社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＣＳＥＣ－38 (28)
2007／7／19

生体情報の情報量に関する一考察

髙橋 健太† 日野 英逸† 村上 隆夫†

† (株) 日立製作所 システム開発研究所，川崎市麻生区王禅寺 1099
E-mail: †kenta.takahashi.bw@hitachi.com

あらまし 指紋や静脈，虹彩などを用いた生体認証技術の普及が進んでいる．本稿では，個人識別情報として生体情報が持つ情報量について考察し，その評価指標を提案する．まず生体情報の情報量を相互情報量として定義し，その漸近的な近似として，本人同士の照合スコア分布 $f_G(x)$ と他人同士の照合スコア分布 $f_I(x)$ の Kullback-Leibler 情報量 $D(f_G \parallel f_I)$ が導かれることを示す．そこで $D(f_G \parallel f_I)$ を生体情報の情報量評価指標とすることを提案する．また従来の精度評価指標である ROC カーブとの関係や，マルチモーダルバイオメトリクスにおける情報量，プライバシー保護型生体認証技術におけるプライバシー保護性能の評価指標としての適用可能性などについて考察する．最後に，提案する指標に基づく具体的な評価手順を述べる．

キーワード 生体認証，バイオメトリクス，情報量，マルチモーダルバイオメトリクス，プライバシー保護型生体認証

Kenta TAKAHASHI†, Hideitsu HINO†, and Takao MURAKAMI†

† Hitachi, Ltd., Systems Development Laboratory, 1099, Ohzenji, Asao-ku, Kawasaki-shi, Kanagawa, 215-0013 Japan
E-mail: †kenta.takahashi.bw@hitachi.com

Abstract Due to the high security and convenience, biometric authentication is used at access control, ATM and many kinds of identity verification. In this paper, we consider the information amount of a biometric feature such as a fingerprint or a vein pattern in the sense of personal-identifying information. Firstly, we define the amount of personal-identifying information contained in a biometric feature by mutual information. Then we show that the mutual information can be approximated asymptotically by Kullback-Leibler divergence between the genuine score distribution $f_G(x)$ and the imposter score distribution $f_I(x)$. We propose to use this KL divergence as a metrics of biometric information in a certain biometric identification system. It is also discussed about the relationship between the metrics and ROC curve, information of multimodal biometrics, and possible application of the metrics to privacy protecting biometric technologies. Finally some methods for experimental estimation of biometric information based on the metrics are described.

Key words biometrics, information, metrics, multi-modal biometrics, privacy protecting biometrics

1. はじめに

指紋や顔，静脈，虹彩などの生体の測定データ (生体情報) に基づいて個人を識別する生体認証技術の普及が進んでいる．生体認証に用いる生体情報は，一生変化せずいつ測定しても一定であること（終生不変），異なる人間 (生体) の生体情報は必ず区別できること（万人不同）が望ましいとされる．しかし終生不変の性質を厳密に満たすことは困難であり，経時変化や測定誤差，ノイズなどの影響により，一般には同じ生体であっても測定の度に少しずつ異なる生体情報が取得される．このため二つの生体情報を照合する際，完全に一致していなくても「距離」がある程度近ければ一致（同一人物）と見なすが，そのために異なる人間の生体情報が一致と判定される場合があり，万人不同性を厳密には満たすことも困難である．そこで，生体認証技術の個人識別能力を定量的に評価，比較することが重要となる．

個人識別能力の評価指標として最も広く使われるものは，本人 (同一生体)/他人 (異なる生体) の判定に関する誤り確率 (精度) である．判定誤りには 2 種類あり，本人の生体情報を不一致と判定してしまう誤り確率を FRR(False Rejection Rate)，他人の生体情報を一致と判定してしまう誤り確率を FAR(False Acceptance Rate) と呼ぶ．これらの誤り確率は生体情報間の距離に対する一致／不一致の判定しきい値 t に依存して変化するため，$(FAR(t), FRR(t))$ を平面上の点としてプロットし，t を変化させたときの点の軌跡 (ROC カーブ) を用いて精度を表

現する方法が標準化されている [1]. ROC カーブは生体認証技術の精度を詳細に記述することができるが，その解釈は容易でなく，例えば互いに ROC カーブが交わる持つ 2 つの認証技術について，どちらが高い識別能力を持つか，といった端的な比較は困難である．

一方，生体情報が持つ情報量に基づいて，生体認証技術の個人識別能力を評価する試みがなされている [2], [6], [7] 情報量として表現することで，生体認証技術同士の比較が容易となるだけでなく，パスワードや暗証番号などとの対比も可能となり，識別能力をより直観的に理解することができる．しかし生体情報が持つ情報量の定義に関して現在のところコンセンサスはなく，任意の生体認証技術に対して統一的かつ容易に適用可能な評価方法も確立していない．

本稿では，生体情報の測定によって得られる個人識別情報の量を相互情報量を用いて定義し，その漸近的な近似として導かれる照合スコア分布の KL 情報量を，生体情報の情報量評価指標として用いることを提案する．この評価指標は照合スコア分布のみから計算できるため，精度評価と同様の手順により，任意の生体認証技術に対し評価可能である．本稿ではまた，評価指標の性質について述べ，マルチモーダルバイオメトリクスやプライバシー保護型生体認証技術への応用の可能性について考察する．最後に，提案する指標に基づく具体的な評価手順を述べる．

2. 関 連 研 究

生体情報の情報量に基づいて識別能力を評価する試みの一種として，指紋の万人不同性に関する理論的な評価研究が挙げられる [2]．これは，指紋画像に含まれるマニューシャ(特徴点)の集合を特徴量としたとき，二つの異なる指紋の特徴量が一致する確率 (FAR) を理論的に評価することで，指紋の万人不同性の根拠を与えるとともに，指紋認証システムの性能限界を見積もることを目的としている．しかし，2 つのマニューシャがどの程度近ければ一致とみなすのかといった誤差許容量に関するパラメータ設定に依存して評価結果は大きく変動するため，他の認証手段 (例えば虹彩) との比較を目的とした場合，評価指標としての有用性は低い．またこれらの研究では，マニューシャの座標や方向が独立に一様分布に従うといった仮定を置いているが，実際にはこの仮定は成り立たない．例えば隆線の連続性から，ある点をとったときその近傍のマニューシャはほぼ同じ方向を向いている．また指紋の隆線パターンは 5 種類程度に分類できることが知られており [8]，座標と方向は強い相関を持つ．上記文献ではこのような現実の制約をモデルに反映していないため，FAR の理論値は実際の値と比較して極端に小さく評価されている．更に実際の指紋認証システムでは，マニューシャに加えて 2 つのマニューシャ間の隆線数 (リレーション) を用いる方式 [3], [4] や，周波数解析によって指紋画像自体をマッチングする方法 [5] などが実用化されており，上記のような単純なモデル化により識別性能を評価することは困難である．

上記の研究例が生体情報をモデル化して理論的な評価を試みているのに対し，より実験的・実証的な研究例として，Daugman による虹彩情報量の評価が挙げられる [6]．具体的には，虹彩認証システムを用いて多数の異なる虹彩情報同士の照合実験を行い，虹彩情報間の距離 x の分布 (以下，他人分布と呼ぶ) を調べる．これを以下の二項分布で近似したときの N を，虹彩の情報量とする．上記文献ではこれを "Discrimination Entropy" と呼んでいる．

$$f(x) = \frac{N!}{m!(N-m)!} p^m (1-p)^{N-m}, \left(x = \frac{m}{N}, p = 0.5 \right) \tag{1}$$

Daugman は実験結果から $N = 249$ と見積もっている．N は 2 つの虹彩情報が完全に一致する確率 $P = f(0)$ を用いて $N = -\log_2(P)$ と表せ，虹彩情報のエントロピーと解釈することができる．しかし既に述べたように，本人の生体情報同士の照合であっても完全一致 ($x = 0$) となることは稀であり，このため距離がしきい値 t より小さければ一致と見なす．本人の生体情報間の距離分布 (以下，本人分布と呼ぶ) と他人分布が離れていれば，t を適切に設定することで判定誤差 (FAR,FRR) を小さくすることができるため，識別性能は高いと言える．逆に分布間の重なりが大きいと識別性能は低い．Discrimination Entropy N による評価は，このような生体情報の個人内変動を考慮していないため，識別性能の評価指標として適切ではない．

個人内変動を考慮した評価指標として，Adler らは生体情報の特徴量の確率分布 (以下，特徴量分布) に関する Kullback Leibler 情報量 (以下，KL 情報量) を用いることを提案している [7]．具体的には，特定の個人から測定した特徴量分布 $p(\mathbf{X})$ と，全人間の特徴量分布 $q(\mathbf{X})$ との KL 情報量

$$D(p \parallel q) = \begin{cases} \int p(\mathbf{X}) \log_2 \frac{p(\mathbf{X})}{q(\mathbf{X})} d\mathbf{X} & \text{(連続の場合)} \\ \sum_{\mathbf{X}} p(\mathbf{X}) \log_2 \frac{p(\mathbf{X})}{q(\mathbf{X})} & \text{(離散の場合)} \end{cases} \tag{2}$$

を，その個人の生体情報が持つ情報量とし，これを全個人について平均した値をシステムの個人識別性能の評価指標とする．これは，(個人識別性の意味で) 生体情報が持つ情報量として，自然な性質を持つ．例えば $p(\mathbf{X}) = q(\mathbf{X})$ のとき $D(p \parallel q) = 0$ となるが，これは特定個人の特徴量分布が全人間の特徴量分布と一致するとき，生体情報の測定によってその個人であるか否かの情報は全く得られない，と解釈できる．$D(p \parallel q)$ を評価するためには $p(\mathbf{X}), q(\mathbf{X})$ を推定する必要があり，Adler は $\mathbf{X}$ がユークリッド空間上のベクトルとして表現できるとき，$p(\mathbf{X}), q(\mathbf{X})$ を多次元正規分布と仮定して推定することを提案している．しかし安定した分布推定のためには，一般に $\mathbf{X}$ の次元数に対して十分多くのサンプルが必要になる．特に $p(\mathbf{X})$ は特定の個人に関する特徴量分布であるため，その推定に用いるサンプルは一人の人間から測定しなくてはならない．このため $\mathbf{X}$ の 次元が大きい場合 (例えば虹彩特徴量は数千次元)，この方法を用いた評価は現実的でない．また，例えばマニューシャの順序なし集合 (要素数不定) で表現される指紋特徴量のように，$\mathbf{X}$ の構造が複雑な場合，特徴量分布をモデル化すること自体が困難となる．

以上の研究例を表 1 にまとめる．評価レベルの欄は，生体情報の特徴量に基づいて情報量を評価する場合に「特徴量レベ

ル」，照合スコア (生体情報間の距離や類似度) に基づいて評価する場合に「スコアレベル」とした．

表 1　研究例の比較

研究例	Pankanti [2]	Daugman [6]	Adler [7]
評価対象	指紋 (マニューシャ方式)	虹彩	任意 (特徴量分布が推定可能なもの)
評価指標	FAR	Discrimination Entropy	特徴量分布間の KL 情報量
評価方法	理論的	実験的	実験的
評価レベル	特徴量レベル	スコアレベル	特徴量レベル
問題点	モデルが非現実的，評価結果がモデルのパラメータに依存	個人内変動を考慮せず	一般に特徴量分布の推定は困難

3. 生体情報の情報量評価指標の提案

本章では，あるデータが個人識別情報として持つ情報量を定義し，これを元に任意の生体認証技術に対して評価可能な，生体情報の情報量評価指標を導く．また提案する情報量評価指標の性質を述べ，精度評価指標 (ROC カーブ) やマルチモーダル生体認証との関係について議論する．更に，逐次的マルチモーダル生体認証における入力順序の最適化や，プライバシー保護型生体認証技術の性能評価などへの適用可能性について考察する．

3.1 個人識別情報の情報量

ある (識別されていない) 個人 $U \in \mathcal{U} = \{U_1, \cdots, U_N\}$ に関して，あるデータ $X \in \mathcal{X}$ を観測したとき，それをもとに U が $U_1, \cdots, U_N$ の中の誰であるのかを識別することを考える．X が個人識別に関して持つ情報量は，X の観測による U のあいまいさ (エントロピー) の減少量として定義するのが自然である．そこで，U と X の相互情報量

$$I(U;X) = H(U) - H(U|X) = \begin{cases} \sum_U \int_{\mathcal{X}} p(U,X) \log \frac{p(U,X)}{p(U)p(X)} dX & (\text{連続の場合}) \\ \sum_U \sum_X p(U,X) \log \frac{p(U,X)}{p(U)p(X)} dX & (\text{離散の場合}) \end{cases} \quad (3)$$

により，X が持つ個人識別情報としての情報量を定義する．ここで $H(U)$ は X を観測する前の U のエントロピー，$H(U|X)$ は観測後のエントロピー (事後エントロピー) である．また $p(\cdot)$ は確率密度関数を表すものとし，log の底は 2 とする．

例えば $\mathcal{U}$ を日本人の集合，X を住所 (都道府県情報のみ) として，X が U の識別に関して持つ情報量を計算してみる．日本の総人口を N，X 県の人口を N_X とすると，$p(U) = 1/N$, $p(X) = N_X/N$ である．また住所が X である日本人の集合を $\mathcal{U}_X$ とすると，

$$p(U,X) = p(X|U)p(U) = \begin{cases} 1 \cdot 1/N = 1/N & (U \in \mathcal{U}_X) \\ 0 \cdot 1/N = 0 & (otherwise) \end{cases} \quad (4)$$

より，X が持つ情報量は

$$I(U;X) = \sum_X \sum_{U \in \mathcal{U}_X} \frac{1}{N} \log \frac{1/N}{(1/N) \cdot (N_X/N)} = \sum_X \frac{N_X}{N} \log \frac{N}{N_X} = 5.07 \ \text{(bit)},$$

と計算できる．また $\mathcal{U}$ をある銀行のキャッシュカード利用者の集合とし，X を 4 桁の暗証番号とすると，全ての暗証番号 (0000〜9999) の登録頻度が等しいと仮定すれば，暗証番号の情報量は住所の場合と同様に，以下の通り計算できる．

$$I(U;X) = \sum_X \frac{1}{10000} \log 10000 = \log 10000 = 13.3 \ \text{(bit)}.$$

ところで上記の例はいずれも $I(U;X) = H(X)$ となっているが，これは U に対して X が一意に決まるためである．実際このとき，U が観測 (識別) された後の X に関する事後エントロピーは $H(X|U) = 0$ となるため，$I(U;X) = H(X) - H(X|U) = H(X)$ が成立する．しかし X が生体情報のように個人内変動を含む場合，$H(X|U) > 0$ となるため $I(U;X)$ と $H(X)$ は一致しない．なお文献 [9] などではパスワード X の (平均) 強度をエントロピー $H(X)$ で定義しているが，これは上記の理由から，相互情報量 $I(U;X)$ の特殊な場合と考えることができる．

3.2 生体情報の情報量

前節の定義に基づき，生体情報 B の測定によって獲得できる (個人識別情報としての) 情報量の評価指標を，任意の生体認証システムに対して評価可能な形で導出する．各個人の生体情報 B に関する分布 $p(B|U_i)$ $(i = 1, 2, \cdots, N)$ が全て既知ならば，式 (3) に従って $I(U;B)$ を計算可能であるため，これを情報量評価指標とすることができる．しかし一般に B の空間は高次元 (画像なら数万〜数百万次元) であり，主成分分析などの特徴抽出により次元を圧縮したとしても，分布推定のためには各個人から膨大な数の学習サンプルを測定する必要がある．また生体認証システムをブラックボックスとして扱う必要がある場合 (例えば第三者機関に評価を委託する場合など)，B の構造が未知であるため $p(B|U_i)$ をモデル化すること自体不可能である．

ところで未知の個人 $U \in \mathcal{U}$ から指紋や虹彩といった生体情報 B を測定しても，一般的にはそれだけで U を識別することはできず，既知の個人 $U_i \in \mathcal{U}$ と紐付けられた生体情報 T_i (テンプレート) のデータベース $\{T_1, \cdots, T_N\}$ と照合することで，はじめて個人識別が可能となる．そこで，個人識別に利用できる情報は B そのものではなく，B と各テンプレートとの照合スコアの列

$$X = (x_1, \cdots, x_N), \quad (x_i \text{は } B \text{ と } T_i \text{の照合スコア}) \quad (5)$$

であると考え，B の測定によって獲得できる個人識別情報としての情報量 (生体情報の情報量) を，$I(U;X)$ で定義する．

3.3 情報量評価指標の導出

前節で定義した生体情報の情報量 $I(U;X)$ に関して，以下の定理が成立することを証明できる．

定理 U の事前分布が $p(U_i)=1/N$ $(i=1,\cdots,N)$ であるとする．また $x_1,\cdots,x_N$ は独立であり，同一の個人 (生体) の生体情報同士の照合スコアは本人分布 $f_G(x)$ に従い，異なる個人 (生体) 同士の照合スコアは他人分布 $f_I(x)$ に従うとする．このとき，

$$I(U;X)\to D(f_G(x)\parallel f_I(x))\ \ (N\to\infty). \tag{6}$$

(証明) 以下，照合スコア x_i は連続な実数値を取るものとして議論するが，離散値の場合でも同様に証明できる．$p(U_i)=1/N$ より，相互情報量の式 (3) は以下のように書き直せる．

$$\begin{aligned} I(U;X) &= \sum_i \int_{\mathcal{X}} p(X|U_i)p(U_i)\log\frac{p(X|U_i)}{\sum_j p(X|U_j)p(U_j)}dX \\ &= \frac{1}{N}\sum_i \int_{\mathcal{X}} p(X|U_i)\log\frac{p(X|U_i)}{\sum_j p(X|U_j)/N}dX. \end{aligned} \tag{7}$$

積分範囲は $\mathcal{X}=\mathbb{R}^N$ である．x_i は互いに独立なので，$U=U_i$ であったときに照合スコア列 $X=(x_i,\cdots,x_N)$ を観測する確率は

$$p(X|U_i)=\prod_{j=1}^{N} p(x_j|U_i), \tag{8}$$

と分解できる．ここで $p(x_j|U_i)$ は，U_i の生体情報 B とテンプレート T_j の照合スコアが x_j となる確率密度を表す．仮定より

$$p(x_j|U_i)=\begin{cases} f_G(x_j) & (i=j) \\ f_I(x_j) & (i\neq j), \end{cases} \tag{9}$$

なので，式 (8) は以下のように書き直せる．

$$p(X|U_i)=\frac{f_G(x_i)}{f_I(x_i)}\prod_{j=1}^{N} f_I(x_j). \tag{10}$$

ここで $F(X)=\prod_{j=1}^{N} f_I(x_j)$，$g(x)=f_G(x)/f_I(x)$ と置くと，式 (7) (10) より

$$\begin{aligned} I(U;X) &= \frac{1}{N}\sum_i \int_{\mathcal{X}} F(X)g(x_i)\log\frac{F(X)g(x_i)}{\sum_j F(X)g(x_j)/N}dX \\ &= \frac{1}{N}\sum_i \int_{\mathcal{X}} F(X)g(x_i)\log\frac{g(x_i)}{\sum_j g(x_j)/N}dX \\ &= \frac{1}{N}\sum_i \int_{\mathcal{X}} F(X)g(x_i)\log g(x_i)dX \\ &\quad -\frac{1}{N}\sum_i \int_{\mathcal{X}} F(X)g(x_i)\log\left(\frac{1}{N}\sum_j g(x_j)\right)dX, \end{aligned} \tag{11}$$

と変形できる．右辺第一項は

$$\begin{aligned} &\frac{1}{N}\sum_i \int_{\mathcal{X}} F(X)g(x_i)\log g(x_i)dX \\ &= \frac{1}{N}\sum_i \int_{\mathbb{R}} f_I(x_i)g(x_i)\log g(x_i)dx_i \prod_{j\neq i}\int_{\mathbb{R}} f_I(x_j)dx_j \\ &= \frac{1}{N}\sum_i \int_{\mathbb{R}} f_G(x_i)\log\frac{f_G(x_i)}{f_I(x_i)}dx_i \prod_{j\neq i} 1 \\ &= \int_{\mathbb{R}} f_G(x)\log\frac{f_G(x)}{f_I(x)}dx \\ &= D(f_G\parallel f_I). \end{aligned} \tag{12}$$

一方，

$$y_i=g(x_i),\ \ \bar{y}=\frac{1}{N}\sum_{i=1}^{N} y_i, \tag{13}$$

とおくと，式 (11) の右辺第二項は以下のように変形できる．

$$\begin{aligned} &-\frac{1}{N}\sum_i \int_{\mathcal{X}} F(X)g(x_i)\log\left(\frac{1}{N}\sum_j g(x_j)\right)dX \\ &= -\int_{\mathcal{X}} F(X)\left(\frac{1}{N}\sum_i g(x_i)\right)\log\left(\frac{1}{N}\sum_j g(x_j)\right)dX \\ &= -E_{F(X)}[\bar{y}\log\bar{y}]. \end{aligned} \tag{14}$$

最後の項は，X が $F(X)$ に従うときの $\bar{y}\log\bar{y}$ の期待値を表す．大数の法則より，x_i が $f_I(x)$ に従うならば，$N\to\infty$ のとき $\bar{y}$ は以下のように確率収束する．

$$\begin{aligned} \bar{y}\xrightarrow{p} E_{f_I(x)}[g(x)] &= \int_{\mathbb{R}} f_I(x)g(x)dx \\ &= \int_{\mathbb{R}} f_G(x)dx = 1. \end{aligned} \tag{15}$$

また関数 $y\log y$ は $y=1$ で連続なので，スラツキーの定理より

$$\bar{y}\log\bar{y}\xrightarrow{p} 1\log 1=0\ \ (N\to\infty), \tag{16}$$

が成立する．従ってその期待値は

$$E_{F(X)}[\bar{y}\log\bar{y}]\to 0\ \ (N\to\infty), \tag{17}$$

となり，式 (11) の右辺第二項は $N\to\infty$ のとき 0 に収束することがわかる．式 (11) (12) (14) (17) より，

$$I(U;X)\to D(f_G(x)\parallel f_I(x))\ \ (N\to\infty), \tag{18}$$

となって，定理が示された．(証明終わり)

本人分布 $f_G(x)$，他人分布 $f_I(x)$ は，複数の被験者から生体情報サンプルを取得し，本人同士，他人同士の照合スコアを算出することで推定可能であり，これによって KL 情報量を計算することができる (評価方法の詳細は 4. 章で述べる)．そこで，$D(f_G(x)\parallel f_I(x))$ を，生体情報が持つ情報量の評価指標とする．

3.4 評価指標の性質

非負性

任意の分布 $f_G(x), f_I(x)$ に対し

$$D(f_G(x)\parallel f_I(x))\geqq 0. \tag{19}$$

等号成立は $f_G(x) = f_I(x)$ のときに限る (証明は文献[10] を参照のこと). この性質は以下の意味で自然である. 本人分布と他人分布が完全に一致する場合, 生体情報の照合スコアからは本人 (同一生体) か他人 (異なる生体) かを全く判別できないため, 個人識別に関する情報は得られない (情報量は 0). そうでない場合, わずかでも分布が異なれば個人識別に関して情報を得ることができる (情報量は正).

スコア変換に対する不変性 (ROC カーブとの関係)

生体情報 B とテンプレート T を入力とし, その類似度 (または距離)$x \in \mathbb{R}$ を照合スコアとして出力する生体認証システム S に対し, x のかわりに $\hat{x} = \phi(x)$ を出力する生体認証システム $\hat{S}$ を考える. ただし $\phi : \mathbb{R} \to \mathbb{R}$ は単調増加で連続な関数とする. S における判定しきい値 t に対して S' の判定しきい値を $\hat{t} = \phi(t)$ と設定すれば, 両システムの FAR,FRR は等しくなり, 従って ROC カーブも一致する. このとき, 以下のように両システムにおける情報量評価指標の値も等しくなることが示せる.

S における x の本人分布, 他人分布をそれぞれ $f_G(x), f_I(x)$ とし, $\hat{S}$ における分布を $\hat{f}_G(\hat{x}), \hat{f}_I(\hat{x})$ とする. $f_G(x) = \phi'(x)\hat{f}_G(\phi(x)), f_I(x) = \phi'(x)\hat{f}_I(\phi(x))$ (確率分布の変数変換公式) より,

$$\begin{aligned} D(f_G \parallel f_I) &= \int f_G(x) \log \frac{f_G(x)}{f_I(x)} dx \\ &= \int \phi'(x)\hat{f}_G(\phi(x)) \log \frac{\phi'(x)\hat{f}_G(\phi(x))}{\phi'(x)\hat{f}_I(\phi(x))} dx \\ &= \int \hat{f}_G(\phi(x)) \log \frac{\hat{f}_G(\phi(x))}{\hat{f}_I(\phi(x))} d\phi(x) \\ &= D(\hat{f}_G \parallel \hat{f}_I). \end{aligned} \tag{20}$$

このように, ROC カーブを不変とする変数変換 ϕ に対し, 情報量評価指標の値も不変となる (図 1).

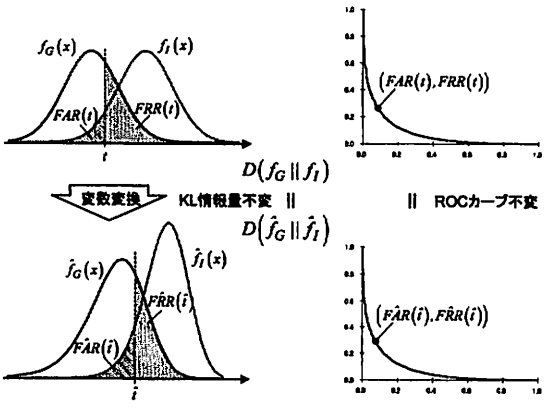

図 1 変数変換に対する不変性

Fig. 1 Invariance under variable transformation

加法性 (マルチモーダル生体認証における情報量)

2 つの異なる生体認証技術 (例えば指紋認証と虹彩認証) を組み合わせることで識別性能を高めるマルチモーダル生体認証システムを考える. 各生体情報が独立ならば, 組み合わせたときの情報量が各情報量の和 (以下) となることを示すことができる. 以下, 詳細に説明する.

マルチモーダル生体認証システム S は, 図 2 のように各生体情報を照合するサブシステム S^1, S^2 と, 各照合スコア $x^1, x^2 \in \mathbb{R}$ から統合スコア $x = T(x^1, x^2) \in \mathbb{R}$ を計算する機能から構成される. ただし統合スコア関数 $T : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ は連続とする.

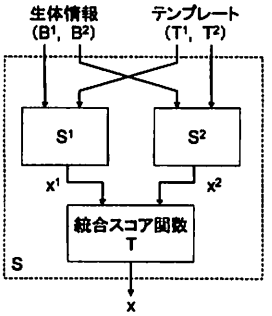

図 2 マルチモーダル生体認証システム

Fig. 2 Multimodal biometric system

S^i $(i = 1, 2)$ における本人分布, 他人分布を $f_G^i(x^i), f_I^i(x^i)$ とし, 統合スコア $x = T(x^1, x^2)$ の分布を $f_G(x), f_I(x)$ とする. また, 本人同士, 他人同士の照合における x^1, x^2 の同時確率密度分布をそれぞれ $f_G^{12}(x^1, x^2), f_I^{12}(x^1, x^2)$ とする.

x^1, x^2 が独立ならば, KL 情報量の加法性[10] より

$$\begin{aligned} &D(f_G^{12}(x^1, x^2) \parallel f_I^{12}(x^1, x^2)) \\ &= D(f_G^1(x^1) \parallel f_I^1(x^1)) + D(f_G^2(x^2) \parallel f_I^2(x^2)). \end{aligned} \tag{21}$$

また, KL 情報量に関する Data Processing Therem[10] より, 以下の不等式が成立する.

$$D(f_G^{12}(x^1, x^2) \parallel f_I^{12}(x^1, x^2)) \geqq D(f_G(x) \parallel f_I(x)) \tag{22}$$

等号成立条件は, 任意の x^1, x^2 に対して

$$\frac{f_G^{12}(x^1, x^2)}{f_I^{12}(x^1, x^2)} = \frac{f_G(T(x^1, x^2))}{f_I(T(x^1, x^2))}. \tag{23}$$

式 (21) (22) より, x^1, x^2 が独立ならば以下の不等式が成立する.

$$D(f_G \parallel f_I) \leqq D(f_G^1 \parallel f_I^1) + D(f_G^2 \parallel f_I^2). \tag{24}$$

この式は, マルチモーダル生体認証システムにおける生体情報の情報量 (左辺) が, 各サブシステムにおける生体情報の情報量の和 (右辺) 以下であることを示している.

なお左辺の情報量は統合スコア関数 $T(x^1, x^2)$ に依存し, これを最大化する T の条件 (等号成立条件) は式 (23) で与えられる. 例えば統合スコア関数として尤度比 $T(x^1, x^2) = f_G^{12}(x^1, x^2)/f_I^{12}(x^1, x^2)$ を用いれば, この条件を満たすことが

できる．これは x^1, x^2 を観測データとしたときの本人/他人の判別に尤度比検定を用いることを意味し，このとき FRR をある一定値以下とする任意の統合スコア関数 (検定) に対して最小の FAR を達成する (最強力検定である) ことが知られている (Neyman-Pearson の補題)．

このようにマルチモーダル生体認証における精度と情報量の間には，エラー確率を最小化する統合スコア関数が情報量を最大化する，という関係がある．

3.5 逐次的マルチモーダル生体認証における解釈と応用

逐次確率比検定 (SPRT) を用いたマルチモーダル生体認証が提案されている [12]．これは例えば指紋，静脈，虹彩を組み合わせて認証を行うときに，まず指紋を測定して照合し，利用者が本人である確率 P(本人 | 指紋) と他人である確率 P(他人 | 指紋) の比 P(本人 | 指紋)/P(他人 | 指紋) を計算する．これがある閾値 t を上回っていればその時点で本人として受理し，認証処理を終了する．そうでない場合は次に静脈を測定，照合し，P(本人 | 指紋，静脈)/P(他人 | 指紋，静脈) を計算して同様の処理を行う．全ての生体情報を照合しても t を上回らなければ他人と判定する．このように逐次的に生体情報の取得，照合，判定を行うことで，全ての生体情報を入力しなくても認証可能とし，精度とともに利用者の利便性を高めることができる SPRT は，観測系列が i.i.d. のとき，同じ精度を達成するあらゆる検定の中で最も観測回数が少ない方法であることが証明されている [11]．また一般に i.i.d. とはならないマルチモーダル生体認証に適用した場合でも，従来の (逐次的でない) マルチモーダル生体認証に対して，平均入力回数を半減しつつ同じ精度を達成できることが報告されている [12]．

SPRT を用いたマルチモーダル生体認証において，逐次的に観測される照合スコアの列を $x^1, x^2, x^3, \cdots$ と表し，それぞれが従う本人分布，他人分布を $f_G^i(x), f_I^i(x)$ $(i = 1, 2, 3, \cdots)$ とする．本人，他人の事前確率を各々 $p, 1-p$ とし，各照合スコアが独立であると仮定すると，n 回の照合を行ったときの確率比 R_n は

$$R_n = \frac{p}{1-p} \prod_{i=1}^{n} r_i, \quad r_i = \frac{f_G^i(x^i)}{f_I^i(x^i)}, \tag{25}$$

両辺の対数をとると，

$$L_n = \log \frac{p}{1-p} + \sum_{i=1}^{n} l_i, \quad l_i = \log \frac{f_G^i(x^i)}{f_I^i(x^i)}, \tag{26}$$

と書ける．したがって SPRT を用いたマルチモーダル生体認証は，x^i を観測するたびに対数尤度を $L_i \leftarrow L_{i-1} + l_i$ と更新し，L_n が $\log t$ 以上となった時点で本人として受理することで実現できる．x^i の観測による増加する対数尤度比の期待値 $E[l_i]$ は，システム利用者が本人であった場合，以下のように $f_G^i(x), f_I^i(x)$ の KL 情報量に等しい．

$$E[l_i] = \int f_G^i(x) \log \frac{f_G^i(x)}{f_I^i(x)} dx = D(f_G^i \parallel f_I^i). \tag{27}$$

つまり SPRT が，逐次的に入力される生体情報から「本人性に関する情報」を蓄積していく過程であると考えれば，$D(f_G \parallel f_I)$ は，1 つの生体情報から獲得できる情報量の期待値であると解釈できる．

ところで SPRT の受理条件は $L_n \geqq \log t$ であるため，一般に $D(f_G \parallel f_I)$ が大きい方が少ない回数で受理されやすいと考えられる．実際，照合スコアが i.i.d. であり閾値 t が十分大きいならば，利用者が本人であった場合の認証成功までの平均入力回数 $E[n]$ は，漸近的に以下のように評価できる [11]

$$E[n] \sim \frac{\log t}{D(f_G \parallel f_I)}. \tag{28}$$

そこで，逐次的マルチモーダル生体認証において，各生体情報の情報量 $D(f_G^i \parallel f_I^i)$ が大きい順に入力 (および照合，判定) を行うことで，入力回数を低減し利便性を高められる可能性がある．ただし実際のシステムでは組み合わせる生体情報の数に限界があり，この順序が常に入力回数を最小化するものではない．有効性の実験的評価は今後の課題である．

3.6 プライバシー保護型生体認証への応用

近年，ネットワークを介した生体認証システムなどにおいて，サーバに対し生体情報を秘匿したまま照合することにより，生体情報の漏洩リスクを低減するとともに利用者のプライバシー保護を実現する，プライバシー保護型生体認証技術の研究が活発に行われている．提案した情報量評価指標は，このような技術のプライバシー保護性能を定量的に評価する指標としても利用可能であると考える．

例えば生体情報を特殊な暗号化関数により変換したままの状態で照合する，キャンセラブル生体認証技術 [13]〜[15] を考える．キャンセラブル生体認証システムでは，登録時に取得した生体情報 A を，秘密の変換パラメータ R に依存して決定する変換関数 F_R により変換 (一種の暗号化) し，$T = F_R(A)$ をテンプレートとしてサーバに登録する．なお R は登録時にランダムに選択し，クライアントが保存する．認証時にはクライアントが新たに取得した生体情報 B を R で変換し，$V = F_R(B)$ をサーバに送信する．サーバは T, V を照合し，一致/不一致を判定する．変換関数 F_R が生体情報間の類似度 (または距離) を保存するように設計することで，サーバは元の生体情報を知ることなく，一致/不一致の判定を行うことができる．

キャンセラブル生体認証によりプライバシーが保護されるためには，変換後の生体情報から個人を識別できないことが必要である．ここで個人の識別とは，テンプレート (変換後の生体情報) と紐付いたシステムの利用者 ID を決定することではなく，変換前の生体情報と紐付いた個人を識別することである．そこで，変換前の生体情報 A と変換後の生体情報 $V = F_R(B)$ を入力とし，A, B の類似度 (または距離) を推定して出力する照合器を考え，この照合器に関する本人分布 $f_G(x)$，他人分布 $f_I(x)$ の KL 距離 $D(f_G \parallel f_I)$ を考える．この値が小さい (0 に近い) ほど，変換後の生体情報から個人を識別することが困難であるため，プライバシー保護性能が高いと言える．そこで $D(f_G \parallel f_I)$ を，キャンセラブル生体認証におけるプライバシー保護性能の評価指標とすることができる．これにより，例えばあるキャンセラブル生体認証システムにおいて $D(f_G \parallel f_I)$ が 5(bit) 程度であったならば，漏洩するプライバシー情報 (個人

識別情報) の量が，都道府県のみの住所情報と同程度 (3.1 節参照) である，といった直観的な理解が可能になる．

なお変換前の生体情報 A と変換後の生体情報 $F_R(B)$ を照合する照合器のアルゴリズムとしては，例えば考えうる全てのパラメータ R' に対して総当り的に $F_{R'}(A)$ を作成して $F_R(B)$ と照合し，類似度の最大値 (または距離の最小値) x を，A, B の類似度 (または距離) の推定値とするなどの方法が考えられる．

4. 評価方法

本章では，実際の生体認証システムに対して情報量 $D(f_G \parallel f_I)$ を評価する方法を述べる．$f_G(x), f_I(x)$ の真の分布は未知であるため，複数の生体情報サンプルを収集・照合し，得られた照合スコアから $f_G(x), f_I(x)$ を推定して $D(f_G \parallel f_I)$ を計算する．

4.1 サンプルの収集・照合

標準的な精度評価方法 [1] と同様の手順に従い，生体情報サンプルの収集と照合を行う．

まず N 人の被験者の生体から，それぞれテンプレート $(T_1, T_2, \cdots, T_N)$ と，照合用生体情報 $(B_1, B_2, \cdots, B_N)$ を取得する (指紋のように 1 人が複数の独立とみなせる生体を持つ場合には，これらを別にカウントしてもよい)．評価結果の信頼性を高めるためには，N をできるだけ大きくすることが望ましい．

次にこれらを総当り的に照合する．T_i と B_j の照合スコアを x_{ij} とすると，x_{ii} は本人同士，$x_{ij} (i \neq j)$ は他人同士の照合スコアである．なお x_{ij} と x_{ji} は統計的に従属と考えられるため，計算量を減らすためにいずれか一方の照合を省略してもよい．こうして得られた本人同士の照合スコアの集合を X_G，他人同士の照合スコアの集合を X_I とする．

4.2 分布推定と KL 情報量の計算

前節の方法で得られた照合スコアを学習データとして本人分布 $f_G(x)$，他人分布 $f_I(x)$ を推定し，KL 情報量を計算する．

照合スコア x が離散値の場合は，単純に出現頻度をヒストグラムとして推定すればよい．例えば 1(一致) または 0(不一致) の 2 値を取る場合，X_G, X_I に含まれる 1 の個数をそれぞれ n_G, n_I とし，$p = n_G/|X_G|$, $q = n_I/|X_I|$ とおくと

$$f_G(1) = p, \quad f_G(0) = 1 - p,$$
$$f_I(1) = q, \quad f_I(0) = 1 - q,$$

と推定できる．このとき KL 情報量は以下のように計算できる．

$$D(f_G \parallel f_I) = \sum_{x=0,1} f_G(x) \log \frac{f_G(x)}{f_I(x)}$$
$$= p \log \frac{p}{q} + (1-p) \log \frac{1-p}{1-q}. \qquad (29)$$

一方 x が連続値の場合，分布推定方法には大きく分けてパラメトリックな方法，ノンパラメトリックな方法，セミパラメトリックな方法がある．

パラメトリックな方法としては，正規分布モデルを仮定して，平均，分散を計算する方法などがある．計算が容易だが，真の分布がモデルから大きく外れている場合に評価結果の信頼性が低くなる．

ノンパラメトリックな方法としては，核関数に基づく方法などがある．これは例えば正規分布 $N(0, \sigma^2)$ を核関数としたとき，

$$f_G(x) = \frac{1}{|X_G|} \sum_{x_i \in X_G} N(x_i, \sigma^2),$$

として推定する．分布の滑らかさを決定するパラメータ σ^2 は，汎化能力が最大となるよう，クロスバリデーション (CV) やブートストラップ (BS) 法などを用いて決定する．真の分布がどのような形であっても適用できるが，データ数が大きい場合に後述する KL 情報量の計算量が大きくなる．

セミパラメトリックな方法としては，例えば混合正規分布を仮定して，平均，分散，混合比などのパラメータを EM アルゴリズムによって推定する方法がある．混合数 (メタパラメータ) は CV 法や BS 法などを用いて決定する．パラメトリックモデルより複雑な分布を推定可能であり，ノンパラメトリックモデルより KL 情報量の計算量が小さくてすむ利点がある．

これらの推定方法には一長一短があり，学習データ (照合スコア) のサイズや統計的な性質などによって適切な方法を選ぶ必要がある．ただし同じ学習データであっても推定方法の違いによって $D(f_G \parallel f_I)$ の評価値が異なるため，分布推定方法の相違に対する評価結果の安定性や，異なる推定方法で評価した情報量同士の比較の正当性については，今後の検討課題である．

$f_G(x), f_I(x)$ を推定したら，最後に KL 情報量 $D(f_G \parallel f_I)$ を計算する．$f_G(x), f_I(x)$ をヒストグラムや正規分布などとして推定した場合などは，解析的に KL 情報量を計算することができるが，そうでない場合には数値積分により近似的に計算する．

5. まとめ

本稿では，生体情報が持つ個人識別情報としての情報量について考察し，その評価指標を提案した．本指標は情報量として自然な性質を持ち，また任意の生体認証技術に対して容易に評価可能であるという特長を持つ．本指標に基づいて生体認証技術の個人識別性能を評価することで，生体認証技術同士の比較が容易となるだけでなく，パスワードや暗証番号などとの対比も可能となり，識別性能をより直観的に理解することができる．また本指標は，プライバシー保護型生体認証におけるプライバシー保護性能の評価指標としても有用であると考える．

文献

[1] A. J. Mansfield and J. L. Wayman, "Best Practices in Testing and Reporting Performance of Biometric Devices," National Physical Laboratory, Center for Mathematics and Scientific Computing, Tech. Rep., Version 2.01, 2002.

[2] S. Pankanti, S. Prabhakar and A. K. Jain, "On the individuality of Fingerprints," IEEE Trans. on PAMI, Vol. 24, No. 8, pp. 1010–1025, 2002.

[3] 浅井 紘, 星野 幸夫, 木地 和夫, "マニューシャネットワーク特徴による自動指紋照合—特徴抽出過程—," 信学論, Vol. J72-D-II, No. 5, pp.724–732, 1989.

[4] 浅井 紘, 星野 幸夫, 木地 和夫, "マニューシャネットワーク特徴による自動指紋照合—照合過程—," 信学論, Vol. J72-D-II, No. 5, pp.733–740, 1989.

[5] 中島寛, 小林孝次, 森川誠, 勝亦敦, 伊藤康一, 青木孝文, 樋口龍

雄, "位相限定相関法に基づく指紋照合技術 — 一般住宅向け指紋照合装置のためのアルゴリズム設計と実現 —," 電気学会論文誌 E, Vol. 126, No. 2, pp. 38–46, February 2006.
[6] Daugman, J., "The importance of being random: Statistical principles of iris recognition," Pattern Recognition, Vol. 36, No. 2, pp. 279-291, 2003.
[7] A. Adler, R. Youmaran, and S. Loyka, "Towards a measure of biometric information," in Proc. Can. Conf. Comp. Elec. Eng. (CCECE), 2006.
[8] E. Henry, "Classification and Uses of Fingerprints," Routledge, London, 1900.
[9] W. Burr, D. Dodson, and W. Polk, "Electronic authentication guideline," NIST Special Publication 800-63, 2004.
[10] S. Kullback and R. A. Leibler, "On Information and Sufficiency," Ann. Math. Statist. Vol. 22, No. 1, pp. 79–86, 1951.
[11] A.Wald, "Sequential Analysis," John Wiley and Sons, 1947.
[12] 高橋健太, 三村昌弘, 磯部義明, 瀬戸洋一, "逐次確率比検定とロジスティック回帰を用いたマルチモーダル生体認証," 信学論, Vol. J89-D, No. 5, pp. 1061–1065, 2006.
[13] N.K. Ratha, J.H. Connell, and R.M. Bolle, "Enhancing security and privacy in biometricbased authentication systems," IBM System Journal, Vol.40, No.3, 2001.
[14] 高橋健太, 三村昌弘, "キャンセラブル指紋照合方式の提案," In CSS2005, pp. 379–384, 2005.
[15] 比良田真史, 高橋健太, 三村昌弘, "画像マッチングに基づく生体認証に適用可能なキャンセラブルバイオメトリクスの提案," 情報処理学会研究報告, 2006-CSEC-34, pp. 435–440, 2006.