A Framework for Biometric Visual Cryptography

Koray Karabina*
Florida Atlantic University
777 Glades Road, Boca Raton, FL, 33431, US
kkarabina@fau.edu
Angela Robinson
Florida Atlantic University
arobin65@my.fau.edu
July 5, 2017

Abstract

Visual cryptography is an increasingly popular cryptographic technique which allows for secret sharing and encryption of sensitive data. This method has been extended and applied to secure biometric data in various protocols. Recently, Karabina and Robinson proposed a general framework to help assess the security of these extended biometric visual cryptographic schemes (e-BVC), and formalized the notion of perfect resistance against false authentication [16]. In this paper, we extend the framework in [16] with respect to indistinguishability and index privacy notions. Based on our definitions, we present theoretical analysis of e-BVC schemes and propose new attack strategies. We show that our framework can be applied to derive new and quantifiable upper bounds on the security of e-BVC schemes. We also discuss the practical impact of our attacks in detail and present several case analyses for a recent implementation of a face recognition protocol by Ross and Othman [25]. In particular, we conclude that the scheme in [25] is not secure with respect to our definitions. We show that sheet indistinguishability and index privacy notions are violated in [25], and that adversarial success probability (in authenticating to a server) can be increased from 0.005 to 0.45 by deploying one of our new attack strategies.

1 Introduction

Biometric authentication systems are employed worldwide, in both public and private sectors. For example, facial and fingerprint recognition systems are valuable border control tools, and are currently deployed by the United States via the
Global Entry program \(^1\) as well as at automated border patrols in the Frankfurt Rhein-Main international airport \(^2\). Biometric authentication systems are convenient for users, requiring no generation and memorization of passwords. However, there is a greater risk in the event that the database storing biometric information is compromised or hacked. One may always create a new password, but one cannot easily create a new face or fingerprint. Thus confidentiality and privacy of biometric data is of supreme importance. The sensitive nature of enrolled biometric information requires heightened security and privacy measures of cryptographic protocols in biometrics. There are several techniques to design secure biometric schemes. Some examples are biometric cryptosystems \([15]\), cancelable biometrics \([23]\), secure multiparty computation, encryption, private information retrieval \([9, 5, 30, 6, 8]\), and hybrid biometrics \([10, 14]\).

Biometric visual cryptography (BVC) \([17, 25]\) is another approach to design secure and privacy-preserving biometric systems. Visual cryptography (VC) allows for concealment of a secret image such that the recovery procedure does not require any computation. The main ingredient of a classical visual cryptographic construction is a \((t, n)\)-threshold secret sharing scheme \([26, 7]\), where a secret is divided into \(n\) shares and the secret can be recovered if \(t\) or more shares are available. Otherwise, a collection of less than \(t\) shares is not supposed to reveal any information about the secret. For example, when \(t = n = 2\), a secret image is divided into two secret shares such that none of the shares reveal any information about the original image. The original image can be reconstructed only when both shares are combined together. Therefore, VC enjoys the fact that sensitive information can securely be distributed over several databases rather than storing it in a central database. Naor and Shamir \([19]\) are credited with the first visual cryptographic scheme using a \((t, n)\)-threshold secret sharing scheme. In the case \(t = 2\), reconstruction of an image in \([19]\) is achieved by overlaying any of the 2 out of \(n\) secret shares, where the shares are in the form of transparencies. Semantic security is achieved in \([19]\) because secret transparencies are indistinguishable from random transparencies, whence they do not reveal any information about the original image. \([4]\) extends the work in \([19]\) and establishes a framework for visual cryptography for general access structures while preserving semantic security. In \([19]\), the authors discuss how to extend their scheme (from VC to Extended VC (e-VC)) so that the shares of a secret image looks like meaningful images rather than random transparencies. This approach is further extended \([3, 17]\) to work with natural images and to improve the quality of output images. The extension of VC to e-VC in biometrics is motivated in \([25]\) as follows:

\(^1\)http://www.cbp.gov/travel/trusted-traveler-programs/global-entry

\(^2\)http://www.easypass.de/EasyPass/EN/Service/FAQ/captured-data.html
Since these sheets (shared secrets) appear as a random set of pixels, they may pique the curiosity of an interceptor by suggesting the existence of a secret image. To mitigate this concern, the sheets could be reformulated as natural images as stated by Naor and Shamir.

It is noted in [17] that there is a trade-off between the image quality and the security, and that their e-VC scheme is not perfectly secure. It is also noted that security assessments should take the human perception into account. Similarly, [25] reports on an implementation of an e-VC scheme for securing face images. In particular, equal error rates are presented with respect to a various set of parameters and databases, and the security of their scheme is discussed based on experiments. Based on experimental results in [25], several security claims are made. For example, based on Experiment 7 in [25], it is stated that exposing the identity of a secret face image by using the sheets alone is difficult. On the contrary, the picture taken from [25] (see Figure 1) suggests that a single sheet of a secret image reveals significant information about the image itself. In Figure 1, the generated sheets have similar appearance to the original image. Similarly, based on Experiment 8 in [25], it is stated that performing cross-matching across different applications is difficult.

In summary, we are not aware of a concrete formal security analysis of the protocols proposed and implemented in [17] and [25]. Several other visual biometric authentication schemes exist such as [18, 22, 25, 24], but there is no formal framework for analyzing biometric visual cryptographic schemes and quantifying their security claims.

Extensive analysis has been given to fuzzy extractors and their applications to biometric data [2, 21, 13, 31, 28, 11]. Biometrics are noisy sources of information, making the application of fuzzy extractors ideal when constructing biometric protocols. When fuzzy extractors are applied to biometric data, random strings

Figure 1: The picture is taken from [25].
are produced and require helper data to recover the original biometric information [13, 28]. The randomized sketching and recovery functions add to the privacy of the protocol and underlying biometric information. The notion of fuzzy sketch indistinguishability has been defined and explored [28, 11] by defining and analyzing security games involving a challenger and adversary. However, we cannot readily adapt these fuzzy extractor security results to e-BVC schemes. The inherent goal of e-BVC schemes is to avoid producing “random-looking” images or sets of pixels. For this reason, we must define new security notions and security games to quantify the security and privacy of e-BVC schemes. We add that although random variables defined on metric spaces are necessary in the discussion of fuzzy extractors, our level of abstraction does not require these tools.

In this paper, we extend our initial study [16] on the formal security analysis of biometric e-VC schemes (e-BVC). In [16], we proposed a general framework to help assess the security of e-BVC, and we formalized the notion of perfect resistance against false authentication. In this paper, we extend our framework with respect to indistinguishability and index privacy notions. As a result, we attempt a comprehensive theoretical analysis of e-BVC, and also discuss the practical impact of our framework and analysis on some recent implementations of biometric authentication schemes. In summary, our overall contributions are as follows:

1. In Section 2, we develop a framework and describe BVC schemes generically under our framework. In particular, we show how the face recognition protocol, recently proposed by Ross and Othman [25], fits our framework. In our analysis and examples, we choose [25] because, to our knowledge, it stands as the state-of-the-art e-BVC implementation with the most reasonable false accept and false reject rates. Moreover, [25] includes detailed security discussions with some strong security claims. However, none of the claims were proven due to the lack of a formal framework. For example, it is noted in [25] that experimental results (see Experiment 7 in [25]) confirm the difficulty of exposing the identity of the secret face image by using the sheets alone. However, [25] does not include a theoretical or quantitative analysis of such an adversarial task. Therefore, [25] is a natural choice to emphasize the practical impact of our framework.

2. In Section 3, we formalize the security notion of sheet indistinguishability and define perfect indistinguishability for BVC schemes. We present two attacks for challenging sheet indistinguishability, namely a guessing attack and a new distinguishing attack. As a result, we are able to provide a necessary condition for a BVC scheme to achieve perfect indistinguishability; see Corollary 3.4. Our case analysis in Section 3.3 shows that the face recognition protocol in [25] does not achieve perfect indistinguishability.
3. In order to demonstrate the practical impact of our indistinguishability notion, we introduce the index recovery notion and define perfect index privacy for BVC schemes in Section 4. We present a new index recovery attack and obtain a necessary condition for satisfying perfect index privacy; see Corollary 4.4. In particular, we show that [25] does not achieve perfect index privacy; see Section 4.2. We find that the success probability of an adversary can be at least twice better than that of random guess when attacking the given IMM database and Dataset G in [25]. See Section 4.2 for more details.

4. In Section 5, we formalize the notion of perfect resistance against false authentication under our framework and show that our formalization captures the traditional false acceptance attack under plausible assumptions; see Definition 5.1 and Remark 5.3. In Section 5.2, we propose a new and generic strategy for attacking e-BVC schemes. As an application, we present a case analysis for a recent implementation of a face recognition protocol in [25]. We verify that the protocol in [25] does not achieve perfect resistance against false authentication. More concretely, we show that an adversary can utilize our new attack and authenticate with probability of success greater than 0.45. To our knowledge, this attack idea has not been considered and quantitatively analyzed in the literature before. We should emphasize that our new attack strategy is expected to have significantly better success probability than the traditional false accept rate attacks in general. For example, in the case analysis of [25], we observe that our new attack increases the success probability from 0.005 to 0.45; see Section 5.3.

5. As a result of our framework and analysis, we are able to derive a new and quantifiable upper bound on the security of e-BVC schemes; see Remark 5.7.

Remark 1.1. As is common in provable security works [27, 1], our framework contains definitions of security games and reductions. The purpose is to provide more rigor in the security assessment of e-BVC schemes as well as creating proofs which are easy to verify.

2 Framework

Visual biometric authentication protocols require an enrollment and an authentication phase. During enrollment, a biometric image is captured and decomposed into, say \( n \), obfuscated images. These decomposed components of the image are then distributed into \( n \) databases. During the authentication phase, some biometric image is captured and systematically compared against reconstructed images. Here, input to the reconstruction procedure is a subset of images held in the
databases. This comparison is performed through a matching algorithm that computes a matching score. The matching score must exceed a certain value, so called a matching threshold, for a successful authentication.

To illustrate this idea, we elaborate on one of the biometric authentication protocols proposed in [25]. During the enrollment phase proposed in the face recognition scheme in [25], a biometric image is decomposed into two other face images, called sheets. The sheets are stored in separate databases, and according to security claim in [25] the individual sheets do not reveal the identity of the private face image. In fact, the private image is supposed to be recovered only when both sheets are present. The reconstruction is performed by superimposing the two sheet images to recover the original biometric image. This process of overlaying images is equivalent to the OR operator at the bit level [25]. Finally, the authentication of an image $\alpha$ requires the ORing of all pairs of sheet images until one ORed pair is a match with $\alpha$ with respect to a given matching threshold. We formalize this concept as follows.

Let $\Omega$ be a space of biometric images and $S$ a space of images (not necessarily biometric). Note that $\Omega$ is a subset of $S$. In the following, $M$ is a well-ordered set with “$\geq$” the comparison operator. Our framework requires the following oracles.

1. **Decomposition** is defined by the function
   \[
   D_n : \Omega \to S \times S \times \cdots \times S, \quad n \text{ copies}
   \]
   which decomposes one biometric image into $n$ images (a.k.a. sheets), not necessarily biometric.

2. **Reconstruction** is defined by the function
   \[
   R_t : S \times S \times \cdots \times S \to \Omega, \quad t \text{ copies}
   \]
   which takes $t$ sheets as input, and constructs a biometric image.

3. **Matching** is defined by the function
   \[
   M : \Omega \times \Omega \to M,
   \]
   which outputs some matching score $m_0 \in M$ given a pair of biometric images as input.
4. **Authentication** is defined by the function

\[ A_m : \Omega \times S \times S \times \cdots \times S \rightarrow \{0, 1\}, \]

where \( m \in M \) is the matching threshold of the authentication protocol. \( A_m \) takes a tuple \((\alpha, s_1, s_2, \ldots s_t)\), \( \alpha \in \Omega \), \( s_i \in S \) as input. Suppose \( \beta = R_t(s_1, s_2, \ldots, s_t) \) and \( m_0 = M(\alpha, \beta) \). Then the output of \( A_m \) is 1 if \( m_0 \geq m \), indicating a successful authentication. Otherwise, \( A_m \) outputs 0.

Suppose now that \( D_n(\alpha) = (s_1, s_2, \ldots s_n) \) and \( \beta = R_t(s_i_1, s_i_2, \ldots, s_i_t) \), where \( i_j \in \{1, \ldots, n\} \) are pairwise distinct. For the robustness of a system, it is expected that \( M(\alpha, \beta) = m_0 \geq m \). That is, \( A_m(\alpha, s_i_1, s_i_2, \ldots, s_i_t) = 1 \).

In our framework, we may denote a BVC scheme by the tuple \((\Omega, S, M, D_n, R_t, M, A_m)\).

**Naor and Shamir in our framework** As mentioned earlier in Section 1, Naor and Shamir [19] pioneered visual cryptography. It is easy to observe that construction of secret transparencies from an image (using a \((t,n)\)-visual secret sharing scheme) and the reconstruction of the original image from transparencies in [19] are captured by our oracles \( D_n \) and \( R_t \). Naor and Shamir’s (extended visual) cryptographic scheme can be naturally extended to a biometric authentication scheme with the addition of matching and authentication algorithms \( M \) and \( A_m \). We denote Naor and Shamir’s extended biometric authentication scheme by NS-e-BVC throughout the rest of this paper.

**Ross and Othman Scheme in our framework** The face recognition protocol presented by Ross and Othman in [25] fits our framework with \( t = n = 2 \) as follows.

The protocol employs a preselected collection of face images, called **host images**. Once a face image \( \alpha \) is presented for enrollment, an **Active Appearance Model** (AAM) is created, as outlined in [12, 29], based on facial landmarks and textures. Once the AAM has been created, the image undergoes annotation and has an associated registration cost. These factors determine which two host images \( h_1, h_2 \) are selected for the given image. These three images \((\alpha, h_1, h_2)\) are then sent through a digital halftoning and pixel expansion process before \( \alpha \) is decomposed into two sheets. We may denote this decomposition in our framework as:

\[ D_2(\alpha) = (s_1(\alpha), s_2(\alpha)). \]

The reconstruction algorithm is performed by stacking the two sheet images atop each other. This is computed as the binary OR operation on each pair of bits in the
sheets. We may denote this process in our framework as:

\[ R_2(s_1, s_2) = s_1 \oplus s_2, \]  

(2.2)

where \( \oplus \) denotes the binary OR operator.

Due to the nature of the digital halftoning and pixel expansion process, the stacking of sheets will not fully reconstruct the original image \( \alpha \). However, the face image will be recognizable to the human visual system as well as by the matching software. These claims are supported by experimental results in [25]. The matching and authentication oracles \( M \) and \( A_m \) are implemented by the Verilook SDK [20]. We denote Ross and Othman’s extended biometric authentication scheme (for face recognition) by RO-e-BVC throughout the rest of this paper.

As mentioned earlier in Section 1, RO-e-BVC is based on a further extension of e-VC, which improves on the quality of output images. The main motivation is to improve on the performance (e.g. equal error rates) of the biometric scheme. The trade-off between image quality and security is already noted in [17] even though we are not aware of a concrete analysis of this trade-off. On the contrary, some strong security properties about RO-e-BVC are claimed in [25]. In Section 3, we attempt to quantify the security of BVC schemes with respect to several security notions including indistinguishability and index privacy. In particular, we show that RO-e-BVC in [25] does not achieve perfect security. We also demonstrate some practical attacks on RO-e-BVC.

3 Indistinguishability Notion

In this section, we define the sheet indistinguishability notion for BVC schemes. Our motivation is to measure the advantage of an adversary who is trying to distinguish between pairs of genuine and imposter biometric images, defined below, by exploiting the sheets of the images. Note that adversaries should not have any non-trivial advantage in an ideal BVC scheme because a sheet of a biometric image is not supposed to reveal any information about the image itself.

First, we recall some common definitions in biometrics. A genuine pair is a pair of biometric images or some cryptographic transformation of images derived from the same person or entity. An imposter pair is a pair of biometric images which do not correspond to the same person. Given some matching oracle \( M \) and authentication oracle \( A_m \), we define a Genuine Accept as the event that the matching oracle \( M \) computes a matching score \( m_0 \geq m \), given a genuine pair of biometric images. That is, \( A_m(\alpha, \beta) = 1 \) for a genuine pair \( (\alpha, \beta) \). A False Reject is the event that \( A_m(\alpha, \beta) = 0 \) for a genuine pair \( (\alpha, \beta) \). A Genuine Reject is the event that \( M \) computes \( m_0 < m \), given an imposter pair. That is, \( A_m(\alpha, \beta) = 0 \)
for an imposter pair \((\alpha, \beta)\). A False Accept is the event that \(A_m(\alpha, \beta) = 1\) for an imposter pair \((\alpha, \beta)\). False Reject Rate \(\text{FRR}(m)\) with respect to a matching threshold \(m\) is computed by counting the number of false rejects found from a list of genuine pairs, and dividing this number by the size of the list. Similarly, False Accept Rate \(\text{FAR}(m)\) with respect to a matching threshold \(m\) is computed by counting the number of false accepts found from a list of imposter pairs, and diving this number by the size of the list.

3.1 Indistinguishability Game

Let \((\Omega, S, M, D_n, R_t, M, A_m)\) represent a BVC scheme. For simplicity, we assume \(t = n = 2\). We define the sheet indistinguishability of BVC with the following game \(G_{\text{IND}}\). Our definition is inspired from the indistinguishability definition in [28]. In \(G_{\text{IND}}\), \(A\) is a computationally bounded adversary and \(C\) represents a challenger.

**Indistinguishability Game** \(G_{\text{IND}}\)

1. The challenger \(C\) generates a private biometric data \(\alpha \in \Omega\) uniformly at random.

2. \(C\) selects uniformly at random a bit \(b \in \{0, 1\}\). If \(b = 0\), then \(C\) generates another private biometric data \(\beta \in \Omega\) uniformly at random such that \((\alpha, \beta)\) is an imposter pair. If \(b = 1\), then \(C\) generates some private biometric data \(\beta \in \Omega\) uniformly at random such that \((\alpha, \beta)\) is a genuine pair. The challenger sends the pair \((s_1(\alpha), s_1(\beta))\) to the adversary, where \(D_2(\alpha) = (s_1(\alpha), s_2(\alpha))\) as before.

3. \(A\) guesses \(b' \in \{0, 1\}\). \(A\) wins \(G_{\text{IND}}\) if \(b' = b\).

We define the success probability of \(A\) in \(G_{\text{IND}}\) as \(\Pr[b' = b]\), and the advantage of \(A\) attacking an e-BVC scheme in \(G_{\text{IND}}\) as

\[
\text{Adv}_{A}^{\text{IND}} = \left| \Pr[b' = b] - \frac{1}{2} \right|
\]

We say that an e-BVC scheme preserves sheet indistinguishability if \(\text{Adv}_{A}^{\text{IND}}\) is negligible for all possible \(A\). In particular, we say an e-BVC achieves perfect indistinguishability if \(\text{Adv}_{A}^{\text{IND}} = 0\) for all possible \(A\).

3.2 Indistinguishability Attacks

In this section, we analyze the security of a general e-BVC scheme with respect to the indistinguishability notion defined in Section 3.1.
Guessing Attack Suppose the adversary \( A \) plays the indistinguishability game \( G_{\text{IND}} \). Then \( A \) receives some tuple \((s_1(\alpha), s_1(\beta))\) from the challenger \( C \) and tries to produce a bit \( b' \) so that \( b' = b \). In the guessing attack, \( A \) guesses \( b \) by choosing a bit \( b' \) uniformly at random from \( \{0, 1\} \). Clearly, we have the following theorem.

**Theorem 3.1.** The success probability of \( A \) in the guessing attack is \( \Pr[b' = b] = \frac{1}{2} \) and the advantage of \( A \) is \( \text{Adv}^\text{IND}_{A} = 0 \).

In order to gain a non-trivial adversarial advantage (rather than \( \text{Adv}^\text{IND}_{A} = 0 \) as in the case of a guessing attack), we present a new distinguishing attack (NDA), where the adversary does not simply guess a bit \( b' \). We assume that \( A \) is provided with explicit definitions of algorithms and parameters in the e-BVC scheme under attack. In particular, \( A \) is assumed to have access to the matching oracle \( M \) and knows the matching threshold \( m \). This is a valid assumption because many protocols, such as [25], employ commercial software that can be purchased by anyone.

Before we describe the NDA, we define new genuine accept and genuine reject notions. Our definitions are analogous to the standard definitions of genuine accept and genuine reject notions except that they are specifically defined for the sheets rather than the original biometric images.

**Definition 3.2.** Let \((\Omega, S, M, D_n, R_t, M, A_m)\) represent an e-BVC scheme. \( \text{GAR}'(m) \) (or simply \( \text{GAR}' \)) is defined to be a function of the matching threshold \( m \) and denotes the rate at which \( M(s_1(\alpha), s_1(\beta)) \geq m \) given that \( (\alpha, \beta) \) is a genuine pair. Similarly, \( \text{GRR}'(m) \) (or, simply \( \text{GRR}' \)) is a function of \( m \) and denotes the rate at which \( M(s_1(\alpha), s_1(\beta)) < m \) given that \( (\alpha, \beta) \) is an imposter pair.

\( \text{GAR}' \) and \( \text{GRR}' \) definitions play a key role in analyzing the success probability of adversaries in our framework. More concretely, in an ideal e-BVC scheme one would intuitively expect that \( \text{GAR}' \approx 0 \) and \( \text{GRR}' \approx 1 \) because a sheet of a biometric image is not supposed to reveal any information about the image itself. In fact, our analysis throughout this paper confirms this intuition and provides a quantitative security analysis of e-BVC schemes; see Corollary 3.4 and Corollary 4.4.

**A New Distinguishing Attack (NDA)** Suppose \( A \) plays \( G_{\text{IND}} \) and receives \((s_1(\alpha), s_1(\beta))\) from \( C \). Then \( A \) queries the matching oracle \( M \) with this pair. If the matching score \( m_0 = M(s_1(\alpha), s_1(\beta)) \geq m \), then the adversary outputs \( b' = 1 \). Otherwise, if \( m_0 < m \), the adversary outputs \( b' = 0 \).

**Theorem 3.3.** The success probability of \( A \) in NDA is

\[
\Pr[b' = b] = \frac{1}{2}(\text{GAR}' + \text{GRR}')
\]  (3.1)
and the advantage of $A$ is

$$\text{Adv}_{A}^{\text{IND}} = \frac{1}{2} |\text{GAR}' + \text{GRR}' - 1|,$$  \hspace{1cm} (3.2)

**Proof.** The success probability of $A$ in NDA can be computed as

$$\Pr[b' = b] = \Pr[b = 0] \Pr[b' = 0|b = 0] + \Pr[b = 1] \Pr[b' = 1|b = 1]$$

$$= \frac{1}{2} (\Pr[b' = 0|b = 0] + \Pr[b' = 1|b = 1]). \hspace{1cm} (3.4)$$

Recall that when $b = 0$, the challenger selects an imposter pair $(\alpha, \beta)$. In NDA, $A$ computes the matching score $M(s_1(\alpha), s_1(\beta))$ and if this value is less than $m$, $A$ outputs $b' = 0$. Similarly, when $b = 1$, $C$ selects a genuine pair $(\alpha, \beta)$. $A$ computes the matching score $M(s_1(\alpha), s_1(\beta))$ and if this value is greater than or equal to $m$, $A$ outputs $b' = 1$. Therefore, we can rewrite (3.4) as follows:

$$\Pr[b' = b] = \frac{1}{2} \Pr[M(s_1(\alpha), s_1(\beta)) < m| (\alpha, \beta) \text{ Imposter}]$$

$$+ \frac{1}{2} \Pr[M(s_1(\alpha), s_1(\beta)) \geq m| (\alpha, \beta) \text{ Genuine}] \hspace{1cm} (3.6)$$

$$= \frac{1}{2} (\text{GRR}' + \text{GAR}') \hspace{1cm} (3.7)$$

It follows that

$$\text{Adv}_{A}^{\text{IND}} = \left| \Pr[b' = b] - \frac{1}{2} \right| = \frac{1}{2} |(\text{GRR}' + \text{GAR}') - 1|. \hspace{1cm} (3.8)$$

Our analysis yields a necessary condition for the perfect indistinguishability of an e-BVC scheme as stated in the following corollary.

**Corollary 3.4.** An e-BVC scheme cannot achieve perfect indistinguishability if $\text{GAR}' + \text{GRR}' \neq 1$.

**Proof.** It is clear from (3.2) that $\text{GAR}' + \text{GRR}' = 1$ is necessary for the perfect indistinguishability of a BVC scheme. \qed

**Remark 3.5.** Satisfying the equality $\text{GAR}' + \text{GRR}' = 1$ may not guarantee the perfect indistinguishability of an e-BVC scheme because NDA is just one way of attacking the system and there may exist other attack methods.

**Remark 3.6.** We have described the game $G_{\text{IND}}$ in which $A$ receives the pair $(s_1(\alpha), s_1(\beta))$ from $C$. Similarly, $G_{\text{IND}}$ can be defined such that $A$ receives the pair $(s_2(\alpha), s_2(\beta))$ from $C$. The advantage of $A$ may be different in these two cases; see Section 3.3 for example.
Table 1: The advantage of $\mathcal{A}$ in $G_{\text{IND}}$ (in percentages): Attacking RO-e-BVC under the new distinguishability attack.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>$s_1$ vs. $s_1$</th>
<th>$s_2$ vs. $s_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMM XM2</td>
<td>5.3 14.0</td>
<td>5.8 16.2</td>
</tr>
<tr>
<td>IMM XM2</td>
<td>14.3 18.3</td>
<td>10.0 11.7</td>
</tr>
<tr>
<td>IMM XM2</td>
<td>16.2 12.2</td>
<td>10.5 10.7</td>
</tr>
</tbody>
</table>

3.3 A Case Analysis for RO-e-BVC

As described earlier in Section 2, a visual face recognition protocol (RO-e-BVC) was proposed and implemented in [25]. Several experiments were conducted in [25] to analyze the security and privacy-preserving properties of RO-e-BVC. In particular, Experiment 7 in [25] considers the possibility of recovering a secret biometric image given only the first (second) copies of sheet images $s_1(\alpha)$ ($s_2(\alpha)$) as $\alpha$ runs through all enrolled images in a given database. It is noted in [25] that experimental results confirm the difficulty of exposing the identity of the secret face image by using the sheets alone. However, we are not aware of a concrete analysis or a proof of this claim. In this section, we apply our framework and security model to present a formal security analysis of the RO-e-BVC scheme with respect to the indistinguishability notion and show that RO-e-BVC does not achieve perfect indistinguishability.

In Experiment 7 in [25], 6 different subexperiments are performed. In particular, the face recognition protocol in [25] is implemented for 2 different databases (IMM and XM2VTS) and each database is considered with respect to 3 different datasets (A, F, and G) with a various number of host images. In Table IX in [25], equal error rates are reported in three different categories: 1) Matching reconstructed images i.e., $R_2((s_1(\alpha), s_2(\alpha))$ vs. $R_2((s_1(\beta), s_2(\beta))$; 2) Matching the first sheets of the decomposed images i.e., $s_1(\alpha)$ vs. $s_1(\beta)$; and 3) Matching the second sheets of the decomposed images i.e., $s_2(\alpha)$ vs. $s_2(\beta)$. Note that, an equal error rate $e$ in the second (and third) category yields $\text{GAR'} = \text{GRR'} = 1 - e$ in Theorem 3.3, which determines the advantage of an attacker as

$$\text{Adv}^{\text{IND}}_{\mathcal{A}} = \frac{1}{2}|1 - 2e|.$$ 

Based on the equal error rates reported in Table IX in [25], we summarize in Table 3.3 the advantage of $\mathcal{A}$ in $G_{\text{IND}}$ attacking RO-e-BVC under the new distinguishability attack (NDA). As seen in Table 3.3, various databases and datasets
yield various results. The adversarial advantage is non-zero in all of the cases and so RO-e-BVC does not achieve perfect indistinguishability.

4 Practical Impact of the New Distinguishing Attack: Index Recovery Notion

In this section, we further explore the practical impact of the advantage of an adversary in the indistinguishability game $G_{\text{IND}}$. In particular, we argue that the adversarial advantage can be exploited in a more practical attack scenario. We formally define the Index Recovery Game $G_{\text{REC}}$ and the notion of index privacy. We show that an adversary with non-zero advantage in $G_{\text{IND}}$ can be turned into an adversary with non-zero advantage in $G_{\text{REC}}$; see Corollary 4.6. We present a case analysis for the face recognition scheme RO-e-BVC [25] and show that RO-e-BVC does not achieve perfect index privacy.

4.1 A Practical Attack Scenario

Consider a user, Alice, who is enrolled in two service providers, say $S_1$ and $S_2$, with her biometric images $\alpha$ and $\beta$, respectively. We may assume that both $S_1$ and $S_2$ employ the same biometric visual cryptographic system BVC for authentication purposes. This is a valid assumption because, for example, RO-e-BVC [25] (with the same host image datasets) can be deployed by two different service providers in practice. We further assume that the underlying BVC is represented in our framework with $(D_2, R_2, M, A_m)$. In particular, $S_1$ will decompose Alice’s biometric information $\alpha$ into two sheets $s_1(\alpha)$ and $s_2(\alpha)$ and store them separately in two independent databases. Similarly, $S_2$ will decompose Alice’s biometric information $\beta$ into two sheets $s_1(\beta)$ and $s_2(\beta)$ and store them separately in two independent databases. Note that $\alpha$ and $\beta$ may not be identical even though they form a genuine pair.

Now, suppose that an adversary $A$ obtains one sheet image of Alice’s biometric information, $s_1(\alpha)$, from a database of $S_1$ and that $A$ knows Alice is a member of $S_2$. $A$ is assumed to have access to the first sheets $s_{1,j}$ of the decomposed biometric images in $S_2$’s database but not the second sheets $s_{2,j}$. The adversary’s objective is to recover the index $j$ such that $s_{1,j} = s_1(\beta)$. Recovering index $j$ potentially exposes sensitive information related to Alice which has been stored in the service provider. In the case of a gym or fitness center, birthdate, contact information, frequency of visits, and more may be attached to the user’s index.

This is a valid attack scenario because in an ideal BVC, the first sheet of a decomposed biometric image is not supposed to reveal any information about the original image.
We formalize the index recovery attack through the index recovery game $G_{\text{REC}}$. Let $(\Omega, S, M, D_n, R_t, M, A_m)$ represent a BVC scheme. For simplicity, we assume $t = n = 2$. In $G_{\text{REC}}$, $A$ is a computationally bounded adversary and $C$ represents a challenger.

**Index Recovery Game $G_{\text{REC}}$**

1. The challenger $C$ generates a private biometric data $\alpha \in \Omega$ uniformly at random.

2. Using the decomposition oracle $D_2$, $C$ generates $N$ pairs of biometric sheets $D_2(\beta_j) = (s_1, j, s_2, j)$ such that $(\alpha, \beta_j)$ is a genuine pair for exactly $k$ indices chosen uniformly at random with $1 \leq k < N$. $C$ also generates $D_2(\alpha) = (s_1(\alpha), s_2(\alpha))$.

3. $C$ sends $s_1(\alpha)$ and $\{s_1, j\}_{j=1}^N$ to the adversary $A$.

4. $A$ outputs an integer $j$ and wins if $(\alpha, \beta_j)$ is a genuine pair.

We define the success probability of $A$ in $G_{\text{REC}}$ as $\Pr[j : (\alpha, \beta_j) \text{ Genuine}]$, and the advantage of $A$ attacking an e-BVC scheme in $G_{\text{REC}}$ as

\[ \text{Adv}_{A}^{\text{REC}} = |\Pr[j : (\alpha, \beta_j) \text{ Genuine}] - p|, \]  

where $0 < p = k/N < 1$. We say that an e-BVC scheme preserves index privacy if $\text{Adv}_{A}^{\text{REC}}$ is negligible for all possible $A$. In particular, we say an e-BVC achieves perfect index privacy if $\text{Adv}_{A}^{\text{REC}} = 0$ for all possible $A$.

Note that, in an index recovery attack, $A$ can always choose $j$ at random and hope that $s_1, j = s_1(\beta_j)$. This concept is formalized in the following guessing attack.

**Guessing Attack** Suppose the adversary $A$ plays the index recovery game $G_{\text{REC}}$. Then $A$ receives $s_1(\alpha)$ and $\{s_1, j\}_{j=1}^N$ such that, for exactly $k$ of $s_1, j = s_1(\beta_j)$, $(\alpha, \beta_j)$ is a genuine pair. In the guessing attack, $A$ chooses $j \in [1, N]$ uniformly at random and outputs $j$. Clearly, we have the following theorem.

**Theorem 4.1.** The success probability of $A$ in the guessing attack is $\Pr[j : (\alpha, \beta_j) \text{ Genuine}] = k/N$ and the advantage of $A$ is $\text{Adv}_{A}^{\text{REC}} = 0$.

In an ideal scheme, we would expect that $A$’s success probability is no better than the success probability of a random guess and that $A$ has zero advantage $\text{Adv}_{A}^{\text{REC}} = 0$. Next, we propose a new index recovery attack and compute adversarial advantage. As a result, we obtain a necessary condition for perfect index privacy.
A New Index Recovery Attack (IND-REC)  $A$ receives $s_1(\alpha)$ and $\{s_{1,j}\}_{j=1}^N$ such that, for exactly $k$ of $s_{1,j}$, $s_{1,j} = s_1(\beta_j)$ and $(\alpha, \beta_j)$ is a genuine pair. In the attack, $A$ computes a matching score $m_j = M(s_1(\alpha), s_{1,j})$ for all $j$, and outputs an index $j$ for which $m_j \geq m$. If $m_j < m$ for all $j$, then $A$ chooses $j \in [1, N]$ uniformly at random and outputs $j$.

**Theorem 4.2.** Let $p = k/N$ with $k \in [1, N)$. If $\text{GAR}' = 0$, then the success probability of $A$ in IND-REC is $\Pr[j : (\alpha, \beta_j) \text{ Genuine}] = p$ and the advantage of $A$ is $\text{Adv}_{A}^{\text{REC}} = 0$. If $\text{GAR}' > 0$, then the success probability of $A$ in IND-REC is

$$\Pr[j : (\alpha, \beta_j) \text{ Genuine}] = \frac{p \text{GAR}'}{p \text{GAR}' + (1 - p)(1 - \text{GRR}')},$$

and the advantage of $A$ is

$$\text{Adv}_{A}^{\text{REC}} = \left| \frac{(p - p^2)(\text{GAR}' + \text{GRR}' - 1)}{p \text{GAR}' + (1 - p)(1 - \text{GRR}')} \right|,$$  \hspace{1cm} (4.2)

Proof: If $\text{GAR}' = 0$ then $m_j = M(s_1(\alpha), s_{1,j}) < m$ for all $j$ and $A$ will output $j \in [1, N]$ uniformly at random. Therefore, $\Pr[j : (\alpha, \beta_j) \text{ Genuine}] = p$ and $\text{Adv}_{A}^{\text{REC}} = 0$. Now, assume that $\text{GAR}' > 0$. The success probability of $A$ in IND-REC can be computed

$$\Pr[j : (\alpha, \beta_j) \text{ Genuine}]$$

$$= \Pr[(\alpha, \beta_j) \text{ Genuine} | M(s_1(\alpha), s_{1,j}) \geq m]$$

$$= \Pr[M(s_1(\alpha), s_{1,j}) \geq m | (\alpha, \beta_j) \text{ Genuine}] \cdot$$

$$\Pr[(\alpha, \beta_j) \text{ Genuine}]$$

$$= \text{GAR}' \frac{p}{p \text{GAR}' + (1 - p)(1 - \text{GRR}')},$$

\hspace{1cm} (4.4)
where the last equation follows because

\[
\Pr[M(s_1(\alpha), s_{1,j}) \geq m] = \Pr[(\alpha, \beta_j) \text{ Genuine}] \\
+ \Pr[(\alpha, \beta_j) \text{ Imposter}] \\
= \Pr[M(s_1(\alpha), s_{1,j}) \geq m | (\alpha, \beta_j) \text{ Genuine}] \\
+ \Pr[M(s_1(\alpha), s_{1,j}) \geq m | (\alpha, \beta_j) \text{ Imposter}] \\
= \Pr[(\alpha, \beta_j) \text{ Genuine}] \\
+ \Pr[(\alpha, \beta_j) \text{ Imposter}] \\
(1 - \Pr[M(s_1(\alpha), s_{1,j}) \geq m | (\alpha, \beta_j) \text{ Imposter}]) \\
= p \text{ GAR}' + (1 - p)(1 - \text{ GRR}')
\]

Finally, we write

\[
\text{Adv}_{\text{REC}}^\text{A} = \left| \frac{p \text{ GAR}'}{p \text{ GAR}' + (1 - p)(1 - \text{ GRR}')} - p \right| \\
= \left| \frac{(p - p^2)(\text{ GAR}' + \text{ GRR}' - 1)}{p \text{ GAR}' + (1 - p)(1 - \text{ GRR}')} \right|
\]

as required.

In Theorem 4.3, we derive upper and lower bounds on the success probability \( \Pr[j : (\alpha, \beta_j) \text{ Genuine}] \) of an adversary in \( \mathcal{G}_{\text{REC}} \).

**Theorem 4.3.** Let \( p, \text{ GAR}' \), and \( \text{ GRR}' \) be as defined in Definition 3.2. If \( \text{ GAR}' > 0 \), then the success probability \( \Pr[j : (\alpha, \beta_j) \text{ Genuine}] \) of an adversary in \( \text{IND-REC} \) satisfies the following:

1. \( \Pr[j : (\alpha, \beta_j) \text{ Genuine}] = p \) if \( \text{ GAR}' + \text{ GRR}' = 1 \).
2. \( p < \Pr[j : (\alpha, \beta_j) \text{ Genuine}] < p \frac{\text{ GAR}'}{1 - \text{ GRR}'} \) if \( \text{ GAR}' + \text{ GRR}' > 1 \).
3. \( p \frac{\text{ GAR}'}{1 - \text{ GRR}'} < \Pr[j : (\alpha, \beta_j) \text{ Genuine}] < p \) if \( \text{ GAR}' + \text{ GRR}' < 1 \).

**Proof.** It follows from (4.2) that if \( \text{ GAR}' + \text{ GRR}' = 1 \), then \( \Pr[j : (\alpha, \beta_j) \text{ Genuine}] = p \). If \( \text{ GAR}' + \text{ GRR}' > 1 \), then, using \( 0 \leq (1 - \text{ GRR}') < \text{ GAR}' \) we can write

\[
(1 - \text{ GRR}') < p \text{ GAR}' + (1 - p)(1 - \text{ GRR}') < \text{ GAR}',
\]
and it follows from (4.2) that

\[ p < \Pr[j : (\alpha, \beta_j) \text{ Genuine}] < p \frac{\text{GAR}'}{1 - \text{GRR}'} . \]

Similarly, if \( \text{GAR}' + \text{GRR}' < 1 \), then we can show that

\[ p \frac{\text{GAR}'}{1 - \text{GRR}'} < \Pr[j : (\alpha, \beta_j) \text{ Genuine}] < p . \]

Our analysis yields a necessary condition for the perfect index privacy of an e-BVC scheme as stated in the following corollary.

**Corollary 4.4.** An e-BVC scheme cannot achieve perfect index privacy if \( \text{GAR}' + \text{GRR}' \neq 1 \) and \( \text{GAR}' > 0 \). Moreover, if \( \text{GAR}' + \text{GRR}' \neq 1 \) and \( \text{GAR}' > 0 \), then the advantage \( \text{Adv}_{A}^{\text{REC}} \) of an adversary in IND-REC satisfies

\[ 0 < \text{Adv}_{A}^{\text{REC}} < p \left| \frac{\text{GAR}' + \text{GRR}' - 1}{1 - \text{GRR}'} \right|. \]  

**(4.9)**

**Proof.** It follows from (4.1), Theorem 4.2 and Theorem 4.3 that \( \text{Adv}_{A}^{\text{REC}} = 0 \) if and only if \( \text{GAR}' + \text{GRR}' = 1 \) or \( \text{GAR}' = 0 \). Therefore, perfect index privacy cannot be achieved if \( \text{GAR}' + \text{GRR}' \neq 1 \) and \( \text{GAR}' > 0 \). The inequality (4.9) follows from (4.1) and Theorem 4.3. \( \square \)

**Remark 4.5.** Satisfying the equality \( \text{GAR}' + \text{GRR}' = 1 \) may not guarantee the perfect index privacy of an e-BVC scheme because IND-REC is just one way of attacking the system and there may exist other attack methods.

The next corollary shows that an adversary with non-zero advantage in \( \text{G}_{\text{IND}} \) can be turned into an adversary with non-zero advantage in \( \text{G}_{\text{REC}} \), and vice versa.

**Corollary 4.6.** There exists an adversary with non-zero advantage in \( \text{G}_{\text{IND}} \) if and only if there exists an adversary with non-zero advantage in \( \text{G}_{\text{REC}} \).

**Proof.** The proof follows from (3.2) and (4.3), and from the fact that \( 0 < p < 1 \). \( \square \)

**Remark 4.7.** We have described the game \( \text{G}_{\text{REC}} \) in which \( A \) receives \( s_{1}(\alpha) \) and \( \{s_{1,j}\}_{j} \) from \( C \). Similarly, \( \text{G}_{\text{REC}} \) can be defined such that \( A \) receives \( s_{2}(\alpha) \) and \( \{s_{2,j}\}_{j} \) from \( C \). The advantage of \( A \) may be different in these two cases; see Section 4.2 for example.
4.2 A Case Analysis for RO-e-BVC

As an extension of our analysis in Section 3.3, we now analyze the advantage of \( \mathcal{A} \) in \( G_{\text{REC}} \) attacking RO-e-BVC [25] under the new index recovery attack (IND-REC). We apply our framework and security model to present a formal security analysis of the of the RO-e-BVC scheme with respect to the index recovery notion, and show that RO-e-BVC does not achieve perfect index privacy.

Recall that in Table IX in [25], equal error rates are reported in three different categories and in the last two of these three categories, an equal error rate \( e \) yields \( \text{GAR}' = \text{GRR}' = 1 - e \) in Theorem 4.2, which determines the advantage of an attacker as

\[
\text{Adv}^{\text{REC}}_{\text{A}} = \frac{p(1 - p)(1 - 2e)}{p(1 - e) + (1 - p)e}.
\]

Based on the equal error rates reported in Table IX in [25], we summarize in Table 4.2 the advantage of \( \mathcal{A} \) in \( G_{\text{REC}} \) attacking RO-e-BVC under the new index recovery attack (IND-REC) for a various number of \( N \) values. We also present the success probability \( \text{Pr}^{\text{REC}} = \text{Pr}[\alpha, \beta_j] \text{Genuine} \) of an adversary in IND-REC in comparison with \( \text{Pr}^{\text{Guess}} = \text{Pr}[\alpha, \beta_j] \text{Genuine} \) in the guessing attack.

In Table 4.2, various databases and datasets yield various values for the adversarial advantage. \( \text{Adv}^{\text{REC}}_{\text{A}} \) is non-zero in all of the cases and so RO-e-BVC does not achieve perfect index privacy. It is also interesting to compare the values in Table 4.2 with our theoretical estimates for \( \text{Adv}^{\text{REC}}_{\text{A}} \) in Corollary 4.4. Recall that in Corollary 4.4, we show that if \( \text{GAR}' + \text{GRR}' \neq 1 \) and \( \text{GAR}' > 0 \), then the advantage of an adversary in IND-REC satisfies

\[
0 < \text{Adv}^{\text{REC}}_{\text{A}} < p \left| \frac{\text{GAR}' + \text{GRR}' - 1}{1 - \text{GRR}'} \right|.
\]

For example, we derive from Table IX in [25] that \( \text{GAR}' = \text{GRR}' = 0.553 \) if RO-e-BVC is implemented with the IMM database and Dataset A, and if the first sheets are compared in the attack. Accordingly, we find out that

\[
0 < \text{Adv}^{\text{REC}}_{\text{A}} < p \left| \frac{\text{GAR}' + \text{GRR}' - 1}{1 - \text{GRR}'} \right| = 0.237p.
\]

In particular, if \( p = 0.01 \) and \( p = 0.001 \), then \( 0 < \text{Adv}^{\text{REC}}_{\text{A}} < 0.00237 \) and \( 0 < \text{Adv}^{\text{REC}}_{\text{A}} < 0.000237 \), respectively. We observe in Table 4.2 that the actual adversarial advantage values (0.00234 and 0.000237) are in fact very close to the theoretical upper bounds. We find that the greatest adversarial advantages are obtained when RO-e-BVC is implemented with the IMM database and Dataset G (success probability and advantage are bounded by 1.958\( p \) and 0.958\( p \), respectively) and when RO-e-BVC is implemented with the XM2 database and Dataset F.
Table 2: The advantage of $\mathcal{A}$ in $G_{\text{REC}}$: Attacking RO-e-BVC under the new index recovery attack with $N = 100$ and $N = 1000$.

<table>
<thead>
<tr>
<th>Database Dataset</th>
<th>IMM</th>
<th>XM2</th>
<th>IMM</th>
<th>XM2</th>
<th>IMM</th>
<th>XM2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
<td>F</td>
<td>A</td>
<td>F</td>
<td>G</td>
<td>G</td>
</tr>
<tr>
<td>$(s_1 \text{ vs. } s_{1,j})$</td>
<td>N</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Pr$_{\text{Guess}}$</td>
<td>.01</td>
<td>.01</td>
<td>.01</td>
<td>.01</td>
<td>.01</td>
</tr>
<tr>
<td></td>
<td>Pr$_{\text{REC}}$</td>
<td>.01234</td>
<td>.01764</td>
<td>.01787</td>
<td>.02130</td>
<td>.01940</td>
</tr>
<tr>
<td></td>
<td>Adv$_{A}^{\text{REC}}$</td>
<td>.00234</td>
<td>.00764</td>
<td>.00787</td>
<td>.01130</td>
<td>.00940</td>
</tr>
<tr>
<td>$(s_1 \text{ vs. } s_{1,j})$</td>
<td>N</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td></td>
<td>Pr$_{\text{Guess}}$</td>
<td>.001</td>
<td>.001</td>
<td>.001</td>
<td>.001</td>
<td>.001</td>
</tr>
<tr>
<td></td>
<td>Pr$_{\text{REC}}$</td>
<td>.001237</td>
<td>.00178</td>
<td>.00180</td>
<td>.00215</td>
<td>.00195</td>
</tr>
<tr>
<td></td>
<td>Adv$_{A}^{\text{REC}}$</td>
<td>.000237</td>
<td>.00078</td>
<td>.00080</td>
<td>.00115</td>
<td>.00095</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Database Dataset</th>
<th>IMM</th>
<th>XM2</th>
<th>IMM</th>
<th>XM2</th>
<th>IMM</th>
<th>XM2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
<td>F</td>
<td>A</td>
<td>F</td>
<td>G</td>
<td>G</td>
</tr>
<tr>
<td>$(s_2 \text{ vs. } s_{2,j})$</td>
<td>N</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Pr$_{\text{Guess}}$</td>
<td>.01</td>
<td>.01</td>
<td>.01</td>
<td>.01</td>
<td>.01</td>
</tr>
<tr>
<td></td>
<td>Pr$_{\text{REC}}$</td>
<td>.01259</td>
<td>.01940</td>
<td>.01493</td>
<td>.01601</td>
<td>.01524</td>
</tr>
<tr>
<td></td>
<td>Adv$_{A}^{\text{REC}}$</td>
<td>.00259</td>
<td>.00940</td>
<td>.00493</td>
<td>.00601</td>
<td>.00524</td>
</tr>
<tr>
<td>$(s_2 \text{ vs. } s_{2,j})$</td>
<td>N</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td></td>
<td>Pr$_{\text{Guess}}$</td>
<td>.001</td>
<td>.001</td>
<td>.001</td>
<td>.001</td>
<td>.001</td>
</tr>
<tr>
<td></td>
<td>Pr$_{\text{REC}}$</td>
<td>.00126</td>
<td>.00196</td>
<td>.00150</td>
<td>.00161</td>
<td>.00153</td>
</tr>
<tr>
<td></td>
<td>Adv$_{A}^{\text{REC}}$</td>
<td>.00026</td>
<td>.00096</td>
<td>.00050</td>
<td>.00061</td>
<td>.00053</td>
</tr>
</tbody>
</table>
success probability and advantage bounded by $2.154p$ and $1.154p$, respectively). Therefore, the success probability of an adversary can be at least twice better than that of a random guess when attacking certain implementations of RO-e-BVC.

**Remark 4.8.** In Section 3 and Section 4 we discussed security of e-BVC schemes with respect to indistinguishability and index privacy notions. It is worth noting that the NDA and IND-REC attacks we described are conservative in the sense that they consider rather weak adversaries. We anticipate that there exist stronger attacks. For example, in NDA, the adversary $A$ exploits his access to the matching oracle. $A$’s advantage is likely to increase if the decomposition or reconstruction oracles are also accessed during the attack. Similarly, in IND-REC, the adversarial advantage is likely to increase if $A$ outputs an index $j$ such that $m_j = \mathcal{M}(s_1(\alpha), s_{1,j})$ is maximum among all $\{m_j\}_{j=1}^N$ (rather than outputting an index $j$ with $m_j \geq m$).

## 5 Modified False Acceptance Attack for e-BVC Schemes

In a traditional false acceptance attack, an adversary inserts a biometric image and hopes for a successful authentication. It is known that the success probability of an adversary in this attack is correlated with the false acceptance rate of the system. First, we capture this false acceptance rate attack idea and formalize it under the authentication game $G_{AUTH}$. In particular, the guessing strategy in $G_{AUTH}$ corresponds to an adversary who inserts random biometric images for authentication and whose success probability is asymptotically the same as the false acceptance rate of the underlying scheme.

Before describing $G_{AUTH}$, we induce some natural structure to the space of biometric images $\Omega$. We assume that $\Omega$ is a universal finite set of biometric images so that $\Omega = \{\omega_1, \omega_2, \ldots, \omega_\ell\}$. Let $N$ denote the number of unique individuals with at least one biometric image contained in $\Omega$. We consider a partitioning of $\Omega$ as a disjoint union of $W_i$ subsets, where $W_i$ denotes the set of all genuine images that correspond to the $i$th individual for $i = 1, \ldots, N$. In summary, we have

1. For any $x, y \in \Omega$ and $i \neq j$, if $x \in W_i$ and $y \in W_j$, then $(x, y)$ is an imposter pair.
2. For $x, y \in \Omega$, if $x, y \in W_i$ then $(x, y)$ is a genuine pair.
3. $W_1 \cup W_2 \cup \ldots \cup W_N = \Omega$, $W_i \cap W_j = \emptyset$ for all $i \neq j$, and $\sum_{i=1}^N |W_i| = |\Omega|$.

Now, we are ready to describe $G_{AUTH}$. Let $(\Omega, S, M, D_n, R_t, \mathcal{M}, A_m)$ represent an e-BVC scheme. For simplicity, we assume $t = n = 2$. As before, $A$ is
a computationally bounded adversary and \( C \) represents a challenger. It is assumed that \( A \) knows the parameter set of the e-BVC scheme except the private images (denoted by \( \Omega' \) below). It is also assumed that \( A \) has access to the first sheets of the decomposed biometric images in a database. This is a valid attack scenario because in an ideal BVC, the first sheet of a decomposed biometric image is not supposed to reveal any information about the original image.

5.1 Authentication Game

Authentication Game \( G_{\text{AUTH}} \)

1. The challenger \( C \) chooses \( k \) indices \( i_1, ..., i_k \) uniformly at random, where \( 1 \leq k \leq N \). \( C \) generates a secret subcollection \( \Omega' = \{w_{i_1}, ..., w_{i_k}\} \subseteq \Omega \) of private biometric images, where \( w_{i_j} \in W_{i_j} \).

2. \( C \) computes \( D_2(w') = (s_1(w'), s_2(w')) \) and sends \( s_1(w') \) for all \( w' \in \Omega' \).

3. \( A \) outputs an image \( w \in \Omega \) and wins if \( A_m(w, w') = 1 \) for some \( w' \in \Omega' \).

We define the success probability of \( A \) in \( G_{\text{AUTH}} \) as \( \Pr[A_m(w, w') = 1] \), and the advantage of \( A \) attacking an e-BVC scheme in \( G_{\text{AUTH}} \) as

\[
\text{Adv}_{\text{AUTH}}^{A} = \left| \Pr[A_m(w, w') = 1] - \frac{\sum_{j=1}^{k} |W_{i_j}|}{|\Omega|} \cdot \text{GAR} - \frac{k|\Omega| - \left( \sum_{j=1}^{k} |W_{i_j}| \right)}{|\Omega|} \cdot \text{FAR} \right|. \tag{5.1}
\]

where FAR and GAR are the false acceptance and genuine acceptance rates of the underlying system. The definition of \( \text{Adv}_{\text{AUTH}}^{A} \) makes sense because we show in Theorem 5.2 that the adversarial advantage in the guessing attack is zero as expected.

We are now ready to formalize the notion of perfect resistance against false authentication based on \( G_{\text{AUTH}} \) and \( \text{Adv}_{\text{AUTH}}^{A} \).

Definition 5.1. We say that an e-BVC scheme resists false authentication if \( \text{Adv}_{\text{AUTH}}^{A} \) is negligible for all possible \( A \). In particular, we say an e-BVC achieves perfect resistance against false authentication if \( \text{Adv}_{\text{AUTH}}^{A} = 0 \) for all possible \( A \).

Note that, in an authentication attack, \( A \) can always choose \( w \in \Omega \) at random and hope that \( A_m(w, w') = 1 \) for some \( w' \in \Omega' \). This concept is formalized in the following guessing attack.
Guessing Attack  Suppose the adversary $A$ plays the authentication game $G_{\text{AUTH}}$. Then $A$ receives $s_1(w')$ for all $w' \in \Omega'$. In the guessing attack, $A$ chooses $w \in \Omega$ uniformly at random and outputs $w$.

In the following, we compute the success probability of $A$ in the guessing attack and conclude that it is practically the same as the false acceptance rate of the underlying scheme.

**Theorem 5.2.** The success probability of $A$ in the guessing attack is

$$\Pr[A_m(w, w') = 1] = \min(M, 1),$$

where

$$M = \sum_{j=1}^{k} \left[ \frac{|W_{ij}|}{|\Omega|} \cdot \text{GAR} + \frac{k|\Omega| - (\sum_{j=1}^{k} |W_{ij}|)}{|\Omega|} \cdot \text{FAR} \right].$$

The advantage of $A$ is $\text{Adv}_{\text{AUTH}}^A = 0$.

**Proof.** The success probability of $A$ in the guessing attack can be computed as

$$\Pr[A_m(w, w') = 1] = \min(M, 1),$$

where $M$ is the expected number of matches when $w$ is compared against all $w'$ in the database. We can write

$$M = \sum_{j=1}^{k} \left[ \Pr(w \in W_{ij}) \Pr(M(w, w_{ij}) \geq m|w \in W_{ij}) 
+ \Pr(w \notin W_{ij}) \Pr(M(w, w_{ij}) \geq m|w \notin W_{ij}) \right]$$

$$= \sum_{j=1}^{k} \left[ \frac{|W_{ij}|}{|\Omega|} \cdot \text{GAR} + \frac{|\Omega| - |W_{ij}|}{|\Omega|} \cdot \text{FAR} \right]$$

$$= \sum_{j=1}^{k} \frac{|W_{ij}|}{|\Omega|} \cdot \text{GAR} + \frac{k|\Omega| - (\sum_{j=1}^{k} |W_{ij}|)}{|\Omega|} \cdot \text{FAR},$$

as required. Finally, $\text{Adv}_{\text{AUTH}}^A = 0$ follows from (5.1).

**Remark 5.3.** In a robust authentication system, it is expected that $\text{GAR} > \text{FAR}$, whence,

$$\Pr[A_m(w, w') = 1] \geq \min(k \cdot \text{FAR}, 1). \quad (5.2)$$

On the other hand, in a practical authentication system, $\Pr[A_m(w, w') = 1]$ cannot be much higher than $\min(k \cdot \text{FAR}, 1)$ because it is also expected that $k$ (the number of enrolled users in a database) is much smaller than $N$ (the total number...
of users) and so \( k/N \approx 0 \). Consequently, under the plausible assumption that \( |W_i| \approx |W_j| \) for all \( i, j \), we can write

\[
M = \frac{k}{N} \cdot (\text{GAR} - \text{FAR}) + k \cdot \text{FAR} \approx k \cdot \text{FAR}
\]

and

\[
\Pr[A_m(w, w') = 1] \approx \min(k \cdot \text{FAR}, 1).
\]

Therefore, we see that the guessing attack in \( \text{G}_{\text{AUTH}} \) is a way of formalizing the so-called false acceptance attack.

Based on Remark 5.3, we may state the adversarial advantage in \( \text{G}_{\text{AUTH}} \) in a rather simplified form as follows:

\[
\text{Adv}^\ast_{\text{AUTH}} = \left| \Pr[A_m(w, w') = 1] - \min(k \cdot \text{FAR}, 1) \right|.
\] (5.3)

5.2 A New Strategy for Attacking e-BVC

Note that, in an ideal scheme, one would expect that \( \mathcal{A} \)'s success probability is no better than the success probability of a random guess and that \( \mathcal{A} \) has zero advantage \( \text{Adv}^\ast_{\text{AUTH}} = 0 \) (or \( \text{Adv}^\ast_{\text{AUTH}} \approx 0 \)). In this section, we modify the traditional false acceptance attack and introduce a new strategy for attacking e-BVC schemes. We compute the success probability and advantage of an adversary in this modified false acceptance attack. Finally, we compare the advantage of adversaries in the guessing attack and the new false acceptance rate attack. As an example, our analysis yields that the success probability of an adversary attacking RO-e-BVC [25] under the new false acceptance rate attack increases from 0.005 to 0.45.

First, we define new genuine accept (reject) and false accept (reject) notions.

**Definition 5.4.** Let \((\Omega, S, M, D_n, R_t, \mathcal{M}, A_m)\) represent an e-BVC scheme. \( \text{GAR}''(m) \) (or, simply \( \text{GAR}'' \)) is defined to be a function of the matching threshold \( m \) and denotes the rate at which \( M(s_1(\alpha), \beta) \geq m \) given that \((\alpha, \beta)\) is a genuine pair. Similarly, \( \text{FAR}''(m) \) (or, simply \( \text{FAR}'' \)) is a function of \( m \) and denotes the rate at which \( M(s_1(\alpha), \beta) \geq m \) given that \((\alpha, \beta)\) is an imposter pair.

Note that in an ideal e-BVC scheme one would intuitively expect that \( \text{GAR}'' \approx 0 \) and \( \text{FAR}'' \approx 0 \) because a sheet of a biometric image is not supposed to reveal any information about the image itself. Our new authentication attack and its analysis in Theorem 5.5 confirms this intuition by showing that the success probability and the advantage of an adversary increases as \( \text{GAR}'' \) and \( \text{FAR}'' \) increase.
A New Authentication Attack (N-AUTH) Suppose \(A\) plays \(G_{\text{AUTH}}\) and so she receives a set of sheets \(\{s_{1,j} : s_{1,j} = s_1(w_{ij}), w_{ij} \in \Omega', j = 1, ..., k\}\). \(A\) chooses an index \(j \in [1, k]\) uniformly at random and outputs \(s_{1,j}\) as an attempt for authentication.

**Theorem 5.5.** The success probability of \(A\) in N-AUTH is

\[
\Pr[A_m(w, w') = 1] = \min(GAR'' + (k - 1)FAR'', 1),
\]

and the simplified advantage of \(A\) is

\[
\text{Adv}^\text{AUTH} = \left| \min(GAR'' + (k - 1)FAR'', 1) - \min(k \cdot FAR, 1) \right|.
\]

**Proof.** Note that \(A\) in N-AUTH outputs \(s_{1,j} = s_1(w_{ij})\), where \((w_{ij}, w')\) is an imposter pair for all \(w' \in \Omega'\) except when \(w' = w_{ij}\). Therefore, \(s_{1,j}\) and the set \(\Omega'\) form \((k - 1)\) imposter pairs and 1 genuine pair in total, and we can compute the success probability of \(A\) in N-AUTH

\[
\Pr[A_m(w, w') = 1] = \min(GAR'' + (k - 1)FAR'', 1).
\]

It follows from (5.3) that

\[
\text{Adv}^\text{AUTH} = \left| \min(GAR'' + (k - 1)FAR'', 1) - \min(k \cdot FAR, 1) \right|.
\]

\[\square\]

**Remark 5.6.** In an ideal e-BVC, \(s_1(\alpha)\) is not supposed to reveal any information about the original image \(\alpha\). Therefore, it is expected that the three distributions \(\{(s_1(\alpha), \beta) : (\alpha, \beta) \text{ is genuine}\}, \{(s_1(\alpha), \beta) : (\alpha, \beta) \text{ is imposter}\}, \text{and} \{(\alpha, \beta) : (\alpha, \beta) \text{ is imposter}\}\) are indistinguishable, and hence \(\text{GAR''} \approx \text{FAR''} \approx \text{FAR}\). This implies that, an ideal e-BVC satisfies

\[
\text{Adv}^\text{AUTH} = \left| \min(GAR'' + (k - 1)FAR'', 1) - \min(k \cdot FAR, 1) \right| \approx 0.
\]

In other words, N-AUTH does not yield any adversarial advantage over the guessing attack for ideal e-BVC, as expected.

**Remark 5.7.** Based on our analysis of the guessing attack and the new authentication attack, we can conclude that the success probability of an adversary in an authentication game \(G_{\text{AUTH}}\) is

\[
\Pr[A_m(w, w') = 1] \geq \max \left[ \min(GAR'' + (k - 1)FAR'', 1), \right. \min(k \cdot FAR, 1)].
\]
This gives a quantifiable upper bound on the security of e-BVC schemes, where the quantification is performed based on the size $k$ of the system database, and measurable rates $\text{GAR}''$, $\text{FAR}''$, and $\text{FAR}$. On the other hand, one should be careful assessing the security of the system as this is only an upper bound on the security based on just two attack methods. There may exist other and better attacks in general.

### 5.3 A Case Analysis for RO-e-BVC

As described earlier in Section 2, a visual face recognition protocol (RO-e-BVC) was proposed and implemented in [25]. More concretely, the scheme in [25] is implemented for 2 different databases (IMM and XM2VTS) and each database is considered with respect to 3 different datasets (A, F, and G) with a various number of host images. Several experiments were conducted in [25] to analyze the security and privacy-preserving properties of RO-e-BVC. In particular, Experiment 3 in [25] considers the possibility of matching one of the secret sheets of an image against the image itself, and does not consider this as a security threat.

On the contrary, we observe based on the illustration in Figure 15 in [25] that at least one of the sheets of the decomposed images looks similar to the original image. Therefore, an adversary is expected to have significant advantage in attacking RO-e-BVC by mounting the N-AUTH attack as described in Section 5. In fact, in Experiment 3 in [25] it is reported that the equal error rate of a particular implementation of the RO-e-BVC scheme is very small: $\text{FAR} = \text{FRR} \approx 0$ when the IMM database is used with the dataset A and $\text{FAR} = \text{FRR} \approx 0.005$ when the XM2VTS database is used with the dataset A. It is also reported under the same setting that if single sheets are compared against original images then the resultant equal error rates are greater than 0.45. In other words, $\text{FAR}'' = 1 - \text{GAR}'' > 0.45$. It follows from Theorem 5.5 that the success probability of an adversary in attacking RO-e-BVC under N-AUTH is $\Pr[A_m(w, w') = 1] > 0.45$, which is significantly greater than the success probability of an adversary in attacking RO-e-BVC under the traditional false acceptance attack, or equivalently the guessing attack. We conclude that RO-e-BVC in [25] does not achieve perfect resistance against false authentication and adversaries can gain significant advantage in attacking RO-e-BVC under N-AUTH.

### 6 Conclusion

We developed a framework and described biometric visual cryptographic schemes generically under our framework. We formalized several security notions and def-
initions including sheet indistinguishability, perfect indistinguishability, index recovery, perfect index privacy, and perfect resistance against false authentication. We also proposed new and generic strategies for attacking e-BVC schemes such as new distinguishing attack, new index recovery, and new authentication attack. Our quantitative analysis verifies the practical impact of our framework and offers concrete upper bounds on the security of e-BVC. As an application of our analysis we were able to disprove some of the security claims in [25].

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References


