M_048

生体情報を鍵とするチャレンジ&レスポンス型認証
Challenge-Response authentication based on biometric information

森浩典† 鈴木裕之‡ 小尾高史† 山口雅浩‡ 大山永昭‡
Hironori Mori† Hiroyuki Suzuki‡ Takashi Obi† Masahiro Yamaguchi‡ Nagaaki Ohyama‡

1．はじめに

近年，セキュリティニーズの高まりに伴い，個人認証をより安全に行う方法として，人間の身体的特徴を用いて認証を行う生体認証が普及しつつある．現在の生体認証は建物の入退室管理や銀行 ATM の専用線等の閉じた世界の利用に留まっており，インターネットのようなオープンな世界でのオンライン認証としては利用されていないのが現状である．

生体情報をオープンな世界で利用するためには，ネットワーク上での生体情報の保護が重要である．そのためには，一時的な認証情報と暗号技術を組み合わせたネットワーク認証技術であるチャレンジ&レスポンス型認証が望ましい．しかし，取得する生体情報には揺らぎがあるため，生体情報から一意なレスポンスコードを生成することが困難であるという問題がある．また，生体情報は一度盗まれてしまうと取替えがきかないか，もしくは取替えの回数が限られ，パスワードや暗号鍵などのように容易に破棄・更新をすることができない．

本研究では，生体情報を利用したチャレンジ&レスポンス型認証を実現するために，画像の相関演算をベースとする認証手法を利用して上記の問題を解決する手法を提案する．

2．生体情報を利用したチャレンジ&レスポンス型認証

生体情報を利用したチャレンジ&レスポンス型認証を実現するには，以下の要件を満たす必要がある．

(1) 認証に用いるネットワーク上での生体情報の保護
(2) チャレンジコードから生体情報を用いて一意なレスポンスコードを生成可能
(3) 登録生体情報から元の生体情報は復元困難
(4) 登録生体情報の変更が何度でも可能

要件(3)，(4)を満たす技術としてキャンセラブルバイオメトリクス(Cancelable Biometrics)と呼ばれるテンプレート保護技術が提案されている[1]．キャンセラブルバイオメトリクスでは，生体情報と本人のみが知り得る付加情報を用いて，元の生体情報への復元が困難な別の情報へ変換したものをテンプレートとして登録する．そのため，登録テンプレートが漏洩した場合でも，付加情報の変更により，登録テンプレートの変更が何度でも可能である．しかしこれまでに提案された技術は，要件(1)，(2)を満たすことができない．本研究ではキャンセラブルバイオメトリクスの一手法として，生体情報の他に，個人を識別する別の情報をキー画像として用いた相関演算によるキャンセラブルな認証[2]を利用し，この手法をチャレンジ&レスポンス型認証へ応用することで，(1)～(4)の要件を満たすシステムを提案する．

†東京工業大学大学院総合理工学研究科
‡東京工業大学像情報工学研究施設

3．相関演算を用いたキャンセラブル生体認証

3.1 多重位相限定相関による個人認証

本研究では，位相限定相関(Phase Only Correlation :POC)を多重的に用いることでキャンセラブルな認証を実現する．POC は，振幅成分を一定にしたフーリエ像同士を乗算し，それを逆フーリエ変換することにより得られ，画像が類似している場合は鋭いピークとなり，それ以外はランダムパターンを生成する．特に指紋画像の POC は，本人と他人を識別するのに十分な性能を有することが示されている．

登録時には，生体情報とキー画像の POC 画像をテンプレートとして登録し，照合時は，生体情報とキー画像から生成した POC 画像と登録テンプレートとの畳み込み積分を行う（図 1）．このときの畳み込み積分画像を X とすると，(1)式のようになる．

一方，指紋画像同士の POC 画像とキー画像同士の POC 画像との畳み込み積分画像 Y は(2)式のように書けるが，位相限定相関および畳み込み積分の結合則・交換則により，X と Y は等価となる．ここで，登録テンプレートと照合用 POC 画像がそれぞれ同一のペアから生成されたものである場合を考えると，Y はピーク画像同士の畳み込み積分となるため，鋭いピークが現れるが，組合せが一致しない場合はピークが現れない．よって，X の強度パターンのピーク値を見ることによって本人判定が可能である．

$$X = (A(x,y) \text{☆} B(x,y)) * (A'(x,y) \text{☆} B'(x,y)) \quad (1)$$

$$Y = (A(x,y) \text{☆} A'(x,y)) * (B(x,y) \text{☆} B'(x,y)) \quad (2)$$

$$X = Y \quad (3)$$

$A(x,y)$: 登録用指紋画像，$A'(x,y)$: 照合用指紋画像
$B(x,y)$: 登録用キー画像，$B'(x,y)$: 照合用キー画像
☆: 位相限定相関，*: 畳み込み積分

登録及び照合用 POC 画像からは，元の生体情報およびキー画像を復元することは困難であり，また，登録 POC 画像が漏洩した場合には，キー画像の変更により，登録画像を何度でも変更することが可能である．さらに，キー画像は，生体情報や PASS コード等，様々な画像を用いて実現可能であり，個人情報の選択性として高い自由度を有する個人認証の実現が期待できる．

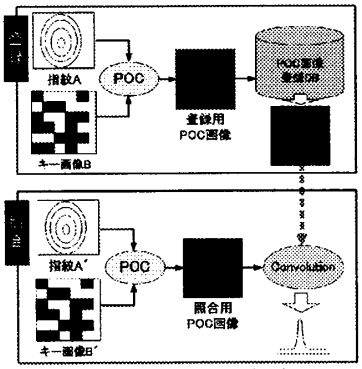

図 1 提案手法の概念

3.2 実験

上記の認証手法の精度を評価するための実験を行った．今回は入力として，指紋および4桁のパスワードを用いた．4桁のパスワードからは乱数を発生させ，ランダムな画像を生成し，キー画像として登録・照合に用いた．指紋画像については，8人の被験者の右手または左手の人差し指から，登録用に4枚，認証用に2～6枚の指紋画像を取得し，実験に用いた．画像サイズは，128×128，256×256，512×512[pixel]の3種類を用意し，それぞれについて実験を行った．また，POCは回転の影響を大きく受ける性質があるため，認証時には，取得した指紋画像を±9°の範囲で3度ずつ回転させながら照合を行った．

画像サイズが512×512[pixel]のときの精度評価結果を図2に示す．横軸はしきい値，縦軸はFRR(False Rejection Rate:本人拒否率)，FAR(False Acceptance Rate)を示し，各曲線は，しきい値を変化させたときのFRRとFARの変化を表す．同図より，適切な閾値を設定することで，本人拒否・他人受入が共に生じないような認証を実現することが可能である．他の2種類の画像サイズの場合についても同様の結果が得られた．

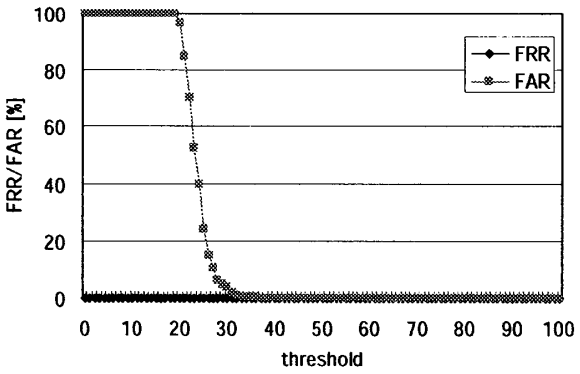

図2 実験結果

また，指紋とパスワードを入力した時から本人他人判定の結果を判定するまでの処理時間についても計測を行った．Microsoft Windows XP Professionalを搭載したパーソナルコンピュータ（主記憶：1.99GB，CPU：Intel Pentium D 2.80GHz）で実装したときの処理時間の測定結果を表1に示す．結果より，512×512[pixel]の場合は非常に処理時間が大きいが，128×128，256×256[pixel]の場合は既存の認証システムに比べて大きく劣ることはなかった．今後の研究によっては十分実用的な処理時間を得られると考えている．

表1 画像サイズと処理時間

画像サイズ[pixel]	128×128	256×256	512×512
処理時間[s]	4	13	50

4. チャレンジ&レスポンス型認証への適用

前節で提案したキャンセラブルな生体認証を拡張することで一時的な情報を用いたオンライン認証であるチャレンジ&レスポンス型認証を実現する．

3.1で述べたキャンセラブル認証手法は，2つの画像を多重に相関演算させた手法であるが，さらにチャレンジコードを画像化させたものを多重化する．つまり，画像化した2つの個人情報と画像化したチャレンジコードの3つの画像のPOCをレスポンスコードとし，レスポンスコードの生成をユーザ側，認証サーバ側の両者で行い，生成したレスポンスコード同士の畳み込み積分を行うことで照合を行う．この手法により，第2節で述べた要件をすべて満たす認証が実現できる．

認証シーケンスを図3に示す．ユーザはあらかじめ，生体情報とキー画像のPOC画像を認証サーバに登録しておくこととする．認証時には以下の処理を行う．

① ユーザは認証サーバに認証要求を出す．
② サーバはチャレンジコードを生成してユーザに送信するとともに，チャレンジコードとユーザの登録画像との位相限定相関により，照合用画像を生成する．
③ ユーザは受け取ったチャレンジコードと，生体情報とキー画像から生成した個人識別画像との位相限定相関を行い，レスポンスコードとしてサーバに返信する．
④ サーバはレスポンスコードを受け取ると，照合用画像とレスポンスコードの畳み込み積分を行い，結果画像のピーク値をしきい値判定することで本人・他人を判定する．

以上の操作により，チャレンジ&レスポンス型認証を実現できる．

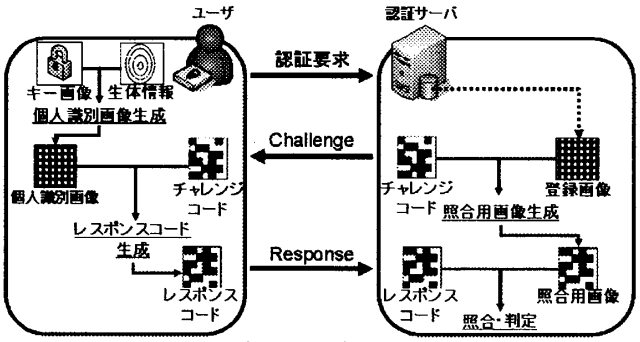

図3 チャレンジ&レスポンス型認証のシーケンス

5. まとめ

画像化した個人情報の多重相関演算を利用したキャンセラブルな生体認証を拡張することで，チャレンジ&レスポンス型認証へ応用可能なことを示した．提案手法を用いることで，ネットワークを介した生体認証を行うことができ，より便利なネットワークサービスを提供できると考えられる．

謝辞

本研究は，文部科学省科学研究費補助金若手研究（B）（課題番号:18760265）の助成により行われた．

参考文献

[1] N.K. Ratha, J.H. Connell, and R.M. Bolle, "Enhancing security and privacy in biometrics based authentication systems", IBM Systems Journal, Vol.40, No.3, pp.614-634, 2001

[2] 森ほか，"二つの個人識別情報を用いた相関演算によるキャンセラブルバイオメトリクス認証"，第53回応用物理学関係連合講演会，23a-E-Ⅲ(2006)，講演予稿集 pp.1075