Some representative instances are BioHashing [2], bloom filter [3], and Index-of-Max (IoM) hashing [4]. Ideally, the following four requirements should be satisfied by any CB scheme:

- *Non-invertibility or Irreversibility*: It should be computationally hard to retrieve original biometric features from a single or multiple compromised templates, even under the case where the transformation parameters e.g. token are known. Hence, compromise of protected templates will not lead to the privacy invasion.
- *Revocability or Renewability*: It should be feasible to re-issue a new protected template when the old one is compromised. Other protected templates should remain unchanged when the replacement is carried out.
- *Non-linkability or Unlinkability*: It is impossible to perform cross matching among multiple protected templates across various applications. When one

or multiple protected biometric templates have been stolen, the templates that derived from the same identity that stored in other databases should not be traced.

- *Performance preservation*: The accuracy performance should not be degraded significantly after transformation. To meet this criterion, the CB scheme has to satisfy the similarity preservation property where the pair-wise distance of templates before and after transformation should be largely preserved.

Despite CB has been proved useful, it is vulnerable to various attacks. Firstly, CB could be attacked by attack via record multiplicity (ARM) (also known correlation attack) [5], which leads to the violation of the unlinkability criteria. The ARM refers to the case when multiple protected templates are stolen, then attackers may correlate those templates that are generated from the same user for cross matching and/or for template generation. Secondly, CB could be harmed by dictionary based attack [6] and brute force [7] attack, which result in violating the irreversibility criteria. Our focus in this paper is similarity attack (SA) or also known as pre-image attack [8]. Similarity attack exploits the similarity preserving property of CB to generate a pre-image from the protected template for impersonation as well as cross-match with the templates in various applications. The preimage is an instance despite not close to the original biometric template, after the transformation, it is highly alike to the targeted protected template. Therefore, SA is harmful to unlinkability.

SA attack has been explored earlier in the literature. Most of the work focus on SA against BioHashing assuming its parameter (secret token) is known [1]. Despite a few proposals such as simple data dimension reduction and permutation, attempted to rectify this issue [9], vulnerability to SA remains critical [8, 10]. Most of the existing SA schemes, such as Genetic algorithm enabled similarity-based attack (GASA) solely exploit similarity preserving property of CB to launch the attack [10, 11]. However, for some CB schemes, besides distance similarity, some other information can be learned from the protected templates. For instance, in IoM hashing, a set of inequalities can be established from each individual hash code [4, 12]. We prove in section 4.3 that when these inequalities are utilized as constraints to compute a preimage, the discrepancy between the two protected templates that transformed from the preimage and from the original biometric template can be eliminated.

In this paper, we propose an attack method called constrained-optimized similarity-based attack (CSA). CSA is built upon the GASA [10] with augmented algorithm-specific equality or inequality relations as constraints. We explain the attempt to seek a preimage generation problem as a form of supervised learning problem (section 3.2)

where the constraints are leveraged to guarantee a minimal loss value (eq. 8 in section 3.2), e.g. minimize to zero for IoM hashing. Therefore, an optimal preimage can be generated. With better preimage quality, the successful attack rate can be elevated remarkably. Since preimage generation is based on the supervised learning approach, overfitting is inevitable. We demonstrate that by enlarging the hash code size, the overfitting problem can be alleviated. With large hash code size, the effectiveness of CSA over GASA is observed. We conduct the experiments to assess the security of IoM hashing under LFW dataset via CSA. Likewise, we conduct extensive evaluation on BioHashing to prove the CSA is generalised for other CB. We share our code at <https://github.com/azrealwang/csa>.

The main contributions of this paper are:

- We propose a constrained optimization based similarity attack abbreviated as CSA. The CSA can be effective to any CB schemes where equality or inequality relations can be formulated.
- We interpret preimage generation problem from the supervised learning perspective, which justifies why CSA outperforms GASA significantly.
- We conduct extensive experiments to demonstrate CSA against IoM hashing and BioHashing with LFW face dataset. We reveal the hash code size is one of the key factors to impact attack performance. We also discuss the implication of CSA on security, parameters setting and efficiency with respect to the attack performance.

2. Related work

2.1. Similarity-based attack (SA)

There are several SA schemes proposed in the literature. Dong et al. [10] and Lacharme et al. [11] propose a SA scheme using genetic algorithm (GA). The GA-enabled SA generates preimage with an iterative procedure of selection, mutation and crossover. The experimental results attest that GA-enabled SA is effective to breach Biohashing based cancellable face and fingerprint templates.

Feng et al. [13] propose a SA scheme based on neural networks. Feng et al. claim that there are several limitations in many SA schemes such that: 1) They rely on less-realistic assumptions, 2) They rely on knowledge of e.g. transformation algorithm and its parameters. Hence, Feng et al. consider two distinct scenarios depending on the availability of transformation algorithm knowledge. With that knowledge, the attack can be launched for preimage generation. If transformation algorithm knowledge is not available, the attack also can be launched by using a multilayer perceptron network and a customized hill climbing [14, 15].

Kaplan et al. [16] propose a SA scheme by utilizing the relation of multiple compromised transformed templates from the same individual. The scheme exploits distance preserving trait of the transformation algorithm. However, Kaplan’s scheme does not apply to the systems that only store one single protected template of each user .

Ghammam et al. [17] propose a constrained optimization SA against IoM hashing. The method applies inequalities as constraints to seek preimage solution.

2.2. IoM hashing

The IoM hashing is a ranking-based locality sensitive hashing method designed for biometric template protection. The IoM hashing transforms a biometric template into a set of top ranked discrete indices of random subspace projection as hash code [4]. Firstly, biometric feature $\mathbf{x} \in \mathbb{R}^N$ is extracted from the biometric data. A set of random matrices $\mathbf{R}_l \in \mathbb{R}^{K \times N}, l = 1, \dots, L$, where L is the hash code size and K is the subspace dimension, are drawn from a standard Gaussian distribution $\mathcal{N}(0, 1)$. Hence, each random projected vector $\mathbf{z}_l \in \mathbb{R}^K$ can be computed as:

$$\mathbf{z}_l = \mathbf{R}_l \mathbf{x}. \quad (1)$$

For each \mathbf{z}_l , the hash code $h_l \in [1, K]$ can be obtained from the first ranked index of vector \mathbf{z}_l . The IoM hash vector is then formed as $\mathbf{h} = \{h_l | l = 1, \dots, L\}$. At verification stage, the hamming distance is calculated between $\mathbf{h}(\mathbf{x})$ and $\mathbf{h}(\mathbf{y})$ [18] and decision can be made by comparing the hamming score with respect to a pre-determined threshold value.

2.3. BioHashing

BioHashing relies on biometric feature $\mathbf{x} \in \mathbb{R}^N$ extracted from the biometric data and a user-specific tokenized random vector $\mathbf{b}_l \in \mathbb{R}^N, l = 1, \dots, L (L \leq N)$, where L is hash code size [2]. A binary discretization is applied to compute a BioHash code h_l as

$$h_l = \text{Sig}(\mathbf{x}^T \mathbf{b}_l - \tau), \quad (2)$$

where $\text{Sig}(\cdot)$ is defined as a signum function and τ is an empirically determined threshold.

3. Constrained-optimized similarity-based attack (CSA)

In this section, the proposed CSA is presented. We begin with a background introduction of similarity-based attack in section 3.1. Then, we address the loss function that we use to optimize the preimage search in section 3.2. Then we reveal the preimage generation with the proposed constrained optimization technique can be analyzed from the supervised learning perspective in section 3.3. Thereafter, as a toy example, IoM hashing is used to evaluate the CSA, particularly, the inequality constraints of IoM hashing is presented

in section 3.4. Note that in section 3 BioHashing algorithm will not be discussed but it will be assessed in experiments to prove the generalization (section 4.3). At last, a preimage generation algorithm, namely Augmented Lagrangian Genetic Algorithm (ALGA) is given in section 3.5.

3.1. Similarity-based attack (SA) framework

A given CB transformation function $f(\cdot)$ could be defined as

$$\mathbf{y} = f(\mathbf{x}). \quad (3)$$

where \mathbf{x} represents the biometric template and \mathbf{y} represents protected template.

Ultimately, the aim of SA is to generate a preimage $\hat{\mathbf{x}}$ [19] of \mathbf{y} . Thus, SA is intuitively an optimization task to search optimal $\hat{\mathbf{x}}$:

$$\arg \min_{\hat{\mathbf{x}}} \|\mathbf{x} - \hat{\mathbf{x}}\|. \quad (4)$$

In a CB system, \mathbf{x} is discarded after transformation, however, the transformed templates \mathbf{y} are stored. In order to preserve accuracy, the relative distances between \mathbf{y} and $\hat{\mathbf{y}} = f(\hat{\mathbf{x}})$ are to be preserved. Thus, eq. 4 can be reformulated to

$$\arg \min_{\hat{\mathbf{x}}} D(\mathbf{y}, \hat{\mathbf{y}}), \quad (5)$$

where $D(\cdot)$ is an algorithm-specific distance function.

3.2. Loss function

The preimage generation that required by CSA can be perceived as a supervised learning problem, where the goal is to learn optimal preimage by utilizing labeled data as a supervising signal. Note that in CSA context, learning/training refers to the preimage generation but not to model training under conventional supervised learning setting. In supervised learning, a training data set \mathbf{X}, \mathbf{Y} is to be availed where \mathbf{X} is input data and \mathbf{Y} is the label of \mathbf{X} . In our context, $f(\mathbf{X})$ in eq. (2) can be seen as a predicted label. Based on eq. 3 and eq. 5, the loss function of CSA preimage generation $\mathcal{L}(\cdot)$ is defined as

$$\mathcal{L} = D(\mathbf{Y}, f(\mathbf{X})). \quad (6)$$

where $D(\cdot)$ is an algorithm-specific distance function.

Specifically for IoM hashing as an example, biometric template \mathbf{x} is *unknown* as it is discarded after transformation, while user-specific matrix $\mathbf{R}^* = \{\mathbf{R}_l^*\}_{l=1}^L$ and the protected template $\mathbf{h} = \{h_l\}_{l=1}^L$ are *available* as they are stored in the database. Recall h_l is the index value of maximum entry of $\mathbf{R}_l^* \mathbf{x}$ (IoM hash code) and L is the hash code size of IoM hashing. The optimal preimage $\hat{\mathbf{x}}$ is the target of searching. Furthermore, for each $\mathbf{R}_l^* \mathbf{x}$, there is a corresponding "label", i.e. h_l from supervised learning perspective. As \mathbf{R}_l^* is *known* and \mathbf{x} is *unknown*, the \mathbf{X}, \mathbf{Y} in eq. 6

can be defined as

$$\begin{aligned} \mathbf{X} = \mathbf{R}^* &= \{\mathbf{R}_l^*\}_{l=1}^L; \\ \mathbf{Y} = \mathbf{h} &= \{h_l\}_{l=1}^L. \end{aligned} \quad (7)$$

Therefore, there are L pairs of $\{(\mathbf{R}_l^*, h_l)\}_{l=1}^L$ can be formed.

Finally, the loss function in eq. 6 can be reformulated as:

$$\mathcal{L}(\hat{\mathbf{x}}) = D(\mathbf{h}, f(\mathbf{R}^*)), \quad (8)$$

3.3. Constrained optimization

In this subsection, the reasons behind the higher attack success rate of the CSA model are discussed and explained. Moreover, the correlation between the hash code size and the security of CB, already addressed in [10], is further analyzed under the perspective of supervised learning. As it will be demonstrated, a larger hash code size leads to lower security.

Let $\mathbf{h} = f(\mathbf{x}; \mathbf{R}^*)$ and $\hat{\mathbf{h}} = f(\hat{\mathbf{x}}; \mathbf{R}^*)$ be the IoM hash vector that generated from biometric template \mathbf{x} and its counterpart that generated from pre-image $\hat{\mathbf{x}}$ during "training" stage. Then suppose $\mathbf{h}' = f(\mathbf{x}; \mathbf{R}^{*'})$ and $\hat{\mathbf{h}}' = f(\hat{\mathbf{x}}; \mathbf{R}^{*'})$ are the IoM hash vectors for verification where $\mathbf{R}^{*'}$ is a new user-specific random matrix for \mathbf{h}' and $\hat{\mathbf{h}}'$ ($\mathbf{R}^{*' \neq \mathbf{R}^*$). For the sake of clarity, we define several terms:

- Definition 1: *Test error (TEE)*, or prediction error, refers to the deviation of true \mathbf{h}' and predicted $\hat{\mathbf{h}}'$ from testing data. It is used to estimate the attack performance of unseen data. As they are integer vectors, TEE can be computed with

$$TEE = \frac{1}{n} \sum_{i=1}^n [D(\mathbf{h}'_i, \hat{\mathbf{h}}'_i)]^2. \quad (9)$$

where $D(\cdot)$ here is the hamming distance and n is the repetitive verification times. In our experiment, we set $n = 10$ (section 4.2). \mathbf{h}'_i and $\hat{\mathbf{h}}'_i$ are generated by different $\mathbf{R}^{*'}$ for each verification.

- Definition 2: *Training error (TRE)* refers to the deviation of true \mathbf{h} and predicted $\hat{\mathbf{h}}$ [20]. Similarly, TRE can be computed with:

$$TRE = [D(\mathbf{h}, \hat{\mathbf{h}})]^2. \quad (10)$$

- Definition 3: *Variance (VAR)* indicates the mean square difference of $\hat{\mathbf{h}}$ and the expected value of $\hat{\mathbf{h}}$ [20]. Under supervised learning setting, VAR can be regarded as a measure of system overfitting. The larger VAR, the more system prone to overfitting. However, since these two values are computed with distinct user-specific matrices, so they are incomparable. Thus, VAR is approximately defined as

$$VAR \approx \frac{1}{n} \sum_{i=1}^n [D(\mathbf{h}'_i, \hat{\mathbf{h}}'_i) - D(\mathbf{h}, \hat{\mathbf{h}})]^2. \quad (11)$$

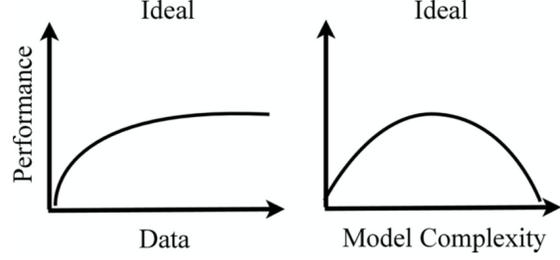


Figure 1. Performance related to dataset size and model complexity under ideal conditions [21].

To gain a decent attack performance (indicated by TEE), both small TRE and VAR are expected [20].

In general, overfitting is determined by the two factors, namely training data size and model complexity. As shown in Fig. 1, in an ideal setting, the test accuracy increases with respect to data size due to good generalization (no overfitting) whereas the test accuracy will deteriorate when the model complexity is overly high due to overfitting. In CSA context, the model complexity is fixed as CSA model does not have learnable parameters. The overfitting issue of the CSA relies solely on IoM hash code size, L , which is equivalent to training data size. Thus, the solution to alleviate the overfitting in the CSA is just to increase the L .

Based on eq. 10, TRE is smaller when \mathbf{h} and $\hat{\mathbf{h}}$ are closer. Ideally, $TRE = 0$ when $\hat{\mathbf{h}} = \mathbf{h}$. The constrained optimization model that we designed for CSA is based on the algorithm-specific inequality or equality relations. The constraints are established to force $\hat{\mathbf{h}}$ be closer to or be (ideally) identical to \mathbf{h} . The details of the algorithm-specific constraints designed for IoM hashing are presented in section 3.4.

3.4. Inequality constraints of IoM hashing

The constraints are established to minimize eq. 8, ideally $\mathcal{L}(\cdot) = 0$. Equation 8 can still converge without the constraints but it would not be optimal.

In IoM hashing, each hash code is derived from the first ranked index after projecting the biometric template onto a random subspace [4]. This facilitates the construction of the inequality relations, which can be exploited as the constraints for CSA. If the constraints are satisfied, the TRE is equal to zero as $\hat{\mathbf{h}} = \mathbf{h}$.

Let $\hat{\mathbf{z}} = [\hat{z}_1, \hat{z}_2, \dots, \hat{z}_K] = \mathbf{R}^* \hat{\mathbf{x}}$ be the random projected vector of preimage and \hat{h} be the first ranked index value of $\hat{\mathbf{z}}$. In the event of CSA, user-specific matrix \mathbf{R}^* and h are compromised. The attacker could leverage the clue $\hat{h} = h$ to minimize the hamming distance. Based on the knowledge of \mathbf{R}^* and h , the inequality relations could be established

as

$$\hat{z}_h \geq \forall \hat{z}_k \in \hat{\mathbf{z}}, k = 1, \dots, K. \quad (12)$$

A constraint function $c(\cdot)$ can be defined based on eq. 12 as

$$c(\hat{\mathbf{x}}) = \{\hat{z}_k - \hat{z}_h | k = 1, \dots, K\}, \text{ where } \hat{z}_k \in \hat{\mathbf{z}} = \mathbf{R}^* \hat{\mathbf{x}}. \quad (13)$$

Thus, the inequality constraint is $c(\hat{\mathbf{x}}) \leq 0$. If the constraint is unsatisfied, we name it as a violation. To quantify the violation, a constraint violation function $v(\cdot)$ is devised as follow:

$$v = \max c(\hat{\mathbf{x}}). \quad (14)$$

In general, the constraint is satisfied if $v(\cdot) \leq \tau$, where $\tau \approx 0$, or $\tau = 0$ ideally. When $v(\cdot) \leq 0$ is satisfied (our case), $\mathcal{L}(\hat{\mathbf{x}}) = 0$.

3.5. Augmented Lagrangian Genetic Algorithm

The original SA is an unconstrained optimization problem based on eq. 8 to approximate $\hat{\mathbf{x}}$, which is kind of ad-hoc. GA is employed in GASA as a searching algorithm [12]. In the traditional GA, the output is produced with a repeated procedure of selection, mutation and crossover until convergence (i.e. meeting stopping criteria). However, traditional GA is limited to solve unconstrained optimization problems [22]. In this paper, we adopt ALGA [23] as a means of searching algorithm to solve $\hat{\mathbf{x}}$ based on the constraints formulated in eq. 8 and eq. 13. ALGA is an iterative 4-steps procedure (one generation) as follows:

- *Step 1:* Combine the loss function $\mathcal{L}(\cdot)$ (eq. 8) and constraint function $c(\cdot)$ (eq. 13) in terms of Lagrangian barrier function $LB(\cdot)$. The goal is to transform a constrained to unconstrained problem, which is applicable to GA. For the definition of Lagrangian barrier function and detailed combination algorithm please refer to [23].
- *Step 2:* Minimize $LB(\cdot)$ with GA.
- *Step 3:* The optimization process will be terminated when $|\mathcal{L}_{n-1}(\cdot) - \mathcal{L}_n(\cdot)| \leq \tau_1$ and $v(\cdot) \leq \tau_2$ where n is the generation number, τ_1 and τ_2 are the selected tolerance where $\tau_* \approx 0$, or $\tau_* = 0$, $*$ =1, 2 ideally.
- *Step 4:* Go to *Step 1* and recreate $LB(\cdot)$ referring to [23], if stopping criteria is not satisfied. It indicates that the inequality constraint must be satisfied when ALGA converges, while the constraint might not be satisfied at every generation.

A complete ALGA algorithm description can be found at algorithm 1 [23].

Other than ALGA, there are more optimization methods where the constraints can be applied. In this work, we are more interested in the constrained optimization than the searching algorithm, so ALGA is only the choice of implementation.

Algorithm 1: Augmented Lagrangian Genetic Algorithm

Input : Compromised template \mathbf{h} and user-specific \mathbf{R}^* , loss function $\mathcal{L}(\cdot)$, constraint function $c(\cdot)$, constraint violation function $v(\cdot)$, stopping criteria τ_1, τ_2

Output: Preimage $\hat{\mathbf{x}}$

- 1 Initialization: Initial $\hat{\mathbf{x}}$ with random standard Gaussian vector
 - 2 **repeat**
 - 3 Complete Lagrangian barrier function $LB(\cdot)$ by combining $\mathcal{L}(\cdot)$ and $c(\cdot)$ refer to [23]
 - 4 Minimize $LB(\cdot)$ with GA
 - 5 Estimate if stopping criteria is met
 - 6 **until** $|\mathcal{L}_{n-1}(\cdot) - \mathcal{L}_n(\cdot)| \leq \tau_1$ and $v(\cdot) \leq \tau_2$
-

4. Experiments

4.1. Dataset

LFW dataset [24] is used to evaluate the CSA on IoM hashing. There are 5749 users in the entire LFW dataset. The subjects with more than 10 images are chosen and the first 10 images of each subject are selected for our experiments. The subset of LFW dataset consists of 1580 images which contains 158 users and 10 images for each user. The face feature is extracted into a 512-dimensional vector by a deep learning model, InsightFace [25].

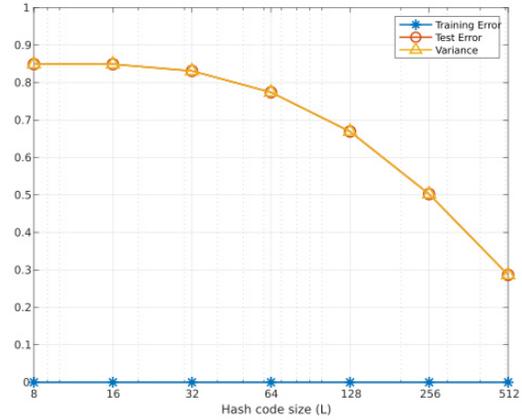
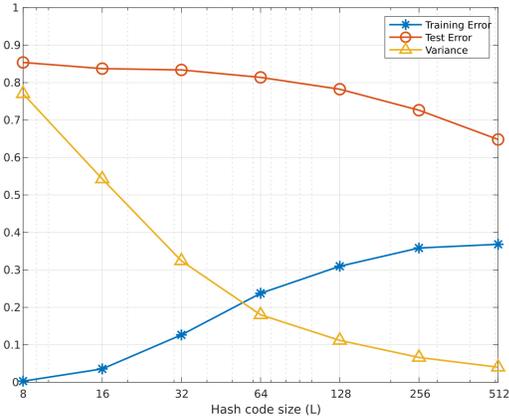
4.2. Experiment protocol

In our experiments, we assume only one protected template is stored in the database for each subject, and this template is transformed from the first sample of each subject in the dataset. The remaining nine samples of each subject are used for verification. This protocol is to evaluate whether the generated preimage is effective to breach the system after the user re-issues a protected template using new face image. Furthermore, we adopt distinctive \mathbf{R}^* in our experiments for preimage generation and verification. This aims to simulate re-issue of protected template scenario and evaluate the possibility of preimage to breach multiple systems. The hash code size L , which varies from 8 to 512 for IoM hashing is examined and the preimage generation process under each scenario of selected L is executed only once due to computational cost.

For attack performance assessment, we propose two new metrics, namely successful attack rate (SAR) and false acceptance increment (FAI). SAR are recorded using acceptance rate of preimage $\hat{\mathbf{x}}$. By excluding false match rate (FMR), $FAI = SAR - FMR$, indicates true attack performance. A higher FAI implies a more effective attack performance. In addition, equal error rate (EER) is computed to evalu-

Table 1. CSA performance with subspace dimension $K = 16$.

Hash code size (L)	IoM			GASA			Proposed CSA		
	θ^2	EER(%)	FMR(%)	SAR(%)	FAI(%)	TEE	SAR(%)	FAI(%)	TEE
8	0.7639	14.40	9.78	10.94	1.16	0.8537	11.06	1.28	0.8491
16	0.7639	8.59	9.44	12.41	2.97	0.8373	11.14	1.70	0.8491
32	0.7101	3.87	2.69	3.96	1.27	0.8338	4.83	2.14	0.8311
64	0.7351	2.00	2.24	5.40	3.16	0.8139	12.03	9.79	0.7740
128	0.7379	1.10	1.10	7.54	6.44	0.7823	42.13	41.03	0.6693
256	0.7455	0.72	0.71	24.11	23.39	0.7263	92.08	91.36	0.5023
512	0.7525	0.60	0.61	64.12	63.51	0.6482	99.19	98.58	0.2866



(a) GASA (b) CSA
Figure 2. Error of GASA and CSA with different hash code size L .

Table 2. CSA efficiency with subspace dimension $K = 16$.

Hash code size (L)	GASA		Proposed CSA	
	Generations	Time (s)	Generations	Time (s)
16	68	11.88	5	142.95
32	87	15.78	5	182.00
64	109	26.13	5	201.87
128	111	34.10	5	364.96
512	94	97.84	5	3661.63

ate the performance of IoM hashing with respect to L . All performance assessments are repeatedly executed ten times with different \mathbf{R}^* .

For efficiency evaluation, the number of generations and computation cost in second are recorded when preimage generation of one sample reaches convergence. The machine we used for simulation is equipped with MATLAB Ver. 2019b, 2.7 GHz Dual-Core Intel Core i5 CPU and 1867

MHz 8GB RAM.

4.3. Experiment results

We first investigate the effect of L with respect to the attack performance of CSA. For each L , threshold θ (for the convenience of comparison, it is recorded as θ^2), EER and FMR of IoM hashing, SAR, FAI and TEE of GASA and the proposed CSA are reported in Table 1. The results show that when $L \leq 32$, TEE of CSA is more than 0.83 and it is considerably higher than θ^2 (0.83 vs 0.71). This implies CSA is not so effective against IoM hashing when hash code size is small. However, this is not practical because small hash code size is vulnerable to other security attacks such as brute force attack. On the other hand, when $L > 64$, TEE of CSA is perceptibly reduced and FAI raises dramatically. When $L = 512$, SAR of CSA achieved up to 99.19% and FAI of CSA achieved 98.58%. To benchmark GASA, the attack performance of CSA is close to GASA when L is small (e.g. $L \leq 32$). However, when L increases, TEE of CSA reduces much faster than TEE of GASA. Along with

Table 3. CSA performance against Biohashing.

Hash code size (L)	Biohashing		GASA		Proposed CSA	
	EER(%)	FMR(%)	SAR(%)	FAI(%)	SAR(%)	FAI(%)
512	0.63	0.63	34.43	33.80	72.74	72.11

SAR and FAI, we can observe that CSA largely outperforms GASA in terms of SAR (CSA: 99.19% vs GASA: 64.12%) and FAI (CSA: 98.58% vs GASA: 63.51%).

The experiment results obtained above are indeed consistent with the analysis in section 3. Figure 2 illustrates the error trend of GASA and CSA. Specifically, when L is small, it results high VAR due to overfitting (yellow curve) (section 3.3). Despite TRE (blue curve) of both GASA and CSA are low under this case, TEE (red curve) is still high. This leads to poor attack performance. On the other hand, when L increases, VAR for both GASA and CSA is reduced. The TRE of CSA remains at zero attributed to the inequality constraints, yet TRE of GASA increases due to the increment of L . When L is large enough (e.g. $L = 512$), the attack performance is mainly affected by TRE. With additional constraints, TRE in CSA can be zero while this is not the case for GASA. Therefore, we can point out that CSA outperforms GASA when L is large enough.

To evaluate the efficiency of CSA, the number of generations and time for convergence in second for one preimage generation are recorded in Table 2. The results show that the number of generations to convergence for CSA is significantly lesser than that of GASA while the preimage computational cost of CSA is comparably higher. This is due to natural distinction of the traditional GA and ALGA, where one generation produced by ALGA refers to a solution of each Lagrangian barrier function, and this process likely consists of multiple generations produced by the traditional GA. The number of generations for ALGA is hence less. Referring to section 3.5, ALGA consists of multiple operations, e.g. Lagrangian barrier function $LB(\cdot)$ and GA computation. The total operations of ALGA is much more than just one single GA, hence more computational cost is somehow expected. This demonstrates a phenomenon where high preimage computational cost trades with a good attack performance in CSA. Nevertheless, even approximately one hour (3661.63 seconds) for a successful attack is feasible and worthwhile indeed.

We also conduct CSA on Biohashing by using LFW face dataset. Table 3 reveals that CSA can largely outperform GASA on Biohashing as well in terms of SAR (CSA: 72.74% vs GASA: 34.43%) and FAI (CSA: 72.11% vs GASA: 33.80%). Therefore, CSA can applied to CB which could apply equalities or inequalities as constraints. As limited by the paper length, we will not address more details about Biohashing.

5. Conclusion

In this paper, we propose a novel similarity-based attack on IoM hashing known as CSA. The experiments conducted under LFW face dataset show that CSA is effective in terms of SAR and FAI against IoM hashing and BioHashing. The CSA demonstrates a superior attack performance (SAR and FAI) over GASA due to the employment of constrained optimization. We further analyze that the constraints in CSA can significantly reduce TRE whereas it is impossible for GASA. The theoretical justification on CSA attack performance is consistent with the empirical observations. We further reveal that 1) the attack performance of the CSA is closely related to the IoM hash code size; 2) the CSA trades the preimage computational cost with superior attack performance, nonetheless, the average computational cost for $L = 512$ is approximately one hour, which is acceptable and worthwhile.

However, the CSA model suffers from three limitations. Firstly, the CSA relies on information leakage restrictively. This means it requests the knowledge of the protected template, transformation algorithm and its associated parameters (eq. 8). Secondly, unlike GASA which requires no constraints, CSA expects constraints to be established, which could be difficult for some cancellable biometric schemes such as Bloom filter. However, CSA might outperform GASA if those constraints can be identified. Finally, the generated preimage (i.e. the feature vector) is not available to reconstruct the face image.

In future developments of this research, the generalization of the CSA model against other CB schemes will be addressed. Moreover, countermeasures to enhance the security of CB against attacks including similarity-based attacks, such as adopting non-linear transformation, or integrating permutations before applying the transformation, will be investigated.

Acknowledgment

This work has been partially supported by the European Union COST Action CA16101, University of Sassari fondo di Ateneo per la ricerca 2020, Italian Ministry for Research special research project SPADA, Fundamental Research Grant Scheme (FRGS/1/2018/ICT02/MUSM/03/3) and NVIDIA Corporation donation of the Titan Xp GPU.

References

- [1] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 54–65, 2015.
- [2] A. B. Teoh, A. Goh, and D. C. Ngo, "Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 1892–1901, 2006.
- [3] C. Rathgeb, F. Breiting, and C. Busch, "Alignment-free cancelable iris biometric templates based on adaptive bloom filters," in *2013 international conference on biometrics (ICB)*, pp. 1–8, IEEE, 2013.
- [4] Z. Jin, J. Y. Hwang, Y.-L. Lai, S. Kim, and A. B. J. Teoh, "Ranking-based locality sensitive hashing-enabled cancelable biometrics: Index-of-max hashing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 393–407, 2017.
- [5] H. Kaur and P. Khanna, "Random distance method for generating unimodal and multimodal cancelable biometric features," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 3, pp. 709–719, 2018.
- [6] S.-C. Wu, P.-T. Chen, A. L. Swindlehurst, and P.-L. Hung, "Cancelable biometric recognition with ecgs: subspace-based approaches," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1323–1336, 2018.
- [7] R. M. Bolle, J. H. Connell, and N. K. Ratha, "Biometric perils and patches," *Pattern recognition*, vol. 35, no. 12, pp. 2727–2738, 2002.
- [8] Y. Lee, Y. Chung, and K. Moon, "Inverse operation and preimage attack on biohashing," in *2009 IEEE Workshop on Computational Intelligence in Biometrics: Theory, Algorithms, and Applications*, pp. 92–97, IEEE, 2009.
- [9] A. Lumini and L. Nanni, "An improved biohashing for human authentication," *Pattern recognition*, vol. 40, no. 3, pp. 1057–1065, 2007.
- [10] X. Dong, Z. Jin, and A. T. B. Jin, "A genetic algorithm enabled similarity-based attack on cancellable biometrics," in *IEEE 10th International Conference on Biometrics: Theory, Applications, and Systems (BTAS2019)*, 2019.
- [11] P. Lacharme, E. Cherrier, and C. Rosenberger, "Preimage attack on biohashing," in *2013 International Conference on Security and Cryptography (SECRYPT)*, pp. 1–8, IEEE, 2013.
- [12] X.-B. Dong, Z. Jin, and K. Wong, "A generalized approach for cancellable template and its realization for minutia cylinder-code," in *2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, pp. 908–915, IEEE, 2018.
- [13] Y. C. Feng, M.-H. Lim, and P. C. Yuen, "Masquerade attack on transform-based binary-template protection based on perceptron learning," *Pattern Recognition*, vol. 47, no. 9, pp. 3019–3033, 2014.
- [14] M. Gomez-Barrero, J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Face verification put to test: A hill-climbing attack based on the uphill-simplex algorithm," in *2012 5th IAPR International Conference on Biometrics (ICB)*, pp. 40–45, IEEE, 2012.
- [15] A. Adler, "Sample images can be independently restored from face recognition templates," in *CCECE 2003-Canadian Conference on Electrical and Computer Engineering. Toward a Caring and Humane Technology (Cat. No. 03CH37436)*, vol. 2, pp. 1163–1166, IEEE, 2003.
- [16] E. Kaplan, M. E. Gursay, M. E. Nergiz, and Y. Saygin, "Known sample attacks on relation preserving data transformations," *IEEE Transactions on Dependable and Secure Computing*, 2017.
- [17] L. Ghammam, K. Karabina, P. Lacharme, and K. Atighehchi, "A cryptanalysis of two cancelable biometric schemes based on index-of-max hashing," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2869–2880, 2020.
- [18] X. Dong, S. Kim, Z. Jin, J. Y. Hwang, S. Cho, and A. B. J. Teoh, "Open-set face identification with index-of-max hashing by learning," *Pattern Recognition*, vol. 103, p. 107277, 2020.
- [19] Y. Chen, Y. Wo, R. Xie, C. Wu, and G. Han, "Deep secure quantization: On secure biometric hashing against similarity-based attacks," *Signal Processing*, vol. 154, pp. 314–323, 2019.
- [20] E. Alpaydin, *Introduction to machine learning*, ch. 4, pp. 81–82. MIT press, 3 ed., 2014.
- [21] X. Zhu, C. Vondrick, C. C. Fowlkes, and D. Ramanan, "Do we need more training data?," *International Journal of Computer Vision*, vol. 119, no. 1, pp. 76–92, 2016.
- [22] H. Adeli and N.-T. Cheng, "Augmented lagrangian genetic algorithm for structural optimization," *Journal of Aerospace Engineering*, vol. 7, no. 1, pp. 104–118, 1994.
- [23] A. Conn, N. Gould, and P. Toint, "A globally convergent lagrangian barrier algorithm for optimization with general inequality constraints and simple bounds," *Mathematics of Computation*, vol. 66, no. 217, pp. 261–288, 1997.
- [24] G. B. Huang, M. Mattar, T. Berg, and E. Learned-Miller, "Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments," in *Workshop on Faces in 'Real-Life' Images: Detection, Alignment, and Recognition*, (Marseille, France), Erik Learned-Miller and Andras Ferencz and Frédéric Jurie, Oct. 2008.
- [25] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "Arcface: Additive angular margin loss for deep face recognition," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 4690–4699, 2019.