講演番号：21

登録雑音を考慮した複合通信路を伴う生体識別システム

Biometric identification system with compound enrollment channels

吉村 海渡 * 八木 秀樹 *
Kaito YOSHIMURA Hideki YAGI

* 電気通信大学 大学院情報理工学研究科
*The University of Electro-Communications

1 はじめに

生体識別システム (BIS: Biometric Identification System) についての研究は広く行われている [1],[2]．文献 [1] では，登録雑音を考慮した単一通信路を伴う GS-BIS (Generated Secret-BIS) の容量域が特徴づけられており，文献 [2] では，登録雑音を考慮しない複合通信路を伴う GS-BIS の容量域が特徴づけられている．本稿では，登録雑音を考慮した複合通信路を伴う GS-BIS の容量域を解析する．

2 システムモデル

登録雑音を考慮した複合通信路を伴う GS-BIS のシステムモデル (**登録過程**と**識別過程**) を図 1 に示す．

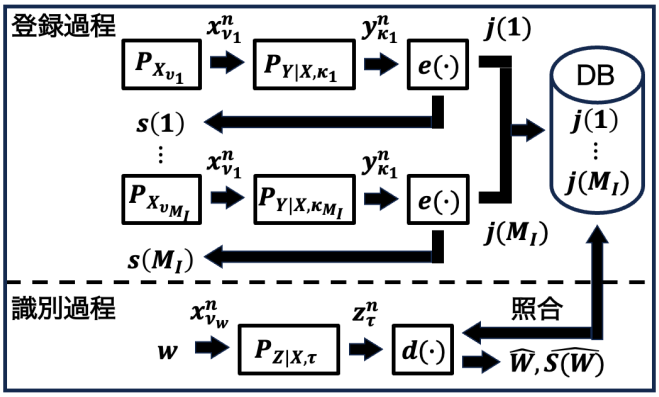

図 1 登録雑音を考慮した複合通信路を伴う GS-BIS

(I) 登録過程: M_I 個の個体の生体情報を登録する．個体 $i \in \mathcal{I} \triangleq [1 : M_I]$ の生体情報系列 $X^n_{\nu_i} \in \mathcal{X}^n$ は，状態 ν_i における確率分布 $P_{X_{\nu_i}} \in \{P_{X_\nu}, \nu \in \mathcal{V}\}$ に従い，独立同分布で生成される．ただし，$\mathcal{V}$ は生体情報の状態集合を表す．ここで，$P_{X_{\nu_i}}$ は $P_{X|V=\nu_i}$ の略記である．

$$P_{X^n_{\nu_i}}(x^n_{\nu_i}) = \prod_{t=1}^{n} P_{X_{\nu_i}}(x_{\nu_i,t}). \tag{1}$$

生成された生体情報系列 $X^n_{\nu_i}$ は，**登録通信路** $\mathcal{P}_e(= \{P_{Y|X,\kappa}|\kappa \in \mathcal{K}\})$ を通して，$Y^n_{\kappa_i} \in \mathcal{Y}^n$ として観測される．ただし，$\mathcal{K}$ は登録通信路の状態集合を表す．符号器 $e(\cdot)$ は $Y^n_{\kappa_i}$ を観測して，符号語 $J(i) \in \mathcal{J} \triangleq [1 : M_J]$ と秘匿情報 $S(i) \in \mathcal{S} \triangleq [1 : M_S]$ を生成する．

$$(J(i), S(i)) = e(Y^n_{\kappa_i}). \tag{2}$$

符号語 $J(i)$ は公開データベースの i 番目に格納され，秘匿情報 $S(i)$ は秘匿性を保ったまま個体 i に渡される．

(II) 識別過程: 事前に登録された未知個体 w の生体情報系列 $X^n_{\nu_w}$ は，**識別通信路** $\mathcal{P}_i(= \{P_{Z|X,\tau}|\tau \in \mathcal{T}\})$ を通して，$Z^n \in \mathcal{Z}^n$ として観測される．ただし，$\mathcal{T}$ を識別通信路の状態集合とする．復号器 $d(\cdot)$ は Z^n を観測すると，DB 内の符号語 $\mathcal{J}_{M_I} \triangleq [J(1) : J(M_I)]$ と照合して，個体インデックスと秘匿情報の組 $(\widehat{W}, \widehat{S(W)})$ を推定する．

$$(\widehat{W},\ \widehat{S(W)}) = d(Z^n,\ \mathcal{J}_{M_I}). \tag{3}$$

3 達成可能性と容量域

定義 1 任意の $\delta > 0$ と十分に大きい n に対して，式 (4)–(8) を満たす符号器と復号器の組が存在するとき，レート組 (R_I, R_S, R_J, R_L) は**達成可能**であるという．ここで，$B_{\nu,\kappa,\tau} = \{V = \nu,\ K = \kappa,\ T = \tau\}$ とおく．

$$\sup_{\nu,\kappa,\tau} \Pr\{(\widehat{W}, \widehat{S(W)}) \neq (W, S(W))|B_{\nu,\kappa,\tau}\} \leq \delta, \tag{4}$$

$$\log M_I \geq n(R_I - \delta),\quad \log M_J \leq n(R_J + \delta), \tag{5}$$

$$\inf_{\nu,\kappa,\tau} H(S(W)|B_{\nu,\kappa,\tau}) \geq n(R_S - \delta), \tag{6}$$

$$\sup_{\nu,\kappa,\tau} I(X^n_\nu; J(W)|B_{\nu,\kappa,\tau}) \leq n(R_L + \delta), \tag{7}$$

$$\sup_{\nu,\kappa,\tau} I(J(W); S(W)|B_{\nu,\kappa,\tau}) \leq n\delta. \tag{8}$$

すべての達成可能なレート組 (R_I, R_S, R_J, R_L) の集合を，**GS-BIS モデルの容量域**といい，$\mathcal{R}_G$ で表す． □

定義 2 GS-BIS モデルを特徴づけるレート領域を定義する．

$$\begin{aligned}\mathcal{A} = \{&(R_I, R_S, R_J, R_L) : R_I \geq 0, R_S \geq 0,\\ &R_I + R_S \leq \min_{\nu,\kappa,\tau} I(Z_\tau; U_\kappa),\\ &R_J \geq \max_{\nu,\kappa,\tau}\{I(Y_\kappa; U_\kappa) - I(Z_\tau; U_\kappa)\} + R_I,\\ &R_L \geq \max_{\nu,\kappa,\tau}\{I(X_\nu; U_\kappa) - I(Z_\tau; U_\kappa)\} + R_I,\\ &\text{for some } U_\kappa \text{ s.t. } Z_\tau - X_\nu - Y_\kappa - U_\kappa\}.\end{aligned} \tag{9}$$

ここで，補助確率変数 U_κ は有限集合 $\mathcal{U}$ $(|\mathcal{U}| \leq |\mathcal{Y}| + |\mathcal{V}|(|\mathcal{T}| + 1))$ に値をとる． □

登録通信路 $P_{Y|X,\kappa}$ と識別通信路 $P_{Z|X,\tau}$ の出力は ν にも依存するため，領域 $\mathcal{A}$ に現れる $I(Z_\tau, U_\kappa)$ および $I(Y_\kappa, U_\kappa)$ は (ν, κ, τ) に関して最大化 (最小化) をとる必要がある．

本研究では，$\mathcal{R}_G$ を系列長 n に依存しない形で特徴づけることが課題であり，次式の定理が示される．

定理 1 $$\mathcal{R}_G \subseteq \mathcal{A}. \tag{10}$$ □

定理 1 では領域 $\mathcal{A}$ が容量域 $\mathcal{R}_G$ の外界になることを示しているが，登録通信路が無雑音の場合 (文献 [2])，領域 $\mathcal{A}$ と容量域 $\mathcal{R}_G$ は一致する．また本研究のシステムモデルの情報源と通信路の状態数が 1 つの場合は，文献 [1] の結果と一致する．

4 今後の方針

領域 $\mathcal{A}$ が GS-BIS モデルの容量域 $\mathcal{R}_G$ の内界になることを証明することと，CS-BIS (Chosen Secret-BIS) の容量域を特徴づけることを予定している．

参考文献
[1] V. Yachongka and H. Yagi, “Fundamental limits of biometric identification system under noisy enrollment,”*IEICE Trans. Fundamentals,* vol. E104-A, no. 1, pp. 283–294, Jan. 2021.

[2] L. Zhou, “Information-theoretic Privacy and Secrecy in Biometric Identification and Authentication,” Doctoral Thesis, KTH Royal Institute of Technology, Stockholm, Sweden, 2022.