Image and Vision Computing xxx (2014) xxx–xxx

Contents lists available at ScienceDirect

Image and Vision Computing

journal homepage: www.elsevier.com/locate/imavis

A measure of information gained through biometric systems[☆,☆☆]

Kenta Takahashi [a,*], Takao Murakami [a,b]

[a] Yokohama Research Laboratory, Hitachi, Ltd., Yokohama 244-0817, Japan
[b] Institute of Industrial Science, The University of Tokyo, Tokyo 153-8505, Japan

ARTICLE INFO

Article history:
Received 27 April 2013
Received in revised form 2 November 2013
Accepted 13 December 2013
Available online xxxx

Keywords:
Biometrics
Entropy
Mutual information
Relative entropy
Divergence

ABSTRACT

We propose a measure of information gained through biometric matching systems. Firstly, we discuss how the information about the identity of a person is derived from biometric samples through a biometric system, and define the "biometric system entropy" or BSE based on mutual information. We present several theoretical properties and interpretations of the BSE, and show how to design a biometric system which maximizes the BSE. Then we prove that the BSE can be approximated asymptotically by the relative entropy $D(f_G(x)\|f_I(x))$ where $f_G(x)$ and $f_I(x)$ are probability mass functions of matching scores between samples from individuals and among population. We also discuss how to evaluate the BSE of a biometric system and show experimental evaluation of the BSE of face, fingerprint and multimodal biometric systems.

1. Introduction

Biometric identification systems, which automatically identify a person based on his/her physical or behavioral features, are widely used for various applications. To be used for personal identification, the biometric features are desired to satisfy the following requirements.

1. Uniqueness: Biometric feature has to be unique to each individual.
2. Stability: Biometric feature has to be unchangeable for each capture.

However most biometrics do not strictly satisfy these requirements, because of the following reasons. Even if feature data are extracted from the same body part of a person, they vary with each capture due to aging, position errors, distortion, measurement errors, environmental noise, and many other factors. These factors make it hard to satisfy the *stability*. Thus, it is general to consider that two features match when they are similar enough to each other, even if not exactly the same. However this fuzziness causes false matches of features extracted from different bodies; the requirement of *uniqueness* is also hardly to be satisfied.

Since these requirements are hard to be satisfied strictly for most biometric modalities (e.g., fingerprints, faces, vein patterns, irises, and so on), biometric systems inevitably make errors in identifying persons. Therefore it is important to evaluate the identification performance of biometric systems quantitatively.

Two kinds of error rates are widely used to evaluate the performance: false match rate (FMR) and false non-match rate (FNMR). FMR is a probability that two feature data extracted from different bodies match, and FNMR is a probability that two feature data from the same person do not match. There is a trade-off between these error rates depending on a threshold parameter t, which is described by a 2-D curve parametrized by $(\mathrm{FRT}(t), 1-\mathrm{FNMRT}(t))$, called ROC (receiver operating characteristic) curve [2]. Though the ROC curve describes the identification performance precisely, it is not straightforward to understand the ROC curve intuitively or to compare some biometrics with other method such as PIN code by using the ROC curve.

On the other hand, there has been some efforts to define and evaluate the individuality of biometrics from the viewpoint of information content or entropy [3–5]. Entropy as a measure of identification performance has the potential to make it possible to compare a certain biometrics (e.g. fingerprints) not only with another biometrics (e.g. irises) but also with PIN, passwords, and many other authentication methods. It has also the potential to enable us to quantify the degree of privacy of biometrics and compare it with other personal identification information such as name, address, birthday, etc. However, no common measure or methodology to evaluate the biometric entropy have been established so far which could be practically applicable to any kind of biometrics.

In this paper, we propose a measure of personally identifying information gained through biometric matching systems, and discuss a methodology of evaluation applicable to any kind of biometrics.

This paper is an extension of a previously published conference paper [1]. The main enhancements are as follows:

1. We discuss the relation between the BSE and the password entropy [6,7] and clarify that both are special cases of a measure of personal identification information defined based on mutual information

[☆] This paper has been recommended for acceptance by Lei Zhang.
[☆☆] A preliminary version of this paper was presented at the 20th IAPR International Conference on Pattern Recognition (ICPR2010), Istanbul, Turkey, August, 2010 [1].
[*] Corresponding author.
E-mail addresses: kenta.takahashi.bw@hitachi.com (K. Takahashi), takao.murakami.nr@hitachi.com (T. Murakami).

0262-8856/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.imavis.2013.12.010

(Section 3). This clarifies the fact that the BSE can make it possible to compare biometrics with other personal identification information such as names, addresses and PINs.

2. In [1], we showed some information theoretical and statistical properties of the relative entropy $D(f_G \| f_I)$ between a genuine score distribution f_G and an impostor score distribution f_I, which is the asymptotic approximation of the BSE. In this paper, we present stronger results: we directly show the properties of the mutual information $I(U;\boldsymbol{X})$ between the user identity U and the set of scores $\boldsymbol{X}$, which is the original definition of the BSE, instead of the approximated version (Section 4). These properties clarify the information theoretical and statistical meaning of the BSE more directly.
3. We show a relation between the BSE and the lower bound of the identification error probability or the Bayes error. The relation indicates that a biometric matching system with larger BSE has potential to achieve lower identification error (Section 4.4).
4. We prove an interesting fact that the maximum of the BSE with respect to a biometric matching system is equal to the Adler's biometric information (BI) of a system [4]. Furthermore we show how to design a biometric matching system so that the BSE achieves the BI of a system (i.e. the maximum value) (Section 5).
5. In [1], we showed that the BSE is asymptotically approximated by $D(f_G \| f_I)$. In this paper, we additionally proved that $D(f_G \| f_I)$ also gives a minimum upper bound of the BSE for a fixed system S (Section 6.2). This would help us to understand the meaning of $D(f_G \| f_I)$ as an approximation of the BSE.
6. We introduce a method of directly estimating the approximated BSE $D(f_G \| f_I)$ without estimating f_G and f_I using the generalized k-NN estimator [8], and use it in our experiments (Sections 7.1(2), 7.2).
7. We experimentally evaluate $D(f_G \| f_I)$ of multimodal biometric systems, in addition to the fingerprint matching system and the face matching system. The results support the property of the BSE of the multimodal biometric system: it is less than or equal to the sum of the BSEs of the subsystems, and depends on the fusion function (Section 7.2).

The rest of this paper is organized as follows. Section 2 is a brief review of the previous works. In Section 3, we propose a new measure of information gained through biometric systems: "biometric system entropy" or BSE. Theoretical properties and interpretations of the BSE are discussed in Section 4. In Section 5, we derive an asymptotic approximation and minimum upper bound of the BSE. In Section 6, we show how to evaluate $D(f_G \| f_I)$ of a biometric system and show experimental evaluation of the BSE of face, fingerprint and multimodal biometric systems. Section 7, we summarize our results and conclusions.

2. Related work

One of the works to evaluate the biometric entropy is Daugman's approach to estimate the entropy of human irises [3]. He investigated a statistical distribution of Hamming distances between different irises, and approximated it using a binomial distribution

$$f(m) = \frac{N!}{m!(N-m)} p^m (1-p)^{N-m}, \quad (p = 0.5). \tag{1}$$

He called the parameter N *discrimination entropy*, and estimated $N = 249$.

Hidano et al. [5] generalized the Daugman's discrimination entropy to the *minimum distance entropy* (*MDE*) based on the Rényi entropy [9] (or collision entropy). The MDE can be applied to any kind of biometric feature and statistical model of distance distributions.

Both the discrimination entropy and the MDE can be expressed as $-\log_2 P$, where P is the probability that two features from different bodies match exactly. If the probability distribution of a feature is uniform, then $P = 1 / M$ where M is the number of distinguishable features, and MDE $= \log_2 M$. In this meaning, they can be regarded as an index of uniqueness of biometric features.

However, the probability of exact match would largely depend on representation parameters of features such as length of iris codes [3] and resolution (or discretization width) of fingerprint minutiae coordinates $(x, y) \in \mathbb{R}^2$ [10]. Such representation parameters would not be essential elements of the individuality of biometrics unless, for example, the resolution is too low. Furthermore, as mentioned above, two biometric features (e.g., iris codes) rarely match exactly even if they are obtained from the same body. Namely, the discrimination entropy and the MDE do not reflect the deviation among features from the same body.

Adler et al. defined the "biometric information (BI) of a person" as *the decrease in uncertainty about the identity of the person due to a set of biometric measurements*, and proposed to use the following *relative entropy* (or *Kullback–Leibler divergence*) [11] as a measure of the BI [4].

$$D(q_i \| q_{all}) = \begin{cases} \displaystyle\int q_i(\boldsymbol{b}) \log \frac{q_i(\boldsymbol{b})}{q_{all}(\boldsymbol{b})} d\boldsymbol{b} & (continuous) \\ \displaystyle\sum q_i(\boldsymbol{b}) \log \frac{q_i(\boldsymbol{b})}{q_{all}(\boldsymbol{b})} & (discrete) \end{cases} \tag{2}$$

where $q_i(\boldsymbol{b})$ is a distribution of biometric features $\boldsymbol{b} \in \mathcal{B}$ ($\mathcal{B}$: feature space) from a person whose identity is i (intra-class feature distribution), and $q_{all}(\boldsymbol{b})$ is one from the population (inter-class feature distribution). Since $D(q_i \| q_{all})$ varies from person to person, they also defined the "BI of a system" as *the mean* $D(q_i \| q_{all})$ *for all persons in the population*.

To evaluate the BI, the relative entropy $D(q_i \| q_{all})$ has to be estimated from a finite number of biometric samples. In general, however, the feature space $\mathcal{B}$ is high dimensional, requiring an exponentially large number of samples to estimate $q_i(\boldsymbol{b})$, $q_{all}(\boldsymbol{b})$ and $D(q_i \| q_{all})$, as well known as the *curse of dimensionality* [12]. This problem is serious especially when collecting the samples from the individual feature distribution $q_i(\boldsymbol{b})$, because in practice, only a limited number of samples of each individual are available. To address this issue, Adler et al. assumed that $\mathcal{B}$ is an n-dimensional Euclidean space, and $q_i(\boldsymbol{b})$,$q_{all}(\boldsymbol{b})$ can be modeled as Gaussian distributions of a limited form (with almost diagonal covariance matrix). In practical cases, however, $q_i(\boldsymbol{b})$, $q_{all}(\boldsymbol{b})$ cannot always be approximated by such a simple model. And further, the structure of $\mathcal{B}$ is often more complicated (e.g. the feature space of the minutiae representation of fingerprints does not have a fixed dimension because the number of minutiae varies from finger to finger) or even unknown (e.g. when the evaluation is performed by a third party).

Bhatnagar et al. [13] considered a biometric verification system as additive white Gaussian noise channels (AWGN), where the genuine and impostor matching scores follow Gaussian distributions $N(\mu_G,\sigma_G^2)$ and $N(\mu_I,\sigma_I^2)$, respectively. As a measure of performance of the system, they defined *constrained capacity* C as follows:

$$C = \frac{1}{2} \log_2 \left\{ 1 + \frac{(\mu_G - \mu_I)^2}{4 \max(\sigma_G^2, \sigma_I^2)} \right\}. \tag{3}$$

However, the AWGN models of matching scores are rather strong assumptions; in general, they do not follow such simple models.

3. A new measure of information gained through biometric systems

The purpose of this section is to provide a new measure of information gained through biometric systems, which can be applied practically to any kind of biometrics, even if the feature distributions or the structure of the feature space is unknown. Firstly, we discuss and define a measure of personally identifying information such as names, addresses, PINs and passwords. Next, we introduce a *black box model* of biometric systems and discuss how information about the identity of a person is derived through the biometric system, and define a new measure named biometric system entropy (BSE).

Please cite this article as: K. Takahashi, T. Murakami, A measure of information gained through biometric systems, Image Vis. Comput. (2014), http://dx.doi.org/10.1016/j.imavis.2013.12.010