Compressed Sensing に基づく生体情報秘匿化センサの生体情報秘匿性向上に関する研究

浦辺　卓矢†　　鈴木　裕之†　　小尾　高史†　　大山　永昭†

†東京工業大学像情報工学研究所
226-8503 神奈川県横浜市緑区長津田町 4259
hiroyuki@isl.titech.ac.jp

あらまし 我々はCompressed Sensing（CS）と呼ばれる信号復元手法を応用することにより，秘匿化された静脈画像を取得可能な撮像システムとその観測データを用いた生体認証手法を提案している．この手法では，照合の際に一旦静脈画像を復元しているが，より安全な生体認証を実現するためには，静脈画像を秘匿化した状態で照合できることが望ましい．そこで本稿では，物体信号の順番をランダムに入れ替える置換行列を導入することにより，静脈画像を秘匿化した状態で照合可能な認証手法を提案する．計算機実験の結果，静脈画像を復元して照合を行う場合と比べて若干の照合精度の劣化はあるが，妥当な照合精度を有することを示した．

A study on improvement of security of secure biometrics sensor based on compressed sensing

Takuya Urabe†　Hiroyuki Suzuki†　Takashi Obi†　Nagaaki Ohyama†

†Imaging Science & Engineering Laboratory, Tokyo Institute of Technology
4259 Nagatsutacho Midoriku Yokohama, Kanagawa
226-8503, JAPAN
hiroyuki@isl.titech.ac.jp

Abstract We have proposed a biometric authentication method using the imaging system that is based on Compressed Sensing. In this approach, we can acquire a transformed vein image, but there is an issue that we restore the raw vein image in the process of verification. To address this issue, we propose a novel authentication method that we can verify a vein image in the transformed space from which it is difficult to restore the original vein image by introducing the permutation matrix for randomizing the object signal. The Experimental evaluation shows that our method has reasonable accuracy although it has a little degradation of accuracy in comparison with the case of the conventional method that uses a raw vein image.

1　はじめに

IC カードや暗証番号等による個人認証が広く用いられているが，盗難や紛失，偽造，不正譲渡等の危険性がある．これに対し，生体認証は盗難や紛失が生じにくく，技術の進歩と社会情勢の変化により急激な普及を見せている．しかし，生体情報は一旦漏洩するとパスワードや鍵のように容易に破棄･更新することができず，また個人のプライバシに関わる情報であることから，厳重な管理が必要となる．この課題を解決するための技術として，生体情報を別の情報へと変換することにより元の生体情報が分からない状態での照合を可能とし，また生体情報が漏洩した場合でも登録情報の破棄・更新が可能なテンプレート保護型生体認証と呼ばれる認証

技術[1-3]が注目されている．

一方，スパース性（零要素が多いという性質）を持つ高次元の信号を低次元の観測データから復元する事ができる Compressed Sensing（CS）と呼ばれる信号復元の手法[4]が注目され，様々な分野での応用が期待されている．CS に基づく信号復元は，推定するスパース信号に対する L1 ノルム最小化を行うことで，サンプリング定理の限界を超えるデータ数での信号復元を可能とし，大幅な観測データの圧縮が実現できる技術であるが，単に観測データ数を削減できるだけでなく，観測系を表現する行列（観測行列）を暗号の鍵とする暗号化・復号技術としての応用についても研究が進められている[5]．CS に基づく撮像システム[6]を用いて生体画像を撮影することを考えると，復号の鍵となる観測行列を知らない限り，取得された観測データから元の生体情報を復元できないため，この撮像システムで取得した観測データは破棄・更新が可能（キャンセラブル）な登録生体情報となりうると考えられる．

そこで我々は先行研究[7]において，CS に基づく撮像システムで取得した観測データをキャンセラブルな登録生体情報として利用する，キャンセラブル生体認証の枠組みを提案している．しかし，先行研究では照合の際に生体画像を復元しており，生体情報保護の観点で安全性が不足している．本稿では，先行研究での信号復元に用いる観測行列に，信号の要素をランダムに並べ替える置換行列を組み込むことにより，生体画像を秘匿化した状態で照合を行うシステムを提案する．

2 Compressed Sensing

N 次元信号$\mathbf{X}$ に対して，M 個の線形観測 $\mathbf{y} = (y_1, \cdots, y_M)^T$が次式により得られたとする．

$$\mathbf{y} = \mathbf{\Phi X} \tag{1}$$

ここで，$\mathbf{\Phi}$は$\mathrm{M} \times \mathrm{N}$ のランダムな値で構成される行列である．観測信号$\mathbf{y}$ から元信号$\mathbf{X}$ を復元する問題は，一般に線形逆問題と呼ばれ，$\mathrm{M} \geq \mathrm{N}$ を満たさなければ正しい解は得られない．しかし CS に基づく信号復元では，$\mathrm{M} < \mathrm{N}$ の場合でも，元信号$\mathbf{X}$ のほとんどの要素が 0 （スパース） であるならば，(1)式を制約条件とし，推定する元信号$\mathbf{X}$ の L1 ノルムを最小化することで，観測信号$\mathbf{y}$ からでも元信号$\mathbf{X}$ を高い確率で復元できるという手法である．つまり，推定信号を$\hat{\mathbf{X}}$ とすると，

$$\mathrm{Minimize}\left\|\hat{\mathbf{X}}\right\|_1 \text{ subject to } \mathbf{y} = \mathbf{\Phi}\hat{\mathbf{X}} \tag{2}$$

を解くことで元信号を推定することができる．L1 ノルム最小化の問題は，線形計画法の様々な解法を適用して解を得られることが知られている．

文献[5]では，(1)式で用いた観測系を表す行列$\mathbf{\Phi}$を暗号の鍵とみなし，観測信号を元信号の暗号化データとして扱う手法について議論しており，暗号化手法として十分機能することが示されている．

3 Compressed Sensing に基づく生体情報秘匿化センサ

ここでは，CS に基づく撮像システムと，このシステムで得られる観測データを利用した生体認証システム[7]の基本原理について述べる．

このシステムで用いられる生体情報取得センサは，物体光にランダムな強度変調を施すための強度変調フィルタ（DMD）と，フィルタを透過した光の強度積分値を取得するフォトディテクタで構成される．このセンサで取得した生体情報（CS で暗号化された観測データ）を認証サーバへ登録する生体情報とする（図 1）．

観測データの取得方法としては，まずユーザーが保有する秘密情報をシードとして，M 種類のランダムな強度変調フィルタパターンを生成しておく(図 1-①)．次に，強度分布$\mathbf{X}$ の生体画像に対し，フィルタを透過し集光された光の強度積分値をフォトディテクタで取得する(図 1-②)．この処理におけるフィルタの入力パターンを時間変化させて得られる M 個の光強度積分値系列を観測データ（暗号化された生体情報）$\mathbf{y}$ とする．

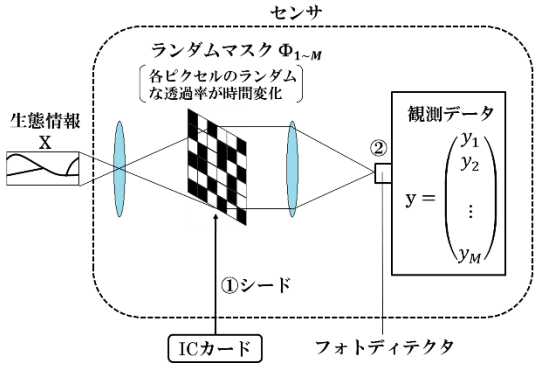

図 1　CS に基づく撮像システム

照合方法は，認証サーバ内で登録用，照合用の生体画像をそれぞれの観測データから一旦復元し，復元した生体画像同士でマッチングを行う．

得られた観測データから信号復元を行う方法としては，線形変換$\boldsymbol{\Psi}$ により$\mathbf{X}$ をスパースな信号 $\mathbf{S}\,(=\boldsymbol{\Psi}\mathbf{X})$ へ変換可能であることを前提とし，観測データ$\mathbf{y}$ と行列$\boldsymbol{\Phi}\boldsymbol{\Psi}^{-1}$から L1 ノルム最小化によってまず$\mathbf{S}$ を推定する．そして，推定したスパース信号を$\hat{\mathbf{S}}$ とすると，復元される生体画像$\hat{\mathbf{X}}$ は，$\hat{\mathbf{S}}$ に対して線形逆変換$\boldsymbol{\Psi}^{-1}$を施すことによって以下のように求めることができる．

$$\hat{\mathbf{X}} = \boldsymbol{\Psi}^{-1}\hat{\mathbf{S}} \tag{3}$$

このとき，観測行列$\boldsymbol{\Phi}$が登録時と照合時で同一であれば，元の生体画像が復元されるが，$\boldsymbol{\Phi}$ が誤っている場合には，ランダムな画像が復元される．照合を行う際は，まず照合用として取得した観測データ$\mathbf{y}'$ と登録情報$\mathbf{y}$ に対し，ユーザーによって入力された復号用の鍵$\boldsymbol{\Phi}$を用いてそれぞれスパース信号$\mathbf{S}'$ と$\mathbf{S}$の推定を行い，線形逆変換$\boldsymbol{\Psi}^{-1}$ を施すことで生体情報$\mathbf{X}'$ と$\mathbf{X}$ を復元し，それらのマッチングをとることで照合を行う．

照合方法の手順をまとめると，次のようになる．

Step1.　認証サーバに照合用の観測データ$\mathbf{y}'$ と観測行列$\boldsymbol{\Phi}$を送信する
Step2.　認証サーバにおいて$\mathbf{y}'$と$\boldsymbol{\Phi}\boldsymbol{\Psi}^{-1}$が既知となるので，CS により$\hat{\mathbf{S}}'$ を推定する
Step3.　$\hat{\mathbf{X}}' = \boldsymbol{\Psi}^{-1}\hat{\mathbf{S}}'$ により生体画像$\hat{\mathbf{X}}'$ を復元する
Step4.　Step2.から Step3.で$\mathbf{y}'$ から$\hat{\mathbf{X}}'$ を復元したように，登録情報$\mathbf{y}$ から生体画像$\hat{\mathbf{X}}$ を復元する
Step5.　$\hat{\mathbf{X}}'$ と$\hat{\mathbf{X}}$ でマッチングを行う

このシステムの特徴としては，観測データをセンサで取得した時点ですでに生体情報が秘匿化されていること，またキャンセラブル化した生体情報（観測データ）が元の生体情報と比較して非常に小さくなることが挙げられる．

一方，問題点としては，登録されている観測データ$\mathbf{y}$ からは，秘密情報である観測行列$\boldsymbol{\Phi}$ を知らない限り生体情報の推定は困難であるが，認証時には生体画像$\mathbf{X}$ を復元して照合を行っているため，認証サーバ内に秘匿すべき生体情報$\mathbf{X}$ が存在することになる．そのため，悪意を持った管理者等による生体情報漏洩のリスクが残る．

4　提案システム

本稿では，先行研究における問題点を解決する手法として，CS に基づく撮像システムで取得した観測データを用いて推定したスパース信号に対して，スパース信号の要素をランダムに並べ替える置換行列を導入して，生体画像を秘匿化した状態で照合を行うシステムを提案する．

4.1　置換行列の導入

先行研究では CS を用いてスパース信号 $\mathbf{S}\,(=\boldsymbol{\Psi}\mathbf{X})$ を推定し，生体画像$\mathbf{X}$ で照合を行っていたが，提案システムでは元の生体画像$\mathbf{X}$ で比較は行わず，以下の式で定義されるスパース信号$\mathbf{S}_{\boldsymbol{R}}$ を推定し，このスパース信号$\mathbf{S}_{\boldsymbol{R}}$ で照合を行う．

$$\mathbf{R}\boldsymbol{\Psi}\mathbf{X} = \mathbf{S}_{\mathbf{R}} \Leftrightarrow \mathbf{X} = \boldsymbol{\Psi}^{-1}\mathbf{R}^{-1}\mathbf{S}_{\mathbf{R}} \tag{5}$$

置換行列 $\mathbf{R}$ は，図 2 に示すようにスパース信号$\mathbf{S}$の要素の順番をランダムに並べ替える行列であり，要素の値は変更しない．

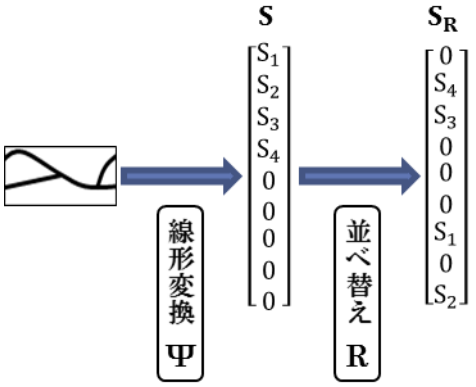

図 2　CS により推定するスパース信号の模式図

提案システムにおける照合方法の手順をまとめると次のようになる.

Step1.　認証サーバに照合用の観測データ$\mathbf{y}'$と行列$\mathbf{\Phi\Psi^{-1}R^{-1}}$を送信する

Step2.　認証サーバにおいて$\mathbf{y}'$と$\mathbf{\Phi\Psi^{-1}R^{-1}}$が既知となるので, CS により$\widehat{\mathbf{S_R}'}$を推定する

Step3.　Step2.から Step3.で$\mathbf{y}'$ から$\widehat{\mathbf{S_R}'}$を推定したように, 登録情報$\mathbf{y}$ からスパース信号$\widehat{\mathbf{S_R}}$を推定する

Step4.　$\widehat{\mathbf{S_R}'}$ と$\widehat{\mathbf{S_R}}$ でマッチングを行う

4.2　生体画像の復元困難性

提案システムにおける生体画像の復元困難性について述べる.

攻撃者が$\mathbf{S_R}$ のみ入手できると仮定した場合, 式(4)を用いて生体画像$\mathbf{X}$ を復元するには置換行列 $\mathbf{R}$ を特定する必要がある. $\mathbf{R}$ は N 個の要素を持つ信号$\mathbf{S}$ の要素の順番を並べ替える行列であり，その候補数は

$$ {}_{N}P_{N} = N! \tag{6}$$

である. ここで N の値が例として$N = 4096$ であるとすると,

$$ N! = 3.64 \times 10^{13019} \tag{7}$$

となる. これより，$\mathbf{R}$ の候補数は極めて大きくなるので，$\mathbf{R}$ を特定することは非常に困難と考えられる.

5　実験

提案システムの有効性を確認するため，商用の指静脈センサで取得した指静脈画像を用いて, CS に基づく撮像システムで得られる観測データを擬似的に生成し，照合実験を行った. 実験に用いた指静脈画像は，(株)フィット・デザイン・システム社製の指静脈センサ FVD-560 を用いて撮影し，画像サイズ 256×64 pixel で取得した指静脈画像を 32×128 pixel(全 4096 pixel)へ圧縮して利用した.

5.1　照合精度実験

提案システムが先行研究と比較してどの程度の照合精度を有しているのかを計算機実験によって調査した.

実験に用いた指静脈画像は，10 人分の指静脈画像を 1 人につき 5 枚用意し（計 50 枚），同一人物の照合を 100 パターン，異なる人物の照合を 2250 パターンで行った. 観測データの要素数 M は, $M = 400,\ 800,\ 1600,\ 2400$ の 4 種類で実験し，指静脈画像をスパース信号に変換するための線形変換には 2D-Cosine 変換$\mathbf{\Psi_C}$ を用いて，本人拒否率（FRR）と他人許容率（FAR）を求め，登録者本人と他人を判定する閾値を変化させることで ROC カーブを求めた. 他人の照合については，他人が ID を手に入れて認証を行った場合（Total Performance Testing ; TPT），トークンと ID の両方を手に入れて認証を行った場合（Biometric Performance Testing ; BPT）の 2 つを想定し，実験を行った. 比較として，先行研究での認証手法（一旦静脈画像を復元し，照合を行う手法）で得られる照合結果との比較を行った.

先行研究のシステムでの照合の際には，認証サーバ内で復元した指静脈画像同士で正規化相互相関（NCC）に基づくパターンマッチングを適用し，提案システムでの照合の際には，推定したスパース信号同士で NCC による照合を行った.

TPT の実験結果について述べる. 図 3，図 4

は先行研究と提案システムの ROC カーブであり，図5は観測データ数に対する Equal Error Rate（EER）の推移である．先行研究では観測データ数が増えるにつれて EER が減少し，観測データ数が 1600 で EER が 0 %に収束するのに対して，提案システムでは EER が常に 0 %となった．先行研究で推定されるスパース信号 $\mathbf{S}$ は，登録者本人と他人のどちらの場合においても静脈画像を 2D-Cosine 変換した変換係数に等しいのに対して，提案システムで推定されるスパース信号 $\mathbf{S}_R$ は $\mathbf{S}$ の要素の順番を並べ替え，本人と他人では変換係数と対応する要素の順番が異なる．そのため，提案システムではスパース信号の要素の値だけでなく，順番も照合結果に影響するので，EER が常に 0 %となったと考えられる．

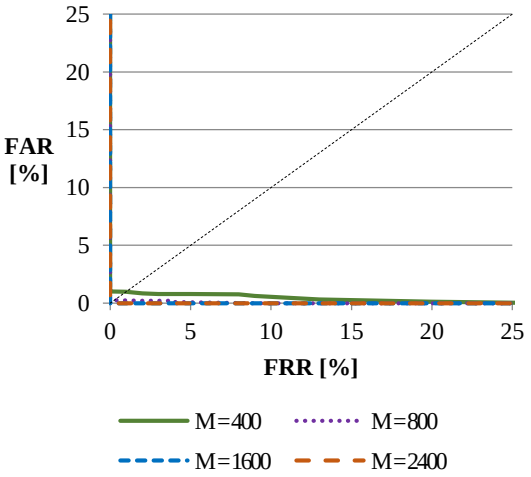

図 3　先行研究における TPT の ROC カーブ

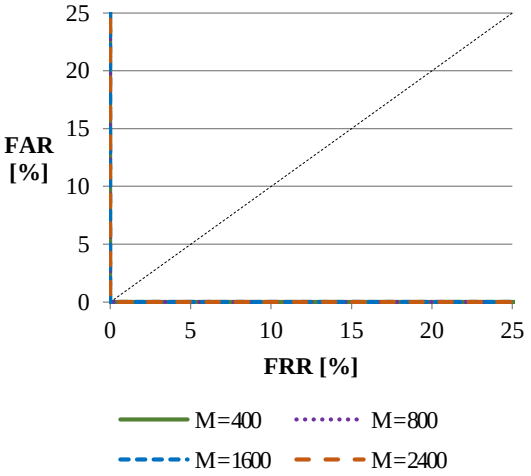

図 4　提案システムにおける TPT の ROC カーブ

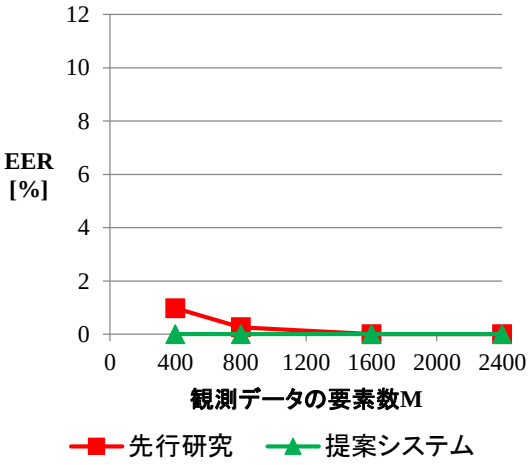

図 5　TPT の EER

次に，BPT の場合の実験結果について述べる．図 6，図 7 は先行研究と提案システムの ROC カーブであり，図 8 は観測データ数に対する EER の推移である．全ての観測データ数において，提案システムは先行研究より EER が大きい結果となった．これは，先行研究では画像同士の照合を行い，センサで指静脈を撮影する際の登録時と認証時の指の位置の違いの影響を抑制できるのに対して，提案システムではスパース信号同士で照合を行うので，指の位置の違いによる影響が大きいことが原因であると考えられる．

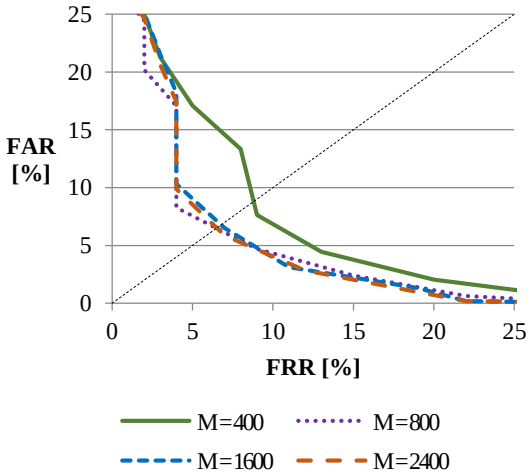

図 6　先行研究における BPT の ROC カーブ

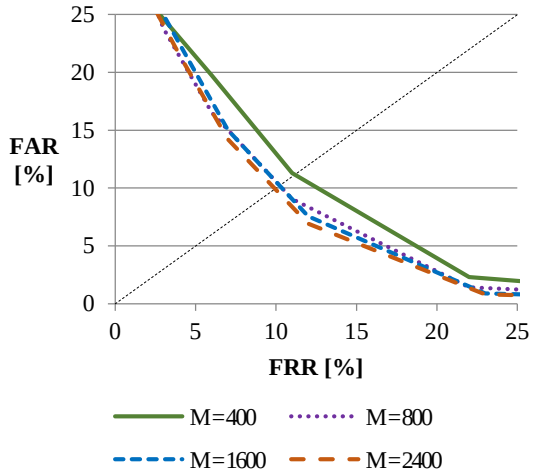

図 7　提案システムにおける BPT の ROC カーブ

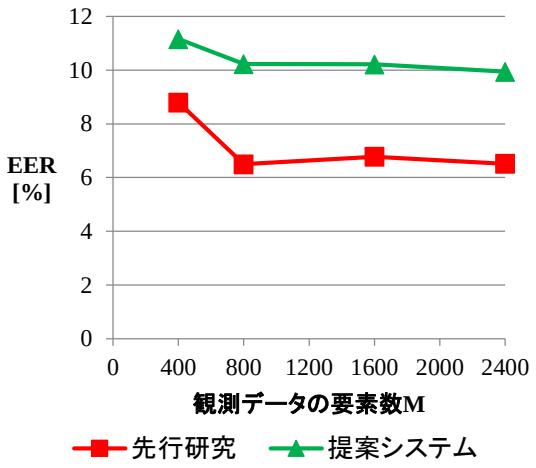

図 8　BPT の EER

6　まとめ

本稿では，秘匿化された静脈画像を取得可能な CS に基づく撮像システムとその観測データを用いた生体認証システムにおいて，静脈画像を秘匿化した状態で照合を行うことが可能な認証手法を提案した．計算機実験を行った結果，BPT の場合，静脈画像を復元して照合を行う場合と比べて若干の照合精度の劣化はあるが，妥当な照合精度を有することを示した．

今後の課題としては，提案システムの照合精度を上げるため，センサで指静脈を撮影する際の登録時と認証時の指の位置の違いの影響を抑制できる照合方法の検討が必要である．また，提案システムでは置換行列 **R** を組み込むことにより照合の際の生体情報の秘匿化をしたが，推定したスパース信号の値が大きい要素に対して **R** の並べ替え規則を解析することにより，静脈画像が容易に解読されることが懸念される．そのため，照合の際の生体情報の秘匿化についても更に検討する必要がある．

参考文献

[1] N. K. Ratha, J. H. Connelland R. M. Bolle, “Enhancing security and privacy in biometrics based authentication systems”, IBM Systems Journal, Vol. 40, No. 3, pp. 614–634 (2001).

[2] Juels A., Sudan M., “A fuzzy vault scheme”, proc. IEEE Int. Symp. Inf. Theory, p.408 (2002).

[3] 高橋健太, 比良田真史, “相関不変ランダムフィルタリングを用いたキャンセラブル指紋認証”, SCIS2008, (2008).

[4] E. J. Candès and M. B. Wakin, “Iroduction to compressive sampling”, inIEEE Signal Processing Magazine, vol. 25, no. 2, pp. 21-30 (2008).

[5] Yaron Rachlin and Dror Baron, “The Secrecy of Compressed Sensing Measurements”, in IEEE Communication, Control, and Computing, 2008 46th Annual Allerton Conference on, pp. 813-817(2008).

[6] Michael Wakin, et.al., “An Architecture for Compressive Imaging”, Proc. International Conference on Image Processing(ICIP) 2006, (2006).

[7] 鈴木理道, 鈴木裕之, 小尾高史, 大山永昭, “Compressed Sensing に基づく生体情報秘匿化センサーに関する研究”, SCIS2012 (2012)