様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２５年６月２１日現在

機関番号：１７３０１
研究種目：若手研究（Ｂ）
研究期間：2009～2011
課題番号：２１７６０２９７
研究課題名（和文）　ワンタイム顔画像認証によるネットサービス利用とプライバシ保護に関する実証的研究
研究課題名（英文）　Research for Privacy Protection and Network Service of One-Time Facial Authentication
研究代表者
上繁　義史（UESHIGE　YOSHIFUMI）
長崎大学・情報メディア基盤センター・准教授
研究者番号：00300666

研究成果の概要（和文）：
本研究は，遠隔での認証に用いる生体認証の研究開発を目的とし，生体情報のプライバシを保護しつつ，ネットワークセキュリティに配慮したシステムを目指した。要素技術となるワンタイム生体認証の実装モデルについて検討した。検討事項は（1）ディジタル画像におけるワンタイム変換を行う情報の種類，(2) ワンタイム変換を実現する写像系の構成方法の 2 点である。（1）については，復号画像を用いるのが適切との結論に至った。(2) については，フラクタル理論に基づく方法を検討してきたが，要件を満たしつつ実装が容易な変換方法を発見するには至らなかった。

研究成果の概要（英文）：
This research aimed at the system with considering network security and the privacy protection of biometric templates for the purpose of research and development of the remote biometric authentication system. The model of the one-time biometrics used as the component engineering was examined. There are two points of this investigation. First one is the kind of information of digital images for one-time mapping. Second one is suitable specification of one-time mapping for software. Using a decoding image resulted in the conclusion of being suitable, about the first one. About the second point, although the method based on fractal theory had been examined, mounting did not discover the easy conversion method, satisfying requirements.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００９年度	1,700,000	510,000	2,210,000
２０１０年度	700,000	210,000	910,000
２０１１年度	700,000	210,000	910,000
年度			
年度			
総　計	3,100,000	930,000	4,030,000

研究分野：工学
科研費の分科・細目：電気電子工学，通信・ネットワーク工学
キーワード：認証，プライバシ保護

１．研究開始当初の背景

近年，入出国管理や銀行ＡＴＭ等で生体認証の導入が進んでいる。これら技術は国際標準化活動の進展に伴い，オンラインバンキングのようなインターネット環境での適用が期待されている。

一方，生体認証において，照合に顔画像や指紋画像などの生体情報を直接用いるため，

一度漏洩すると再登録できないことが指摘されている．この問題の対策として，キャンセラブルバイオメトリクスが研究されている。これはテンプレートが漏洩しても，元の生体情報を復元できないことと，同じ生体情報を用いて新たなテンプレートを生成・登録できることが特徴である。

研究代表者は2006年に元の生体情報を認証が行われるたびに異なる変換を適用してテンプレートとする「ワンタイム生体認証」の概念を下記論文で提案した。

Yoshifumi Ueshige, Kouichi Sakurai, "A Proposal of One-Time Biometric Authentication", Proceedings of the 2006 International Conference on Security and Management (SAM 2006), CSREA Press, pp.78-83, (Jun. 2006)

これは同一利用者の認証であっても毎回異なるテンプレートデータで認証できる特長（ワンタイム性）をもつというものである。本手法の安全性について理論的検討を加えたものである。このアイデアを当時特許として申請していた。しかしながら，研究開始当初，ワンタイム生体認証，キャンセラブルバイオメトリクス共に理論段階の研究であり，具体的な実装方式についての研究には至っていないのが実情であった。

２．研究の目的

本研究は,オンラインバンキングのようなネットサービス等，遠隔での認証に使用可能な生体認証システムの研究開発を目的とした。この研究では，生体認証に特有な生体情報のプライバシを保護しつつ，ネットワークセキュリティの基盤技術としての生体認証の確立を目標としている．本申請において，研究代表者が特許出願した「ワンタイム生体認証」を適用する具体的なアルゴリズム，通信プロトコルについて研究し，プロトタイプの実装を行うことを企図した。

３．研究の方法

助成期間中に，以下の項目について研究を行う予定であった。

（１）ワンタイム生体認証による認証のアルゴリズム関する研究

ディジタル画像に適したワンタイム変換の形式について研究を行う。研究のポイントは以下の性質をもつ変換写像の生成アルゴリズムを理論的に確立することである。

① 画像の圧縮情報から直接変換する
② 変換された生体情報が照合の処理には利用できるが，元の生体情報に関する情報を一切取得できない

（２）ワンタイム認証プロトコルに関する研究

上記（１）と連動して研究を進める。本テーマでは，インターネットにてデータ伝送を行う部分，ＩＣカードと認証装置の通信部分について研究し，ワンタイム生体認証システムの具体的仕様の決定を目標とする。

（３）ワンタイム認証プロトコルの実装

上記（１）及び（２）の検討結果を受けて，プロトタイプの実装をおこなう。

（４）有効性の検証及び改良

実装の結果を受けて，安全性や精度面での有効性を検証し，システムの改良を行う。

４．研究成果

本研究では，図１のようなシステム構成及び処理を想定し，本システムの根幹であるワンタイム変換について研究を行った。

ワンタイム変換はたとえ同一人物の認証においても，毎回変化する必要がある。ワン

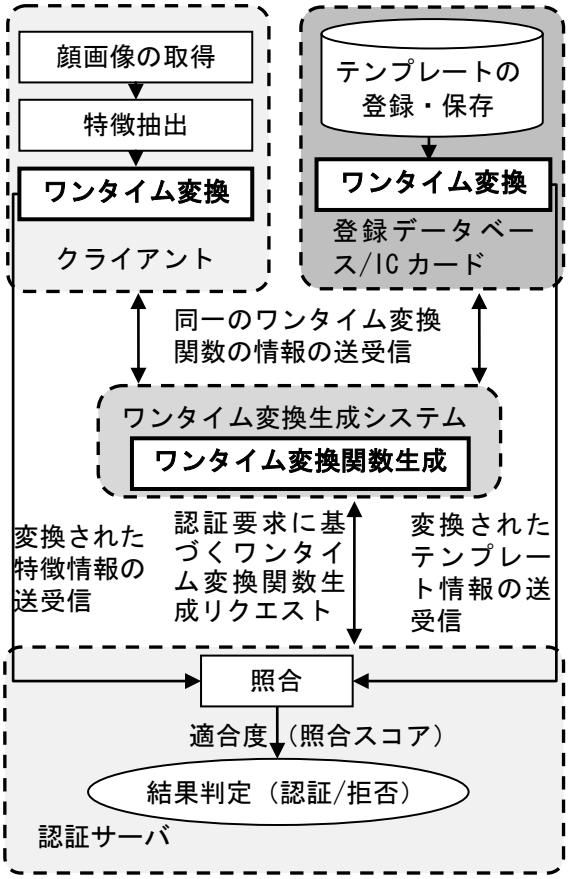

図１　ワンタイム生体認証システム構成と処理の流れの概要図

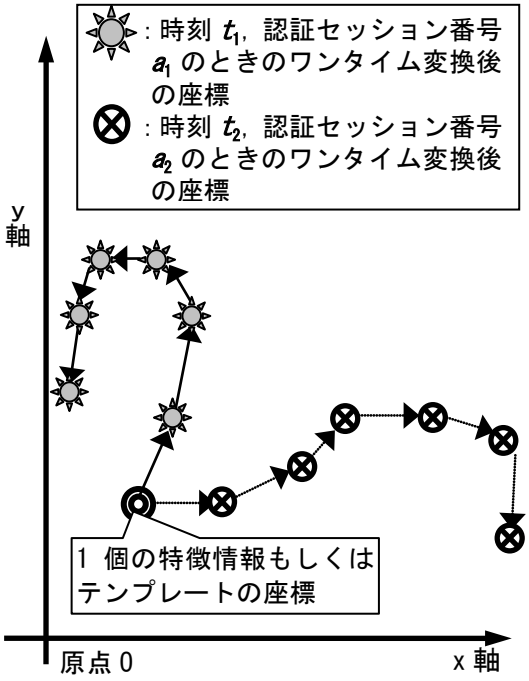

図 2　ワンタイム変換処理の概念

タイム変換において，攻撃者に盗聴された場合に，元のテンプレート情報を秘匿し，なおかつ不正取得したデータを用いた攻撃を不可能とすることが必須との考えから，以下の要件を満たす必要があると考えた。

（1）　特徴点やテンプレートの写像点から元の内容を予測することが不可能，もしくは極めて困難なこと（予測困難性）

（2）特徴点とテンプレート間の距離を保存できること，もしくは，適切な距離関数で評価が可能であること（距離保存性）

（3）ワンタイム変換に関する情報から特徴点とテンプレートに関する情報が抽出できないこと（一方向性）

上記の条件を全て満たすことは一般には困難と思われるが，図 2 の概念図に示すような変換が適しているものと考えた。ワンタイム変換の候補として，フラクタル理論における反復関数系やカオス写像のように何回も反復して変換を行う関数を想定した。例えば，カオス写像は変換点の軌道がパラメータと初期点に依存して大きく変化する性質がある。このような性質をもつ関数であれば，ワンタイム変換後の特徴点及びテンプレートを用いて，元の生体情報を抽出することが極めて困難となることが期待された。

また，認証を行うたびにパラメータを変更することによって，異なる複数の認証セッションを盗聴して，同一人物に関する変換点のデータを入手したとしても，盗聴者にはそれが同一人物から採取されたことを秘匿することができる。

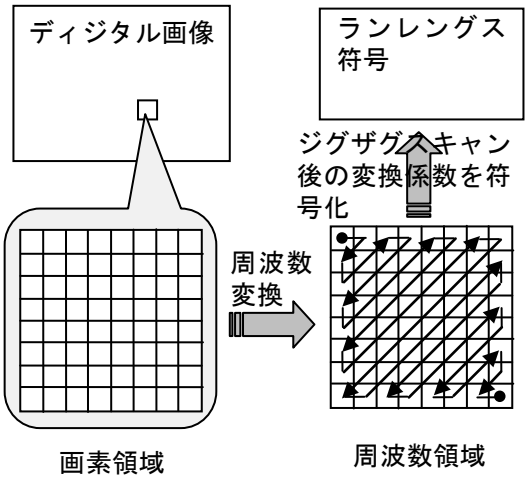

図 3　JPEG 方式の概念

前項で述べた研究代表者の論文にて検討した以上の理論に基づいて，実装のための理論化を行うべく，以下の 2 点について研究を行った。

（1）ディジタル画像におけるワンタイム変換を行う情報の種類

ディジタル画像の分野において，Web での利用やデジタルカメラで撮影した画像の保存など，一般的に流通していることと，多くの生体認証において，センサが取得した画像の保存形式として用いられることから，JPEG 形式を想定した。JPEG 形式の基本的な考え方として，図 2 のように，8 画素×8 画素のブロック単位に対して数学的な周波数変換を施し，変換後の値（変換係数）について 2 進数の符号を割り当てる。

研究開始当初は，IC カードでの処理をも想定していたので，ワンタイム変換における計算処理の内容を軽減する必要があると考え，図 3 におけるランレングス符号を変換の対象とできるかどうかを検討した。しかしながら，ランレングス符号は周波数領域であり，ブロック内の波形情報を保存しているものの，幾何学的な情報（画像における座標）については，8 画素×8 画素ブロックの左上画素の座標のみである点から，本研究において，想定していたワンタイム変換，すなわち反復的に座標変換を行う関数系を構築するのが困難との見通しを得た。

また，ディジタル画像から抽出される特徴情報として，人の左右の眼の距離，鼻の長さ，鼻下～唇の距離といった情報が想定されたが，周波数領域の情報から直接取り出すことが実際的ではないと考えられた。

以上の考察より，ディジタル画像において，ランレングス符号，すなわち周波数領域での

処理よりも，画素領域に変換された後の復号画像を用いることが現実的であるとの見通しを得た。

（２）ワンタイム変換を実現する写像の構成方法

ワンタイム変換を構成する写像については，上述のように，反復関数系あるいはカオス写像を想定していた。当初，反復関数系

$$\{w_1, w_2, \cdots, w_n; p_1, p_2, \cdots, p_n\}$$

について研究を行っていたが，反復変換後の座標において，ワンタイム変換の要件（２）の「距離保存性」を満たす距離関数を導くことが困難との見通しを得た。距離保存性の根拠としては，変換前に適用する距離関数 d_1 と変換後に適用する距離関数 d_2 の間に距離の等価性

$$c_1 d_1(x,y) \le d_2(x,y) \le c_2 d_1(x,y)$$

が成立する必要であると考えた。式中の c_1 及び c_2 は正定数である。これにより，変換の前後で距離の関係が保存されるためである。

上述の検討を行っていた所，2011 年 7 月に以下の論文において，ワンタイム変換による顔認証に関するアルゴリズムとその実装結果が発表されたいたことが判明した。

Yongjin Lee, Yongki Lee, Yunsu Chung, Kiyoung Moon, “One-Time Templates for Face Authentication”, International Conference on Convergence Information Technology 2007

上記論文では，本研究のアプローチとは異なる方法でワンタイム変換を構成していた。画像をワンタイム変換として生成した直交行列とシフト変換を用いていた。上記論文の提案法では逆変換が可能な写像を用いており，本研究におけるワンタイム変換の要件（１）及び（２）を満たしているが，要件（３）が不要であるとみなした。（余談であるが，上記論文では，研究代表者の論文が引用されていた）

これにより，当初検討の土台としていた理論について，そのままのアプローチでの実装可能性や安全性の視点から再検討を加える必要が生じた。助成期間において，ワンタイム変換の３つの要件はそのままで良いとの見通しを得たものの，実装可能なワンタイム変換を得るには至らなかった。

以上により，「３． 研究の方法」に述べた研究内容のうち，（１）のみの検討に止まった。

ただ，このようなアプローチによる生体認証技術の必要性は研究開始当初より高まっているものと考えており，今後も引き続き実装に向けて，ワンタイム生体認証技術の研究をさらに進めていく予定である。

本研究の実施に当たり，本事業の支援をいただいたことに心より感謝する次第である。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計０件）

〔学会発表〕（計１件）

(1) 上繁義史，“生体認証の Health and Demographic Surveillance System への応用” 第 1 回 Health and Demographic Surveillance System 研究会，2010 年 11 月 28 日-29 日，総合地球環境学研究所（京都）

〔図書〕（計０件）

〔産業財産権〕

○出願状況（計０件）

６．研究組織

(1)研究代表者

上繁 義史（UESHIGE YOSHIFUMI）
長崎大学・情報メディア基盤センター・准教授
研究者番号：００３００６６６

(2)研究分担者

なし

(3)連携研究者

なし