Vol.2014-DPS-158 No.26
Vol.2014-CSEC-64 No.26
2014/3/6

ハミング距離を用いた生体認証に対するウルフ安全アルゴリズム

キム　キョンド[1,a)]　井沼 学[2,b)]　大塚 玲[3,c)]　今井 秀樹[1,d)]

概要：本研究の目的は，スコアの正規化を行うことで，ハミング距離を用いる生体認証をより安全にすることである．バイオメトリクス認証における問題としては，ユーザによって FAR や FRR が高くなることが知られているが，これはスコアを正規化することで対処可能である．スコア正規化の例としては，Daugman の提案した虹彩認証アルゴリズム [2] がある．このアルゴリズムでは，照合で有効となるビット数によってスコアの分布や平均を推定することでスコアを正規化する．そこで本研究では，Daugman の手法を拡張し，前述の場合においてもスコアを正規化できる手法を提案する．この提案手法を三浦，長坂，宮武らの指静脈認証 [7] に対して適用したところ，FAR を一定に保てることが実験的に確かめられた．さらに，この指静脈認証アルゴリズムに有効とされるウルフに対しても有効であることがわかった．

キーワード：バイオメトリクス，指静脈認証，虹彩認証，アイリスコード，ウルフ攻撃

1. はじめに

生体情報（指紋，静脈，虹彩など）を利用して個人を認証するバイオメトリクス認証は，銀行 ATM の本人確認，空港の出入国管理，重要施設への入退管理，自治体役場や医療現場での重要データへのアクセス管理など，様々な場面で使用されるようになり，セキュリティ評価技術の確立が急務となっている．バイオメトリクス認証システムへの意図的ななりすまし攻撃に対するセキュリティは，ウルフ攻撃確率（Wolf Attack Probability: WAP）[5] によって評価される．ウルフ攻撃（wolf attack）とは，攻撃者が，不特定多数のテンプレートと高確率で誤一致するサンプル（ウルフ：wolf）を提示するなりすまし攻撃であり，ウルフ攻撃の最大攻撃成功確率がウルフ攻撃確率 WAP（第 2 節参照）である。

[1] 中央大学 理工学部
Department of Electrical, Electronic, and Communication Engineering, Faculty of Science and Engineering, Chuo University, 1-13-27 Kasuga Bunkyo-ku 112-8551Tokyo, Japan
[2] 城西大学理学部数学科
Department of Mathematics, Faculty of Science Josai University, Keyakidai 1-1, Sakado, Japan
[3] 産業技術総合研究所
Advanced Industrial Science and Technology, Umezono Tsukuba-shi Ibaraki 305-8568, Japan
[a)] kim-kyondo@imailab.jp
[b)] inuma@josai.ac.jp
[c)] otsuka@ni.aist.go.jp
[d)] h-imai@imailab.jp

ウルフ攻撃への対策として，人工物や異常なサンプルの提示を検知するセンサや検知アルゴリズムをシステムに組み込むことが考えられるが，攻撃者が検知センサや検知アルゴリズムを破る人工物を提示してウルフ攻撃を行うかもしれず，そのような攻撃の成功確率が十分小さいことを証明するのは困難である．そこで，ウルフ攻撃への対策として，認証時に提示されたどのような特徴情報に対してもテンプレートとの誤一致確率を増加させない，証明可能な安全性を有する照合アルゴリズムの構築が重要である．本稿では，そのような照合アルゴリズムの構築方法に焦点を当てる．

井沼・大塚・今井 [3] は，ウルフ攻撃に対し証明可能安全性を有する照合アルゴリズム構築のためのフレームワークを提案した．井沼らは，認証時に提示された特徴情報に対して，その特徴情報と全ユーザの登録テンプレートとの照合スコア分布を推定して，推定した分布によって判定しきい値を変える（照合スコアを正規化する）照合アルゴリズムを提案し，ウルフ攻撃に対して安全であることを証明した．このとき，照合スコア分布の推定が高精度／高速であるほど，アルゴリズムはより安全／高速となる．

虹彩認証の分野では，J. Daugman が，虹彩画像の位相情報を抽出した 2 値データを特徴情報として照合する虹彩認証アルゴリズムを提案している [1]．この照合アルゴリズムは，まぶたやまつげなどの影響なく十分な位相情報が抽出できたビット (有効ビット) 同士のハミング距離を

照合スコアとして一致／不一致の判定を行う．しかしながら，このアルゴリズムは，有効ビット数が小さい特徴情報ほど誤一致確率が高くなるため，Daugman は，登録側・認証側ともに有効ビットとなるビット (共通有効ビット) の長さに応じて判定しきい値を変える (照合スコアを正規化する) 照合アルゴリズムを新たに提案した [2]．さらに，Daugman は自身の実験から，共通有効ビット長 n である他人の虹彩同士の照合スコア分布が，2 項分布 $B(\lambda n, \frac{1}{2})$ (λ は虹彩の位相情報の相関を反映したある定数) で近似できることを示している．Daugman のアルゴリズム [2] は，この仮定の下で，提示するサンプルの有効ビット長を変化させて誤一致確率を増加させようとするウルフ攻撃に対して安全であることが証明される．

井沼ら [3] の提案したフレームワークの中で Daugman のアルゴリズムを眺めると，それは，広範囲なバイオメトリクス照合アルゴリズム (特徴情報のハミング距離を照合スコアとする照合アルゴリズム) に適用可能で，かつ，ある程度妥当な仮定の下で，一定範囲のウルフ攻撃 (照合に用いる有効ビットの長さをコントロールするウルフ攻撃) に対して証明可能な安全性を有する効率の良いアルゴリズムの具体例を与えている．しかしながら，Daugman のアルゴリズムは，共通有効ビット長 n が変化して 2 項分布の長さ λn が変化しても，反転率 $\frac{1}{2}$ は変化しないという仮定の下で安全である．これは，虹彩特徴情報に対しては妥当な仮定であるが，一般のモダリティに対しては必ずしもそうであるとは限らない．

そこで，本稿では，より一般の特徴情報のハミング距離を照合スコアとして判定する照合アルゴリズムに対して適用可能な，証明可能な安全性を持つ効率の良い照合アルゴリズムを提案する．本稿の仮定は，Daugman のアルゴリズムを包含し，特徴情報はある長さの符号語であり，各ビットはハミング距離の計算に寄与する有効ビット，あるいはハミング距離の計算に寄与しない非有効ビットのいずれかであるとする．そして，登録特徴情報と照合時に入力された特徴情報との有効ビット同士のハミング距離を照合スコアとする．ただし，共通有効ビット長 n である他人の虹彩同士の照合スコア分布は 2 項分布 $B(\lambda n, \Delta(n))$ (反転率 $\Delta(n)$ は n に応じて変化する) で近似できると仮定する．

さらに，本研究では，提案アルゴリズムを，三浦・長坂・宮武ら [7] によって提案された指静脈認証アルゴリズム (以後は MNM アルゴリズムと呼ぶ) に適用し，宇根ら [5] が示したウルフ理論に基づいて森田ら [4] が作成したウルフサンプルを用いてウルフ攻撃実験を行った．その結果，提案アルゴリズムを適用しない場合の誤一致確率が 92.5% であるのに対し，提案アルゴリズム提供後の誤一致確率 0% となり，提案アルゴリズムがある種の強いウルフ攻撃に対して安全であることが確かめられた．

2. ウルフ攻撃確率（WAP : Wolf Attack Probability)

対象となる生体認証システム Π に対して，U は全ユーザの集合，S_h は全ユーザ (人間) のサンプルの集合，S_A はシステム Π に提示可能な (人工物も含めた) サンプル全体の集合とする．$S_h \subset S_A$ である．照合アルゴリズム COMP_Π は，ユーザのサンプル (から生成したテンプレート) $s \in S_h$ と認証時に提示されたサンプル $t \in S_A$ を入力として *accept* (受入) または *reject* (拒否) のいずれかを返す．サンプル $t \in S_A$ に対する誤受け入れ率 FAR_t を次の通り定義する．

$$\mathrm{FAR}_t = \operatorname*{Ave}_{s \in S_h \setminus \{t\}} \Pr[\,\mathrm{COMP}_\Pi(s,t) = \mathit{accept}\,] \qquad (1)$$

ここで，$\operatorname*{Ave}_{x \in X} f(x)$ は，集合 X から $x \in X$ が一様ランダムに選ばれるときの関数 $f(x)$ の期待値である．このとき，他人受け入れ率 FAR はユーザのサンプル $t \in S_h$ に対する FAR_t の期待値である:

$$\begin{aligned}\mathrm{FAR} &= \operatorname*{Ave}_{t \in S_h} \mathrm{FAR}_t \\ &= \operatorname*{Ave}_{t \in S_h} \operatorname*{Ave}_{s \in S_h \setminus \{t\}} \Pr[\,\mathrm{COMP}_\Pi(s,t) = \mathit{accept}\,] \qquad (2)\end{aligned}$$

サンプル $w \in S_A$ に対する誤受け入れ率 FAR_w が他人受け入れ率 FAR より大きいとき，サンプル w をウルフと呼ぶ [3], [5] (脅威となるのは，FAR_w が FAR より極端に大きいウルフである)．

認証アルゴリズムの情報を完全に知っている攻撃者が，ランダムに選ばれたユーザ $u \in U$ に対して，ウルフを提示してなりすまそうとする攻撃をウルフ攻撃と呼ぶ [3], [5]．ただし，攻撃者は，なりすまし対象であるユーザのテンプレート $t_u \in S_h$ を知らないと仮定する．

ウルフ攻撃確率 (Wolf Attack Probability: WAP) は，あらゆるウルフ攻撃にわたる最大攻撃成功確率である [3], [5]:

$$\mathrm{WAP} = \max_{t \in S_A} \operatorname*{Ave}_{s \in S_h} \Pr[\,\mathrm{COMP}_\Pi(s,t) = \mathit{accept}\,] \qquad (3)$$

宇根・大塚・今井 [5] は，公開されている指紋認証アルゴリズム [6] と静脈認証アルゴリズム [7] に対して，FAR は小さいが，WAP が極端に大きな値となる例を示した．強力なウルフ $w \in S_A$ が存在していたとしても，$w \notin S_h$ であったり (人間のサンプルとは程遠いものであるなど)，$w \in S_h$ であっても，そのようなウルフの個数が十分に多くない場合は FAR の値にほとんど影響を与えないため，FAR が小さい値になる場合がある．よって，ウルフ攻撃に対するセキュリティ評価には，FAR だけではなく，WAP による評価が必要である．ウルフ攻撃確率 WAP が十分に小さい認証アルゴリズムをウルフ安全な認証アルゴリズムと呼ぶ．

3. Daugman の虹彩認証アルゴリズム

J．Daugman の虹彩認証アルゴリズム [1], [2] は，虹彩

画像からウェーブレット変換を用いて抽出した位相情報を 2 値データに符号化したもの (アイリスコード) と，瞼やまつ毛などによって虹彩が覆われ十分な位相情報を抽出できない領域を示す 2 値データ (マスクコード) を特徴情報として用いる．マスクコードは，アイリスコードと同じ長さのデータであり，アイリスコードにおいて十分な位相情報が得られた (と判定された) 領域に対応するビットの値を 1 とし (有効ビットと呼ぶ)，そうでない領域に対応するビットの値を 0 とする (非有効ビットと呼ぶ)．

虹彩画像 X のアイリスコードとマスクコードをそれぞれ $\mathrm{code}\,X$, $\mathrm{mask}\,X$ としたとき，2 つの虹彩画像 X, Y に対して $\mathrm{HD}_{\mathrm{raw}}(X,Y)$ を以下のように定義する:

$$\mathrm{HD}_{\mathrm{raw}}(X,Y)=\frac{||(\mathrm{code}\,X\oplus\mathrm{code}\,Y)\cap\mathrm{mask}\,X\cap\mathrm{mask}\,Y||}{||\,\mathrm{mask}\,X\cap\mathrm{mask}\,Y||} \tag{4}$$

ここで，$||c||$ は符号語 c のハミング重みを表し，2 符号つの語 $c=(c_1,c_2,\ldots,c_N)$, $c'=(c'_1,c'_2,\ldots,c'_N)\in\{0,1\}^N$ に対して $c\cap c'=(c_1c'_1,c_2c'_2,\ldots,c_Nc'_N)$ である．$\mathrm{HD}_{\mathrm{raw}}(X,Y)$ は X と Y の共通有効ビット間のエラー率である．$\mathrm{HD}_{\mathrm{raw}}(X,Y)$ がある閾値より大きいかどうかで照合判定した場合に，有効ビット長 $||\mathrm{mask}\,X||$ の小さい虹彩画像 X に対する誤受け入れ率が極端に増加するため，Daugman [2] は次の正規化ハミング距離 $\mathrm{HD}_{\mathrm{norm}}$ によって判定する照合アルゴリズムを提案した．$||\,\mathrm{mask}\,X\cap\mathrm{mask}\,Y||=n$ である X, Y に対して $\mathrm{HD}_{\mathrm{norm}}(X,Y)$ を以下のように定義する．

$$\mathrm{HD}_{\mathrm{norm}}(X,Y)=0.5+(\mathrm{HD}_{\mathrm{raw}}(X,Y)-0.5)\sqrt{\frac{n}{911}} \tag{5}$$

ここで，Daugman は，自身の実験 [2] より，共通有効ビット長 $||\mathrm{mask}\,X\cap\mathrm{mask}\,Y||=n$ のときの $\mathrm{HD}_{\mathrm{raw}}(X,Y)$ の分布が，2 項分布のスカラー倍 $\frac{1}{\lambda n}B(\lambda n,0.5)$ に従うと仮定した．つまり，Daugman は，共通有効ビット間のビット反転の分布が，そのままの長さ n のベルヌーイ分布ではなく，何らかの相関があって n に比例した長さをもつベルヌーイ分布であると仮定した．λ はその比例定数である．よって，$\mathrm{HD}_{\mathrm{raw}}(X,Y)$ の分布は平均 0.5，分散 $\frac{1}{4\lambda n}$ の正規分布で近似される．

式 (5) 中の 911 は Daugman の実験による共通有効ビット長 n の期待値であるが，式 (5) によって定義された $\mathrm{HD}_{\mathrm{norm}}(X,Y)$ の分布は，共通有効ビット長 n に依らず，平均 0.5，分散 $\frac{1}{4\lambda\times911}$ の正規分布で近似される．

これによって，有効ビット数によらずに FAR が一定になるだけではなく，有効ビット数をコントロールするようなウルフ攻撃 (虹彩部分の大半を隠して情報量を極端に少なくすることで有効ビット数を減らすなど) に対しても安全な照合アルゴリズムとなる．

4. 三浦・長坂・宮武の指静脈認証アルゴリズム

三浦・長坂・宮武らの指静脈認証アルゴリズム (以降 MNM アルゴリズムと呼ぶ) [7] は，グレースケールの静脈画像をいくつかの小領域に分割し，各小領域を静脈領域 (ビット値を 0 とする)，背景領域 (ビット値を 255 とする)，あいまい領域 (ビット値を 128 とする) のいずれか 1 つで指定して生成した一定長の 3 値データを特徴情報とする．2 つの静脈画像から抽出した特徴情報 $x=(x_1,x_2,\ldots,x_N)$, $y=(y_1,y_2,\ldots,y_N)\in\{0,128,255\}^N$ に対して x, y のミスマッチ率 $R_m(x,y)$ は以下で定義される:

$$R_m(x,y)=\frac{\#\{i\mid|x_i-y_i|=255\}}{\#\{i\mid x_i=0\}+\#\{i\mid y_i=0\}} \tag{6}$$

ここで，$\#K$ は集合 K の要素数を表す．特徴情報 x_i $(1\le i\le N)$ のうち $x_i=0$ または 255 となるビット i を有効ビット，$x_i=128$ となるビット i を非有効ビットと呼ぶことにすると，$R_m(x,y)$ は，おおよそ，x, y の有効ビット全体に対するエラー率であるが，分母の $\#\{i\mid x_i=0\}+\#\{i\mid y_i=0\}$ では x, y の共通有効ビットが重複して数え上げられていることに注意する．MNM アルゴリズムは，登録特徴情報 x と認証時に入力された特徴情報 y に対して，ミスマッチ率 $R_m(x,y)$ がある閾値以下のとき accept (受入)，閾値より大きいときは reject (拒否) とするアルゴリズムである．

しかしながら，MNM アルゴリズムには，$\mathrm{HD}_{\mathrm{raw}}$ で直接判定する Daugman の初期のアルゴリズム [1] と同様の脆弱性がある．つまり，有効ビット数が極端に少ない静脈画像 x あるいは y に対して誤受け入れ率が著しく増加するということである． 宇根・大塚・今井 [3] では，全てあいまい領域となる特徴情報を持つ静脈画像は，すべての登録テンプレートと一致する強力なウルフ (ユニバーサル・ウルフと呼ばれる) となることが示されている．

そこで，本稿では，第 3 節で紹介した Daugman アルゴリズム [2] を拡張して，ハミング距離を照合スコアとする場合に適用可能なウルフ安全な照合アルゴリズムを提案し，それを MNM アルゴリズムの照合アルゴリズム部分に適用することで，上述のウルフ攻撃に対して安全な指静脈認証を構築する．詳細を次節で述べる．

5. ウルフ安全な照合アルゴリズムの提案

生体認証システムにおいて，登録時，認証時ともに特徴情報 x は一定長の 2 値符号で表されるとする: $x=(x_1,x_2,\ldots,x_N)\in\{0,1,null\}^N$．ここで，そのビットの特徴情報が十分信頼できないものであるとき $x_i=null$ として非有効ビットと呼ぶ．それに対して $x_i=0$ または 1 のビットを有効ビットと呼ぶ．例えば，第 4 節の MNM アルゴリズムにおいて $x_i=255$ ならば $x_i=1$ とし，$x_i=128$ ならば $x_i=null$ として読み直せばよ

い．また，第 3 節の Daugman アルゴリズム [3] の場合は，虹彩画像 X から抽出される長さ N のアイリスコードとマスクコードのペア $\mathrm{code}\,X, \mathrm{mask}\,X$ に対して符号 $x = (x_1, x_2, \ldots, x_N) \in \{0, 1, null\}^N$ を次のように定義する：

$$x_i = \begin{cases} 0 & \text{if } (\mathrm{code}\,X)_i = 0, (\mathrm{mask}\,X)_i = 1 \\ 1 & \text{if } (\mathrm{code}\,X)_i = 1, (\mathrm{mask}\,X)_i = 1 \\ null & \text{if } (\mathrm{mask}\,X)_i = 0 \end{cases} \quad (7)$$
$$(1 \le i \le N)\,.$$

ここで，$(\mathrm{code}\,X)_i, (\mathrm{mask}\,X)_i$ はそれぞれアイリスコードとマスクコードの i ビット目を表す．

登録時と認証時の特徴情報 x, y に対して共通有効ビット間のハミング距離率 $\mathcal{HD}(x, y)$ を以下で定義する:

$$\mathcal{HD}(x, y) = \frac{\#\{i \mid |x_i - y_i| = 1\}}{\#\{i \mid x_i \neq null \wedge y_i \neq null\}} \quad . \quad (8)$$

ここで，MNM アルゴリズムで用いられたミスマッチ率 R_m と $\mathcal{HD}$ を比較するといくつか異なる点がある．R_m では，静脈画像全体に対して，背景領域が広く静脈領域が狭いことを考慮している．x, y ともに背景領域となる部分を分母に含めると静脈領域の一致に対するエラー率 R_m の減少が鈍くなり，本人と他人の識別能力が低下することが懸念される．そこで，MNM アルゴリズムのエラー率 R_m では x, y の静脈領域のみに注目し，x, y ともに背景領域である部分を分母から除いている．しかしながら，あいまい領域 (非有効ビット) も分母に含んでしまったため，宇根・大塚・今井 [3] が指摘したように，非有効ビットのみの特徴情報をもつサンプルがユニバーサル・ウルフとなってしまう。一方，$\mathcal{HD}$ の分母では，x, y ともに背景領域である部分を含むため，識別能力の低下が懸念される．さらに，分母の数え上げから非有効ビットを取り除くことで，上述のユニバーサル・ウルフに対する耐性はあるものの，$\mathcal{HD}$ の値でそのまま判定した場合には，依然として，有効ビット長をコントロールするウルフ攻撃に対する脆弱性を有する．

また，Daugman のアルゴリズム [1], [2] の $\mathrm{HD}_{\mathrm{raw}}$ と $\mathcal{HD}$ の関係は，虹彩画像 X, Y に対応する 3 値符号を x, y とするとき，$\mathcal{HD}(x, y) = \mathrm{HD}_{\mathrm{raw}}(X, Y)$ であるので，やはり，$\mathcal{HD}$ のみによる判定は，有効ビット長をコントロールするウルフ攻撃に対して脆弱である．

そこで，本稿では，第 3 節で紹介した Daugman アルゴリズム [2] を拡張するかたちで，ハミング距離率 $\mathcal{HD}$ を用いたウルフ安全な照合アルゴリズムを提案する．

まず，2 つの特徴情報 x, y の共通有効ビット長が $\#\{i \mid x_i \neq null \wedge y_i \neq null\} = n$ であるとき，ハミング距離率 $\mathcal{HD}(x, y)$ の分布は 2 項分布のスカラー倍 $\frac{1}{\lambda n} B(\lambda n, \Delta(n))$ に従うと仮定する [*1]．つまり，Daugman アルゴリズム [2] と同様に，共通有効ビット間のビット反転の分布が，共通有効ビット長 n に比例して長さが決まるベルヌーイ分布であると仮定する．反転率 $\Delta(n)$ は，Daugman では一定値 (0.5) と仮定したが，提案方式では n によって変化するものと仮定する．実際，MNM アルゴリズムの特徴情報では，反転率 $\Delta(n)$ は n の増加にしたがって減少することが実験で確かめられている (図 1 参照)．つまり，$\mathcal{HD}(x, y)$ は

$$\text{平均} \quad \Delta(n)$$
$$\text{分散} \quad \sigma(n)^2 = \frac{\Delta(n)(1 - \Delta(n))}{\lambda n} \quad (9)$$

の正規分布で近似される．

ここで，正規化ハミング距離率 $\mathcal{HD}_{\mathrm{norm}}(x, y)$ を $\#\{i \mid x_i \neq null \wedge y_i \neq null\} = n$ である x, y に対して

$$\mathcal{HD}_{\mathrm{norm}}(x, y) = \frac{\mathcal{HD}(x, y) - \Delta(n)}{\sigma(n)} \quad (10)$$

と定義する．このとき，上述の仮定から 他人同士の特徴情報 x, y に対する $\mathcal{HD}_{\mathrm{norm}}(x, y)$ の分布は，共通有効ビット長 n によらず，平均 0，分散 1 の正規分布で近似される．

登録テンプレートの特徴情報 x と照合時に入力された特徴情報 y との正規化ハミング距離率 $\mathcal{HD}_{\mathrm{norm}}(x, y)$ によって「受入」または「拒否」のいずれかで判定する照合アルゴリズムは，有効ビット数によらずに FAR が一定となるだけではなく，有効ビット数をコントロールするようなウルフ攻撃に対して安全であり，かつ，効率の良い照合アルゴリズムとなる．

6. 指静脈認証アルゴリズムへの応用

本節では，前節で提案したウルフ安全な照合アルゴリズムを MNM アルゴリズム [7] の照合アルゴリズムに適用して，その認証精度とウルフ攻撃に対する安全性を実験で評価する．

まず，MNM アルゴリズムの特徴抽出アルゴリズムで収集した特徴情報 x, y に対するハミング距離率 $\mathcal{HD}(x, y)$ の平均値 $\Delta(n)$ を実験によって求めた．

MNM アルゴリズムの特徴抽出アルゴリズムは，森田ら [4], [10] が実装したものを使用した．また，指静脈画像は，森田ら [4], [10] の実装した指静脈画像撮影装置で採取した指 30 本分の指静脈画像 120 枚 (1 指につき 4 枚の画像) を使用した．図 1 に，共通有効ビット数 $n = \#\{i \mid x_i \neq null \wedge y_i \neq null\}$ とそのときのハミング距離率 $\mathcal{HD}(x, y)$ の平均値 $\Delta(n)$ (ここでは第 5 節の仮定のもとに $\Delta(n)$ と書く) の関係を示す．この実験データをもと

[*1] 他人同士の共通有効ビット間のビット反転率とウルフが人間の特徴情報に対して達成可能なビット反転率には差があり，$\Delta(n)$ よりも小さいビット反転率を達成可能なウルフが存在するかもしれない．このような仮定の下での厳密な評価は今後の課題とする．

Vol.2014-DPS-158 No.26
Vol.2014-CSEC-64 No.26
2014/3/6

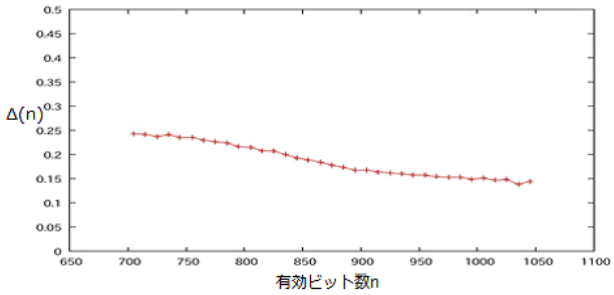

図 1　有効ビット数 n と $\Delta(n)$ との関係図

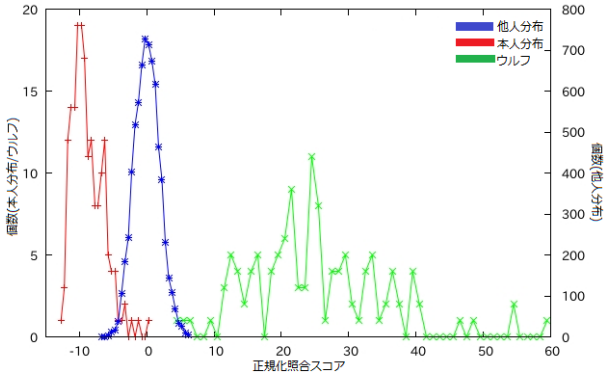

図 2　正規化ハミング距離率 $\mathcal{HD}'_{\mathrm{norm}}$ の分布

に，最小 2 乗法によって $\Delta(n)$ を n の 1 次式で近似した:

$$\Delta(n) = -0.00034n + 0.48117\,. \tag{11}$$

さらに，実験から得られた $\mathcal{HD}_{\mathrm{norm}}(x,y)$ の分布を図 2 に示す．ただし，ここでは，正規化ハミング距離率のスカラー倍 $\mathcal{HD}'_{norm}(x,y) = \dfrac{\mathcal{HD}_{\mathrm{norm}}(x,y)}{\sqrt{\lambda}}$ の分布を示している．式 (9), (10) より，

$$\mathcal{HD}'_{\mathrm{norm}}(x,y) = \frac{\big(\mathcal{HD}(x,y) - \Delta(n)\big)\sqrt{n}}{\sqrt{\Delta(n)(1-\Delta(n))}}$$

である．$\mathcal{HD}_{\mathrm{norm}}$ の代わりに $\mathcal{HD}'_{\mathrm{norm}}$ を用いた理由は λ が未知のままでも実験できるためである [*2]．$\mathcal{HD}'_{\mathrm{norm}}$ と $\mathcal{HD}_{\mathrm{norm}}$ はスカラー倍の違いしかないので，どちらを用いてもその照合アルゴリズムの認証精度と安全性は等しい．正規化ハミング距離率 $\mathcal{HD}'_{\mathrm{norm}}(x,y)$ によって判定するとき，FRR = FAR(= EER) (Equal Error Rate) はおおよそ 2.8% となった．第 4 節で述べたように，MNM アルゴリズムに対しては，すべてのテンプレートと「一致」と判定されるユニバーサル・ウルフが存在する [3]．また，森田ら [4], [10] は，MNM アルゴリズムを実装し，ユニバーサル・ウルフとなるようなウルフ人工物を作成し，実験によって FAR = 1.65%，FRR = 1.66%，WAP $\geq$ 92.5% となることを示した．

そこで，本稿提案の指静脈照合アルゴリズムに対して，森田ら [4], [10] のウルフ人工物を提示して抽出された特徴情報を用いた照合実験を行った．使用したウルフ人工物から抽出された特徴情報 w を図 3 に示す．黒，白，灰色で示されたビットがそれぞれ，静脈領域 ($w_i = 0$)，背景領域 ($w_i = 1$)，あいまい領域 ($w_i = null$) を表す．このウルフに対する誤一致率は 0% であり，WAP の下界は十分小さい値に抑えられた．よって，提案照合アルゴリズムは，あいまい領域 (非有効ビット) の数をコントロールして誤一致率を増加させようとするウルフに対して，ある程度の安全性を有することが示された．今後は，より多くのサンプル数に対する実験よって，信頼性の高い評価を行うことが課題である．

*2　前節の仮定から $\mathcal{HD}'_{\mathrm{norm}}(x,y)$ の分布は，平均 0，分散 λ の正規分布で近似される．

図 3　ウルフ画像

7. まとめ

本論文では，より一般の特徴情報のハミング距離を類似度として判定する照合アルゴリズムに対して適用可能な，証明可能な安全性を持つ効率の良い照合アルゴリズムを提案した．

まず，登録時と認証時の特徴情報 x, y に対して有効ビット間のハミング距離率 $\mathcal{HD}(x,y)$ を定義する．MNM アルゴリズムで用いられたミスマッチ率 R_m と $\mathcal{HD}$ を比較すると，ミスマッチ率 R_m では，あいまい領域を分母に含んでいるため，非有効ビットのみの特徴情報をもつサンプルがユニバーサル・ウルフとなってしまう．そこで，分母のあいまい領域を取り除き，$\mathcal{HD}$ の値で判定をする．また，Daugman の初期のアルゴリズムである $\mathrm{HD}_{\mathrm{raw}}$ と $\mathcal{HD}$ は同じである．しかしながら，有効ビット間のハミング距離率の値で判定をすると，依然として有効ビット数をコントロールするウルフ攻撃に対して脆弱である．Daugman アルゴリズムは，照合で有効となるビットの数に応じて判定閾値を変える (照合スコアを正規化する) ことで，ウルフ攻撃（照合に用いる有効ビット数をコントロールするウルフ攻撃）に対して証明可能な安全性が達成されている効率の良いアルゴリズムの具体例である．そこで，Daugman アルゴリズムを拡張するかたちで，ハミング距離率を用いたウルフ安全な照合アルゴリズムを提案する．さらに，提案アルゴリズムを MNM アルゴリズムに適用し，その認証精度と MNM アルゴリズムにおけるユニバーサル・ウルフを使った攻撃実験を行い，ウルフ攻撃に対する安全性を実験で評価した．その結果，提案アルゴリズムを適用しない場

合の誤一致確率が 92.5% であるのに対し，提案アルゴリズム提供後の誤一致確率 0% となり，提案アルゴリズムがある種の強いウルフ攻撃に対して安全であることが確かめられた．今後は MNM アルゴリズムに強力なウルフの画像を多数確保し，提案方式における信頼性の高い WAP を求めることが課題である．

参考文献

[1] J. Daugman：How iris recognition works, IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 21-30, 2004.
[2] J. Daugman : Probing the Uniqueness and Randomness of Iriscodes : Results From 200 Billion Iris Pair Comparisons, Proc. of the IEEE, vol. 94, No. 11, pp. 1927-1935, 2006.
[3] M. Inuma, A. Otsuka and H. Imai : Theoretical framework for construction matching algorithms in biometric authentication systems, Proc. of International Conference on Biometrics 2009 (ICB 2009), LNCS 5558, pp. 806-815, 2009.
[4] Ryogo Morita, M. Inuma, A. Otsuka and H. Imai : Security evaluation of a finger vein authentication algorithm against the wolf attack, Symposium on Biometrics, Recognition and Authentication 2013(SBRA2013), pp. 13-18, 2013
[5] M. Une, A. Otsuka and H. Imai : Wolf Attack probability: A Theoretical Security Measure in Biometrics Based Authentication Systems, The institute of Electronics, Information and Communication Engineers Trans. on Info. and Sys. 2008, E91-D(5)
[6] N. K. Ratha, J. H. Connell, and R. M. Bolle : Enhancing security and privacy in biometrics-based authentication systems, IBM Syst. J. 40, pp. 614-634, 2001
[7] 三浦直人，長坂晃朗，宮武孝文 : 線追跡の反復試行に基づく指静脈パターンの抽出と個人認証への応用，電子情報通信学会論文誌 D Vol. J86-D2 No. 5, pp. 678-687, May 2003.
[8] 渡辺直彦，繁富利恵，美添一樹，宇根正志，大塚玲，今井秀樹 : 指静脈パターン照合アルゴリズムにおけるユニバーサル・ウルフ，Proc of CSS2006, pp. 621-626, 2006.
[9] 渡辺直彦，繁富利恵，美添一樹，宇根正志，大塚玲，今井秀樹 : 指静脈パターン照合アルゴリズムにおけるユニバーサル・ウルフ -特徴抽出過程を含めた考察-，SCIS2007, 3F3-3, Jan 2007.
[10] 森田 遼伍，井沼 学，大塚 玲，今井 秀樹 : 静脈認証模擬システムへのウルフ攻撃に対する安全性評価，2014 年暗号と情報セキュリティシンポジウム，2014.