**SCIS 2009** The 2009 Symposium on Cryptography and Information Security
Otsu, Japan, Jan. 20-23, 2009
The Institute of Electronics, Information and Communication Engineers

# A new framework for constructing matching algorithms secure against the wolf attack in biometric authentication systems

Manabu Inuma *† Akira Otsuka *† Hideki Imai *†

**Abstract**— In [4], we proposed a theoretical framework to construct matching algorithms for any biometric authentication systems. In this paper, we will introduce the results in [4] and add some comments on the accuracy (*FAR* and *FRR*) of our proposed matching algorithms (Lemma 6, 7, 8). Conventional matching algorithms are not necessarily secure against strong intentional impersonation attacks such as wolf attacks. The wolf attack is an attempt to impersonate a genuine user by presenting a "wolf" to a biometric authentication system without the knowledge of a genuine user's biometric sample. A "wolf" is a sample which can be accepted as a match with multiple templates. The wolf attack probability (*WAP*) is the maximum success probability of the wolf attack, which was proposed by Une, Otsuka, Imai, as a measure for evaluating security of biometric authentication systems [9], [10]. In [4], we presented a principle for construction of secure matching algorithms against the wolf attack for any biometric authentication systems. The ideal matching algorithm determines a threshold for each input value depending on the probability distribution of the (Hamming) distances. Then we showed that if the information about the probability distribution for each input value is perfectly given, then our matching algorithm is secure against the wolf attack (Theorem 9, 10) [4]. Our generalized matching algorithm gives a theoretical framework to construct secure matching algorithms. How lower *WAP* is achievable depends on how accurately the entropy is estimated. Then there is a trade-off between the efficiency and the achievable *WAP*. Almost every conventional matching algorithm employs a fixed threshold and hence it can be regarded as an efficient but insecure instance of our theoretical framework. Daugman's algorithm proposed in [3] can also be regarded as a non-optimal instance of our framework.

**Keywords:** Biometric authentication, The wolf attack probability, Maching algorithm, Framework

## 1 Introduction

Biometric authentication systems automatically identify or verify individuals by physiological or behavioral characteristics. They are used in various services such as the immigration control at an airport, the banking transactions at an ATM, the access control to restricted areas in a building, and so on. The increase in the need of biometric authentication systems makes it important to explicitly evaluate the security of them.

We focus on the security against the intentional impersonation attack such as a brute-force attack, and a zero-effort attack, an artefact attack.

The false acceptance rate (*FAR*) (see the definition (3) in Section 2.2) is traditionally used as a security measure against the zero-effort impersonation attack. The zero-effort approach assumes that an attacker will present his/her own biometric data. But, it is clearly not a rational assumption, since an attacker attempting to impersonate a genuine user will try to present a biometric data of the genuine user or its imitation.

Ratha et al. approximately calculate the success probability of a brute-force attack in a typical fingerprint-minutiae matching algorithm [8]. The brute-force approach assumes that an attacker blindly selects an input value. However, if an attacker has some information about the algorithm employed in the system, the attacker might be able to find a sample which shows high similarity to most of the templates. Such a biometric sample is called a **wolf** (cf. [5]). An attacker could impersonate a genuine user with much higher probability than *FAR* by presenting a wolf to a biometric authentication system.

With regard to the artefact attack, Matsumoto et al. showed that some biometric authentication systems often falsely accepts some artefacts [7]. Therefore we should assume that an attacker may find a special input value not only from biometric samples but also from non-biometric samples. Une, Otsuka, Imai [9], [10] extended the definition of a wolf to include a non-biometric input value and defined the **wolf attack probability (***WAP***)** (see Definition 4). *WAP* can be regarded as the upper bound of the success probability of attacks without the knowledge of a genuine user's biometric sample. Une, Otsuka, Imai proposed that *WAP* can be used as a security measure to evaluate the lower bound of a security level in a biometric au-

* Research Center for Information Security (RCIS) National Institute of Advanced Industrial Science and Technology (AIST) Akihabara-Daibiru Room 1102, 1-18-13, Sotokanda, Chiyoda-ku Tokyo 101-0021 JAPAN

† Department of Electrical, Electronic, and Communication Engineering Faculty of Science and Engineering, Chuo University 1-13-27 Kasuga, Bunkyo-ku Tokyo 112-8551 JAPAN

thentication system.
Our goal is to propose a theoretical framework to construct matching algorithms secure against the wolf attack for any biometric authentication systems. Almost every conventional matching algorithm employs a fixed threshold determined based on *FAR* and the false rejection rate (*FRR*) (see the definition (1) in Section 2.1). However, it is not always secure against the wolf attack as mentioned above.
Surprisingly, as far as we know, no research have been conducted on security of matching algorithms until now.
Suppose a matching algorithm employs a threshold determined for each input value $s$ by using the entropy of the probability distribution of the distances between $s$ and the templates of all genuine users (see Section 3.1 and 3.2). We prove that if, for each input value $s$, the probability distribution is perfectly given, then the above matching algorithm is secure against the wolf attack (Theorem 9). Moreover, in the case where the above distributions are normal, we can construct a optimally secure matching algorithm, namely *WAP* can be minimized to the same value as the average of $AR_u$ over all genuine users (Theorem 10). Note that there is a worry that our proposed matching algorithm might make *FRR* extremely high. However, in the normal distribution case, if we chose a suitable parameter (denoted by $\alpha$) such that $FRR = FAR$, then, by Lemma 6, 7, 8, the proposed matching algorithm can be accurate and secure.
In the real world, it might be difficult to perfectly calculate the entropy for each input value, however, a more accurate computation of the entropy can achieve a lower *WAP*. Then there is a trade-off between the efficiency, that is, the time complexity of the matching algorithm and the achievable *WAP* in the matching algorithm.
Previous results can be regarded as instances of our theoretical framework. Almost every previous matching algorithm employs a fixed threshold. In our theoretical framework, it can be regarded as an efficient but insecure instance as mentioned above.
Daugman [3] proposed a matching algorithm in which a threshold is determined for each match by taking account the number of bits available for comparison. His algorithm can make *WAP* relatively lower than that for an ordinary algorithm employing a fixed threshold. However, his matching algorithm is not optimal against the wolf attack (see details in Section 4).

## 2 Model (Preliminaries)

A biometric authentication system can be used for verification or identification of individuals. In verification, a user of the system claims to have a certain identity and the biometric system performs a one to one comparison between the offered biometric data and the template which is linked to the claimed identity. In identification, a one to all comparison is performed between the offered data and all available template stored in the database to reveal the identity of an individual. In this paper, we will discuss verification systems.
Let $\mathcal{U}$ be a set of all possible users of the biometric authentication system. Namely $\mathcal{U}$ is a set of all human individuals. For each user $u \in \mathcal{U}$, the identity of $u$ can be denoted by $u$, namely the identities of users can be identified with $\mathcal{U}$. Let $\mathcal{M}$ be a finite set with a symmetric prametric function $d : \mathcal{M} \times \mathcal{M} \to \mathbb{R}$, namely $d(x, y) = d(y, x)$, $d(x, y) \geq 0$, $d(x, x) = 0$ for all $x, y \in \mathcal{M}$.
In an enrollment phase, for any user $u \in \mathcal{U}$, an acquisition device measures a biometric data of $u$. After processing the measurement data and extracting relevant features, the features are represented as an element $t_u$ of $\mathcal{M}$. Then the template $t_u$ of $u \in \mathcal{U}$ is stored in the database of the system. In a verification phase (matching phase) *match*, first, a user $v \in \mathcal{U}$ claims an identity $w \in \mathcal{U}$. Here we consider that a user does not always claim a correct identity to the system. Then a biometric measurement is acquired from $v$ and this measurement is transformed into an element $s$ of $\mathcal{M}$. A matching process compares $s$ with $t_w$ and *match* generates a message, *accept* or *reject*, by using a predetermined threshold $\tau \in \mathbb{R}_{\geq 0}$ as follows:

$$match(v, w) = \begin{cases} accept & \text{if } d(s, t_w) < \tau \\ reject & \text{if } d(s, t_w) \geq \tau \end{cases} .$$

For the simplicity, we assume that a user $u \in \mathcal{U}$ presents the same biometric sample of $u$ both in an enrollment phase and in a verification phase. Then $\mathcal{U}$ can be regarded as a set of the biometric samples of the users. For each biometric sample $u \in \mathcal{U}$, let $X_u$ be a random variable on $\mathcal{M}$ representing noisy versions of $u$, namely $P(X_u = s)$ denotes the probability that biometric data of $u$ will be transformed into $s \in \mathcal{M}$. Assume that, for any $u \in \mathcal{U}$, the fluctuation of $u$ in the enrollment phase and that in the verification phase are represented by the same random value $X_u$ and they are independent. Namely, we assume that, for any $u, v \in \mathcal{U}$ and any $s, t \in \mathcal{M}$, $P(X_u = s, X_v = t)$ is the probability that $u$ will be transformed into $s$ in the enrollment phase and $v$ will be transformed into $t$ in the verification phase and

$$P(X_u = s, X_v = t) = P(X_u = s)P(X_v = t) .$$

### 2.1 The false rejection rate

The false rejection rate (*FRR*) is the probability that a genuine user is rejected, namely it is defined by

$$\begin{aligned} FRR &= \operatorname*{Ave}_{u \in \mathcal{U}} P(\, match(u, u) = reject\,) \\ &= 1 - \frac{1}{n} \sum_{u \in \mathcal{U}} \sum_{\substack{(s,t) \in \mathcal{M} \times \mathcal{M} \\ d(s,t) < \tau}} P(X_u = s)P(X_u = t) \end{aligned} \tag{1}$$

where $n = \#\mathcal{U}$. For each user $u \in \mathcal{U}$, let $FRR_u$ denote the probability that the user $u$ with the correct identity claim $u$ will be rejected. Namely, $FRR_u$ is defined by

$$FRR_u = 1 - \sum_{\substack{(s,t) \in \mathcal{M} \\ d(s,t) < \tau}} P(X_u = s)P(X_v = t) . \tag{2}$$

It is easy to check that $FRR = \frac{1}{n}\sum_{u\in\mathcal{U}} FRR_u$.

### 2.2 The false acceptance rate

The false acceptance rate ($FAR$) is the probability that an offer of a user with a wrong identity claim will be incorrectly accepted, namely $FAR$ is defined by

$$\begin{aligned} &FAR \\ &= \operatorname*{Ave}_{\substack{(u,v)\in\mathcal{U}\times\mathcal{U}\\ u\neq v}} P(\,match(u,v) = accept\,) \\ &= \frac{1}{n(n-1)} \sum_{\substack{(u,v)\in\mathcal{U}\times\mathcal{U}\\ u\neq v}} \sum_{\substack{(s,t)\in\mathcal{M}\times\mathcal{M}\\ d(s,t)<\tau}} P(X_u = s)P(X_v = t)\ . \end{aligned} \tag{3}$$

The measure $FAR$ is traditionally used to express a recognition accuracy of biometric systems. It is also used as a measure to evaluate the security of systems against the zero-effort impersonation attack.
The zero-effort approach assumes that an attacker attempting to impersonate a genuine user will present his/her own biometric data. This assumption is clearly so far from reality, since an attacker will try to present a sample which can be accepted by the system with as high as possible probability. Une, Otsuka, Imai [9], [10] proposed a new security measure, the wolf attack probability ($WAP$), against such stronger intentional impersonation attacks in biometric authentication systems, which is introduced in the following subsection.

### 2.3 The wolf attack probability

If an attacker can find an input value which matches many templates, then he succeed in impersonating a genuine user with a higher probability than $FAR$ by presenting the input value to the biometric authentication system. Such an input value obtained from a biometric sample is called a **wolf** by many authors (cf. [5]). However, such an input value might be obtained not only from biometric samples but also from non-biometric samples. Matsumoto et al. show by experimentation that some artefacts can be falsely accepted in some biometric authentication systems [7].
Considering these facts, we will extend the definition of a wolf as follows.
Let $\mathcal{A}$ be a set of all possible samples including non-biometric samples such as artefacts or synthetic samples. For each $w \in \mathcal{A}$, let $FAR_w$ denote the probability that the sample $w$ with a wrong identity claim $v \neq w$ will be incorrectly accepted and let $AR_w$ denote the probability that the sample $w$ with an identity chosen uniformly at random will be accepted. Namely, $FAR_w$ and $AR_w$ are respectively defined by

$$\begin{aligned} &FAR_w \\ &= \operatorname*{Ave}_{v\in\mathcal{U}\setminus\{w\}} P(match(w,v) = accept) \\ &= \frac{1}{\#\,(\mathcal{U}\setminus\{w\})} \sum_{v\in\mathcal{U}\setminus\{w\}} \sum_{\substack{(s,t)\in\mathcal{M}\times\mathcal{M}\\ d(s,t)<\tau}} P(X_w = s)P(X_v = t)\,, \end{aligned} \tag{4}$$

$$\begin{aligned} &AR_w \\ &= \operatorname*{Ave}_{v\in\mathcal{U}} P(match(w,v) = accept) \\ &= \frac{1}{n} \sum_{v\in\mathcal{U}} \sum_{\substack{(s,t)\in\mathcal{M}\times\mathcal{M}\\ d(s,t)<\tau}} P(X_w = s)P(X_v = t)\ . \end{aligned} \tag{5}$$

It is easy to check that $FAR = \frac{1}{n}\sum_{u\in\mathcal{U}} FAR_u$. The following lemma describes the relation between $AR_w$, $FAR_w$ and $FRR_w$.

**Lemma 1.**

$$AR_w = \begin{cases} FAR_w & \text{if } w \in \mathcal{A}\setminus\mathcal{U} \\ \frac{1}{n}(1 - FRR_w) + \left(1 - \frac{1}{n}\right) FAR_w & \text{if } w \in \mathcal{U}\ . \end{cases} \tag{6}$$

*Therefore it immediately follows that*

$$\frac{1}{n}\sum_{u\in\mathcal{U}} AR_u = \frac{1}{n}(1 - FRR) + \left(1 - \frac{1}{n}\right) FAR\ . \tag{7}$$

*Proof.* We omit the proof since the results directly follows from the definitions (2), (4) and (5) of $FRR_w$, $FAR_w$ and $AR_w$, respectively. □

Put

$$AR = \frac{1}{n}\sum_{u\in\mathcal{U}} AR_u = \frac{1}{n}(1 - FRR) + \left(1 - \frac{1}{n}\right) FAR\ . \tag{8}$$

**Definition 2.** (cf. [9, Definition 3]) *A* **wolf** *is defined as a sample $w \in \mathcal{A}$ such that $AR_w > AR$.*

For any $AR < p \leq 1$, a wolf $w$ such that $AR_w = p$ is called a $p$-**wolf**. In particular, 1-wolf is called a **universal wolf**.

**Definition 3.** [9, Definition 4] *Assume the following two conditions.*

(i) *The attacker has no information of a biometric sample of a genuine user to be impersonated. Nemely we assume that, in the verification phase, the attacker chooses an identity uniformly at random.*

(ii) *The attacker has complete information of the algorithms employed in the enrollment phase and the verification phase.*

*The* **wolf attack** *is defined as an attempt to impersonate a genuine user by presenting p-wolves with large p's to minimize the complexity of the impersonation attack.*

Under the assumption of the wolf attack, $AR_w$ can be regarded as the success probability of the attacker who attempts to impersonate a random user by using the sample $w$.

**Definition 4** (Wolf attack probability ($WAP$))**.** (cf.[9, Definition 5]) *The* **Wolf attack probability** *is defined by*

$$WAP = \max_{w\in\mathcal{A}} \operatorname*{Ave}_{v\in\mathcal{U}} P(\, match(w,v) = accept\,) \qquad (9)$$
$$= \max_{w\in\mathcal{A}} AR_w \ .$$

**Definition 5** (Security against the wolf attack)**.** *For any $\delta > 0$, a biometric authentication system is $\delta$-secure against the wolf attack if $WAP \leq \delta$, namely there exists no wolf $w \in \mathcal{A}$ such that $AR_w > \delta$.*

The following lemma states that in the $\delta$-secure system, $FAR$ has an upper bound almost same as $\delta$ for a large enough $n$.

**Lemma 6.** *A $\delta$-secure system satisfies*

$$FAR_w \leq \begin{cases} \delta & \text{if } w \in \mathcal{A}\backslash\mathcal{U} \\ \dfrac{n}{n-1}\delta & \text{if } w \in \mathcal{U} \end{cases} \qquad (10)$$

*for any $w \in \mathcal{A}$. Therefore it immediately follows that a $\delta$-secure system satisfies*

$$FAR \leq \frac{n}{n-1}\delta \ .$$

*Proof.* We omit the proof since it immediately follows form Lemma 1. □

Since there exists a sample $u \in \mathcal{U}$ such that $AR \leq AR_u$, it follows that

$$WAP \geq AR \ . \qquad (11)$$

**Lemma 7.** *The following three conditions are equivalent.*

(i) $WAP = AR$

(ii) *If there exists no wolf in a biometric authentication system, namely $AR_w \leq AR$ for all $w \in \mathcal{A}$.*

(iii) $AR_u = AR$ *for all $u \in \mathcal{U}$ and $AR_w \leq AR$ for all $w \in \mathcal{A}\backslash\mathcal{U}$.*

*Proof.* (i) ⇒ (ii) is trivial from the definitions of a wolf and $WAP$.
In order to show (ii) ⇒ (iii), we will prove the contraposition. If there exists a sample $u \in \mathcal{U}$ such that $AR_u \neq AR$, then there exists a sample $u' \in \mathcal{U}$ such that $AR_u > AR$ since $AR$ is the average of the $AR_u$, $u \in \mathcal{U}$. Then $u'$ is a wolf. Moreover if there exists a sample $w \in \mathcal{A}\backslash\mathcal{U}$ such that $AR_w > AR$ for all $u \in A$. If there exists a human sample $u \in \mathcal{U}$ such that $AR_u < AR$, then $w$ is a wolf. Therefore the contraposition of (ii) ⇒ (iii) is true.
(iii) ⇒ (ii) is clear from the definitions of $AR$ and $WAP$. □

If a biometric authentication system satisfies the above equivalent conditions, then it is said to be **optimal** against the wolf attack. Note that an optimal system is $AR$-secure.
The following lemma indicates that if an optimal ($AR$-secure) system satisfies $FRR = FAR$ and $AR$ is small enough, then the system are accurate and secure for a large enough $n$.

**Lemma 8.** *For any optimal system satisfying $FRR = FAR$, we have*

$$FRR = FAR = \frac{n}{n-2}\, AR - \frac{1}{n-2}$$
$$= \frac{n}{n-2}\, WAP - \frac{1}{n-2} \ .$$

*In particular, for a large enough $n$, we have*

$$FRR = FAR \approx AR = WAP \ .$$

*Proof.* From the optimality, $FRR = FAR$ and (7), we have

$$WAP = AR = \frac{1}{n}(1 - FRR) + \left(1 - \frac{1}{n}\right) FAR$$
$$= \frac{1}{n} + \left(1 - \frac{2}{n}\right) FRR$$

Therefore the result immediately follows. □

## 3 Matching algorithms secure against the wolf attack

For any $s \in \mathcal{M}$ and $x \in \mathbb{R}_{\geq 0}$, if a sample presented by a attacker is transformed into $s$ and the matching algorithm employs $x$ as the threshold, then the probability $P_s(x)$ that the attacker will be accepted is estimated as follows:

$$P_s(x) = \frac{1}{n} \sum_{v\in\mathcal{U}} \sum_{\substack{t\in\mathcal{M} \\ d(s,t)<x}} P(X_v = t) \quad . \qquad (12)$$

If the matching algorithm employs a fixed threshold $\tau$, then we have

$$AR_w = \sum_{s\in\mathcal{M}} P(X_w = s) P_s(\tau) \quad .$$

However a matching algorithm employing a fixed threshold is not always secure. Une, Otsuka, Imai [9], [10] showed that for some modalities employing fixed thresholds, there exist wolves which make $WAP$ extremely higher than $FAR$.
Our matching algorithms proposed in the following subsections determines an "optimal" threshold for each input value $s \in \mathcal{M}$. We will discuss two cases. First, we will define a secure matching algorithm in the general case. For each input value $s \in \mathcal{M}$, the algorithm determines a threshold $\tau_s$ by using the distributions of the $P(X_u = t)$, $u \in \mathcal{U}$, $t \in \mathcal{M}$, and exhaustively searching (the maximum of) the values $x$ such that $P_s(x) < \delta$. Then we prove that the matching algorithm is $\delta$-secure against the wolf attack (Theorem 9). Secondly, we assume that the distributions $P_s(x)$ are normal. We will propose a simpler method for determining a threshold. Then we prove that the matching algorithm is optimal (Theorem 10).

### 3.1 General case

Fix $\delta > 0$. Then we will construct a matching algorithm $\delta$-secure against the wolf attack as follows.
Almost every conventional matching algorithm employs a fixed threshold $\tau$ predetermined based on *FRR* and *FAR*. However, we will employ a threshold $\tau_s$ determined for each element $s \in \mathcal{M}$ obtained from the sample $w \in \mathcal{A}$ offered in the verification phase. For each $s \in \mathcal{M}$, put

$$\tau_s = \max\{x \in \mathbb{R}_{\geq 0} \,|\, P_s(x) < \delta\} \ .$$

Note that a set $S = \{x \in \mathbb{R}_{\geq 0} \,|\, P_s(x) < \delta\}$ is a non-empty closed subset of $\mathbb{R}_{\geq 0}$ and therefore there exists the maximum of $S$.
For the implementation, we need to gather enough templates from each $v \in \mathcal{U}$ and estimate the probabilities $P(X_v = t)$ for all $t \in \mathcal{M}$. Then we can determine the threshold $\tau_s$ for each $s \in \mathcal{M}$ by doing the exhaustive search of all possible $x \geq 0$ such that $P_s(x) < \delta$.
It is clear that

$$WAP = \max_{w \in \mathcal{A}} \sum_{s \in \mathcal{M}} P(X_w = s) P_s(\tau_s) < \delta \quad . \tag{13}$$

The above discussion gives the following theorem.

**Theorem 9.** *If the information about the probability distribution $P_s(x)$ for each $s \in \mathcal{M}$ is completely given, then, for any $\delta > 0$, we can construct a matching algorithm $\delta$-secure against the wolf attack.*

*Proof.* It is clear form (13). □

### 3.2 Normal distribution case

We assume that the distribution $P_s(x)$ is normal with mean $m_s$ and standard deviation $\sigma_s$ for each $s \in \mathcal{M}$, namely

$$P_s(x) = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}\sigma_s} \exp\left(-\frac{1}{2}\left(\frac{x - m_s}{\sigma_s}\right)^2\right) dx \tag{14}$$

for any $x > 0$. More strictly, we assume that $P_s(x)$ can be approximately estimated by the above equation. The distributions of Hamming distances for Daugman's iriscode satisfy this assumption (cf. [2], [3]). Some authors use the Gaussian assumption as the basis of their analysis (cf. [1], [6], [11]). In general, the real-valued features will tend to approximate a Gaussian distribution when they are obtained by a linear combinations of many components, e.g. feature extraction techniques based on the principle component analysis (PCA) or the linear discriminant analysis (LDA) (cf. [1]). Under this assumption, we can construct a secure and simple matching algorithm and show that the matching algorithm is optimal, namely *WAP* is minimized to the (almost) same value as *AR*.
Define the entropy $H(P)$ of the probability distribution $P$ by

$$H(P) = -\int_{-\infty}^{\infty} P(x) \log_2 P(x) \, dx \ .$$

By the assumption (14), it can be easily checked that $H(P_s) = \log_2\left(\sqrt{2\pi e} \cdot \sigma_s\right)$. Note that the entropy $H(P)$ of continuous probability distributions $P$ is not always non-negative, namely if $\sigma_s < \dfrac{1}{\sqrt{2\pi e}}$, then $H(P_s) < 0$.
If a fixed threshold is employed, then an input value $s \in \mathcal{M}$ which has higher entropy $H(P_s)$ and therefore larger deviation $\sigma_s$ can be accepted with higher probability.
Fix a real number $\alpha$. For each $s \in \mathcal{M}$, put

$$\tau_s = \alpha\sigma_s + m_s = \frac{\alpha 2^{H_s}}{\sqrt{2\pi e}} + m_s \tag{15}$$

where $H_s = H(P_s)$. By the assumption (14), we have

$$\begin{aligned} P_s(\tau_s) &= \int_{-\infty}^{\tau_s} \frac{1}{\sqrt{2\pi}\sigma_s} \exp\left(-\frac{1}{2}\left(\frac{x - m_s}{\sigma_s}\right)^2\right) dx \\ &= \int_{-\infty}^{\alpha} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{z^2}{2}\right) dz \end{aligned} \tag{16}$$

for all $s \in \mathcal{M}$. Put

$$\delta(\alpha) = \int_{-\infty}^{\alpha} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{z^2}{2}\right) dz \quad .$$

The following theorem can be immediately proved.

**Theorem 10.** *Assume that the standard deviation $\sigma_s$ (or the entropy $H_s$) and the mean $m_s$ are perfectly given for each $s \in \mathcal{M}$. Then the matching algorithm employing the thresholds $\tau_s$, $s \in \mathcal{M}$, defined by* (15) *is $\delta(\alpha)$-secure against the wolf attack. Moreover, we have $AR_w = AR = WAP = \delta(\alpha)$ for all $w \in \mathcal{A}$ and therefore this algorithm is optimal.*

*Proof.* By the calculation (16), for all $w \in \mathcal{A}$, we have

$$AR_w = \sum_{s \in \mathcal{M}} P(X_w = s) P_s(\tau_s) = \delta(\alpha) \ .$$

Therefore the results follow. □

To increase $\alpha$ makes *FRR* and *FAR* lower and higher, respectively. Therefore there is still a trade-off between *FRR* and *FAR* in this matching algorithm. If we chose a suitable $\alpha$ such that $FRR = FAR$, then, by Lemma 6, 7, 8, the proposed matching algorithm can be accurate and secure.
The purpose of our matching algorithm is to prevent the attacker from impersonating a genuine user by presenting an input value $s \in \mathcal{M}$ which shows high similality to most templates. Even a genuine user can be unfortunately rejected if he/she presents such a suspicious input value. However, a false rejection of such a badly behaved sample inevitably arises in a matching algorithm secure against the wolf attack. It is rather a critical security hole that a conventioal matching algorithm perhaps accepts such a badly behaved input value even though it is presented by an attacker.

## 4 A new framework for the matching algorithms

Our generalized matching algorithm gives a theoretical framework for constructing secure matching algorithms against the wolf attack for any biometric authentication system. Under the ideal condition that for each $s \in \mathcal{M}$, the distribution $P_s(x)$ is completely calculated, our matching algorithm is optimal against the wolf attack.
In the real world, it might be difficult to explicitly calculate the distribution $P_s(x)$ for all $s \in \mathcal{M}$, however, a more accurate computation of $\sigma_s$, $H_s$, or $m_s$ for each $s \in \mathcal{M}$ can achieve a lower $WAP$. Consequently, there is a trade-off between the efficiency of the matching algorithm and the security evaluated by the achievable $WAP$. In the next section, we will reconsider previous results as instances of our theoretical framework.

### 4.1 Review of previous results in our framework

In this section, we will review previous results in the context of our theoretical framework.
A conventional matching algorithm employing a fixed threshold can be viewed as an efficient instance of our framework, which assumes every input value has a constant entropy instead of computing the entropy for each input value. Such a matching algorithm is not secure against the wolf attack.
Daugman [3] proposes a matching algorithm which employs a variable threshold in place of a fixed threshold as follows. He employs a fractional Hamming distance $d = fHD$ defined by $fHD(s,t) = \dfrac{HD(s,t)}{k}$ for any $s, t \in \mathcal{M} = \{0, 1, null\}^{2048}$, where the bits obscured by eyelids, contains any eyelash occlusions, specular reflections, boundary artifacts of hard contact lenses, or poor signal-to-noise ratio are ignored in the calculation of $H(s,t)$ and then $k$ is the number of valid bits. He determines a threshold depending on $k$ as follows:

$$\tau(s,t) = \frac{\alpha'}{\sqrt{k}} + \frac{1}{2} \tag{17}$$

where $\dfrac{1}{2}$ is the average of $fHD(s,t)$ estimated from his database. His algorithm can also be regarded as an instance of our framework, which assumes every bit of each sample independently and identically contributes to the probability distribution.
However, his algorithm is not necessarily secure against the wolf attack, since every bit is not exactly independent and identical and the distributions $P_s(x)$, $s \in \mathcal{M}$, can be considerably different from each other. We assume that an attacker has more accurate information about the distributions $P_s(x)$, $s \in \mathcal{M}$. If the attacker can successfully find a smart input value $s \in \mathcal{M}$ such that the entropy $H(P_s(x))$ is extremely high, then he can be accepted with much higher probability than $AR$. Daugman's matching algorithm is not always secure against the wolf attack, however, it motivated us to research a theoretical framework to construct secure matching algorithms.

## References


[1] Andy Adler, Richard Youmaran, Sergey Loyka, "Towards a measure of biometric feature information," Pattern Analysis and Applications, Springer London, (Online First), DOI 10.1007/s10044-008-0120-3

[2] J. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statstical Independence ," IEEE Trans. on Pattern Anal. Mach. Intell., vol. 15, no. 11, Nov. 1993

[3] J. Daugman, "Probing the uniqueness and randomness of IrisCodes: Results from 200 billion iris pair comparisons, " Proceedings of the IEEE, vol. 94, no. 11, pp. 1927-1935, 2006

[4] M. Inuma, A. Otsuka, H. Imai, "Theoretical framework for constructing matching algorithms in biometric authentication systems, " in submission to ICB 2009

[5] International Organization for Standardization (ISO), International Electronical Commission (ICE): ISO/IEC CD 19792: Imformation technology - Security techniques - Security evaluations of biometrics, 2006

[6] T. Kevenaar, "Protection of Biometric Information," P. Tuyls, B. Skoric, and T. Kevenaar, eds., Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting, chapter 7, pp. 113-125. Springer London, 2007.

[7] T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, "Impact of Artificial 'Gummy' Fingers on Fingerprinting Systems," Opt. Sec. and Count. Det. Tech. IV, Proc. of SPIE 4677, pp. 275-289, 2002

[8] N. K. Ratha, J. H. Connell, R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Syst. J. 40, pp. 614-634, 2001

[9] M. Une, A. Otsuka, H. Imai, "Wolf Attack Probability: A New Security Measure in Biometric Authentication Systems," Advances in Biometrics, LNCS, vol. 4642, Springer-Verlag Berlin Heidelberg, pp. 396-406, 2007

[10] M. Une, A. Otsuka, H. Imai, "Wolf Attack Probability: A Theoretical Security Measure in Biometrics-Based Authentication Systems," IEICE, Transactions on Information and Systems 2008, E91-D(5): pp. 1380-1389

[11] Wayman, J.S., "The cotton ball problem," Biometrics Conference, Washington DC, USA, Sep. 20-22, 2004.