東海大学大学院 2012 年度 修士論文

複数の指紋を組み合わせた認証方式の研究

A study on combination of multiple fingerprints in authentication

指導教員 菊池 浩明 教授

東海大学大学院 工学研究科 情報理工学専攻

0LDRM004 蘇　継遠

目次

第1章 序論

1.1 背景

個人認証の安全性を向上させるために、パスワードの代わりに生体認証はよく使われている。パスワードによる個人認証では、忘却や紛失などの原因で本人でも認証できなくなる可能性がある。また、漏洩や盗難などにより、本人ってない他人を認証される犯罪の事件でもよく発生している。

生体認証は個人的な生体特徴を用いたので、それらの危険性は低いと考えられ、簡単な認証手段や第三者が認証されることを防止できる。いま現在、入口、銀行の ATM や入出国の本人認証などによく採用されている。しかし、生体認証では器官の先天性破損、病気や怪我などにより、認証ができない場合がある。また、経年変化と言うことで、認証ができなくなることも明らかに存在している。

指紋認証は生体認証の一つである。工業的な材料で偽造される危険性がある。松本らの研究では、偽造された人工指で本人と認証できることを報告され、漏洩するリスクも指摘されている[1]。これに対して、小林らはいくつかの指紋を組み合わせて、認証に用いる方式を報告している[2][3]。複数の指を組み合わせることで、認証情報を変更する回数は多く安全性も向上させる[3]。しかし、彼らの方式は操作が複雑になり、本人拒否率も高い。

国分らの研究ではパスワードによる認証について、同じな画面で複数のボータン同時に押し暗証番号認証である[8]。彼らの方式では安全性が向上させたが、組み合わせが長期記憶保持するのが困難である。また、入力画面の領域が大きくないため、入力ミスと入力時間も問題がある。

大野らの研究では赤外線で手形状を撮影し、指の本数や種類などの情報で認証する方式である[4]。彼らの方式では、認証率が低い。

1.2 目的

単一の指紋認証の技術を用いて、小林らの研究より操作が簡単になり、本人拒否率が低い新しい指紋認証方式を提案する。指紋情報だけの認証ではなく、指紋をくみあわせる順列情報も認証する秘密情報のひとつとして利用する。本研究では、本来の手法で単一の指に対してマニューシャを抽出し、マニューシャ情報を比較する。類似度によるスコアで認証が行う。その結果で２本指の場合の理論的な認証結果を計算する。単一の指と２本指の認証結果を比較した上で認証精度を評価する。

1.3 論文構成

本論文の構成は次の通りである。第１章は研究背景と目的を述べる。第２章は生体認証の一つとしての指紋認証を述べる。第３章は従来研究の手法を述べる。第４章は研究に利用する要素技術を説明する。第５章は実験と実験の評価を述べる。第６章は結論と今後の課題を述べる。

第 2 章　指紋認証

2.1 生体認証

個人認証は知識認証、所有物認証と生体認証三つがある。

知識認証：　知識として暗記させる情報での認証である。
忘却の可能性がある。情報の変更も必要。
所有物認証：持っている物での認証である。
紛失の可能性がある。持つのは必要。
生体認証：　体の特徴に対する認証である。
認証方式により、認証率が違う。

安全性としては生体認証は一番高く、所有物認証は一番低い。

生体認証は登録された生体特徴の情報と認証する時に取得された特徴情報を照合し、類似度を特定閾値τで判断し、本人かとかが認証する方式である。認証ができるように、以下の三つの条件が必要である。

１、特徴は全ての人が持つ。

２、誰でも違う。

３、経年変化が少ない。

2.2 指紋認証

生体認証ではいくつかの種類があるが、指紋認証がひとつとして、安全性と精度が高く、装置のコストが低い。また、誰でも持つことが明らかにわかって、万人不同と終生不変の特徴も持つ。指紋認証は指先の隆起線による特徴で本人かとかの生体認証である。今は広く範囲で使われている。入国管理局によると、日本では 2007 年 11 月 20 日から入国審査で指紋の登録が義務化として導入された。

第３章　従来研究

3.1 小林らの認証手法[2][3]

小林らの方式は複数の指紋により暗証番号を表現する方式を報告する。暗証番号は個人認証としてよく使われているが、他人に漏洩されて、不正に使う危険性がある。指紋認証はこの危険を防止できるが、偽造される危険がある。複数指紋を用いて、組み合わせた順列で指紋を偽造されても不正者が利用困難である。

暗証番号では 0…9 の数字で組み合わせるので、ひとつの数字がひとつ以上の指紋をくみあわせて、対応する。左右手の全ての指でも使う。各数字を区別できるため、区切り記号をひとつだけの指紋で表現する。区切り記号は最後に入力する数字に対して、省略する。２つの指を利用する場合に指が A と S にすれば、１から６までは A が１回から６回まで入力し、７から９までは S が２回から４回まで入力する。０は S が５回入力し、区切り記号は S が１回入力する。この方式で、ひとつの数字とひとつの区切り記号を入力するためには、((5+1+2+3+4+5+6+2+3+4)+ 10)/10 = 4.5 回の入力が必要である。同じ方法で三つの指を使うときに、3.5 回の入力が必要、４つの場合は 3 回が必要、５つの場合は 2.7 回が必要である。

結論としては安全性が向上できる。しかし、この方式では入力回数が多いため、操作が複雑であるとかんがえられ、本人拒否率（FRR）が高いと考えられる。

3.2　国分らの認証手法[8]

国分らの研究では、暗証番号の入力においてひとつずつのの入力だけではなく、複数の数字を同時に入力することも可能である認証手法が考察した。通常の方式と国分らの方式を比較するのは図１のように表す。しかし、入力ボタンにより、入力するときに連続する数字がこの方式において、入力できない。

今回の実験はこの問題に対して、代用キーを図２のように追加する。１回の連続はひとつの代用キーを数字と同時に押し、２回は２つを数字と同時に押し、３回は３つを数字と同時に押す。

表１　入力に関する実験結果　　（文献[8]より引用）

	平均入力時間 (sec)	標準偏差 (msec)	最短時間 (sec)	最長時間 (sec)
同時押し認証	3.012	1342	1.393	9.496
暗証番号認証	2.742	861	1.407	5.488

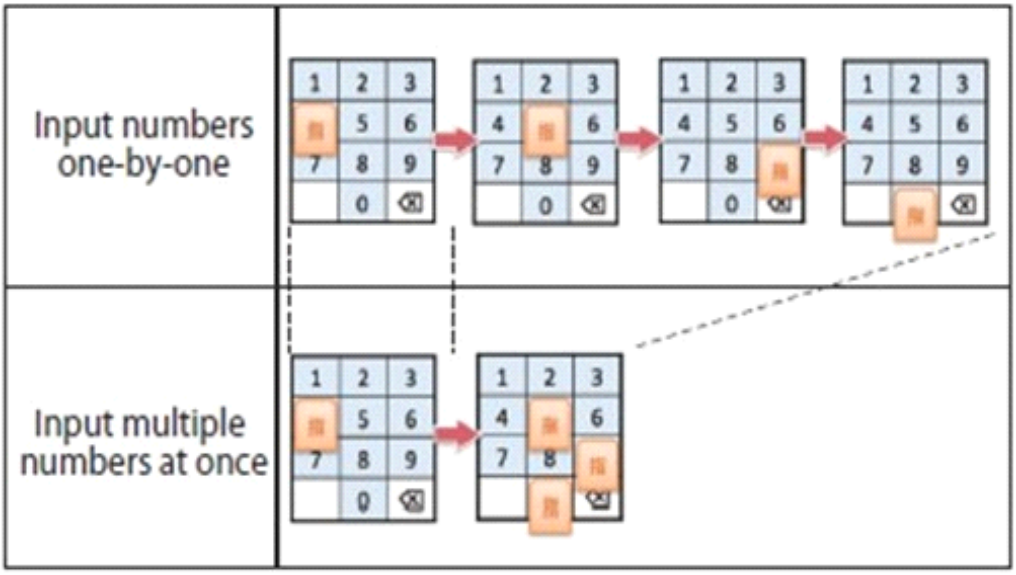

図１　通常の入力と国分らの方式の比較（文献[8]より引用）

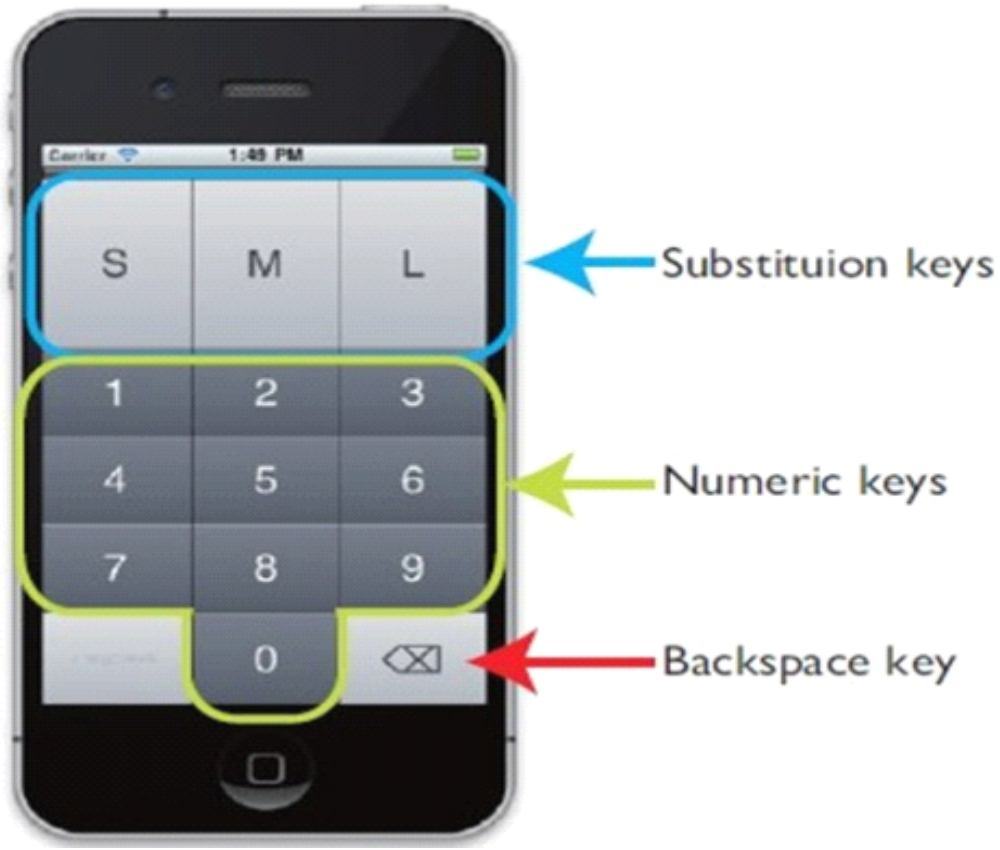

図２　国分らの方式の入力画面（文献[8]より引用）

記憶保持について、実験日、４日目と９日目に被験者６名において、ひとりずつ５回４桁の暗証番号を入力し、実験を行う。３回目にはひとりが失敗した。通常の方式と国分らの方式において、入力時間は表１と図３のように表す。

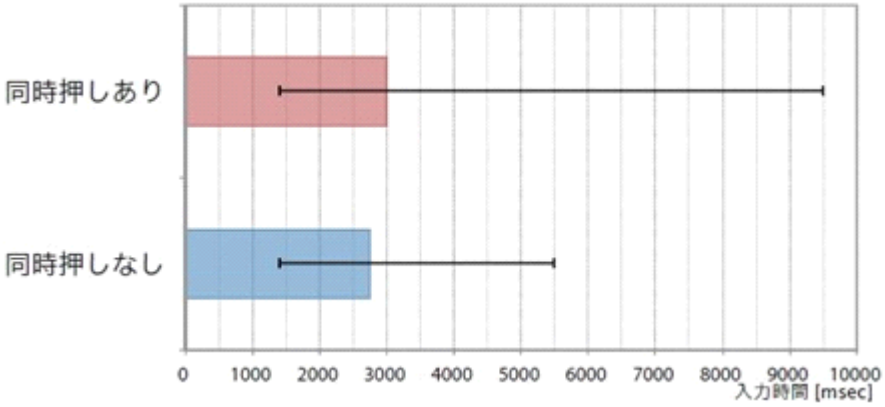

図３　通常方式と国分らの方式の比較（文献[8]より引用）

入力ミスについて、７名の被験者に特定の暗証番号を教え、実験を５回行う。通常方式の方がミスは発生しなかった。国分らの方式においての実験結果は表２のように表す。

表２　国分らの方式における修正回数と秘密情報の関係
（文献[8]より引用）

秘密情報	修正回数
(013)9	4
(357)9	1
0(15)2	1

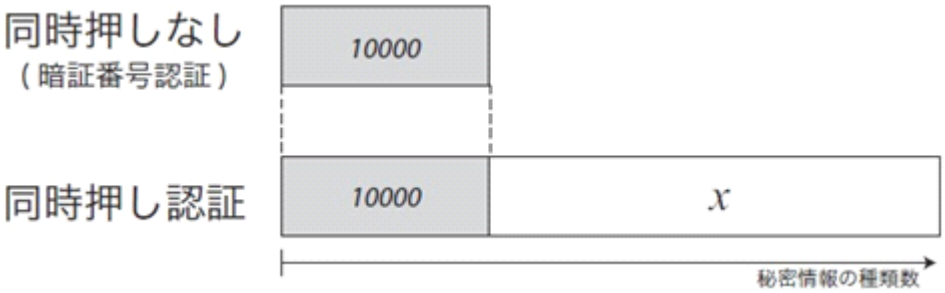

図４　秘密情報の種類数比較（文献[8]より引用）

結果は国分らの方式が短期記憶として困難ではないが、長期記憶保持はむずかしくなる。入力時間が長くなって、入力ミスが既存研究より多くなる。安全性が従来の方式より高くなる。実験の設備として、iPod　touch を使うため、入力画面の領域が小さいのは入力ミスが多い原因になる。

3.3　大野らの認証手法[4]

大野らの研究では赤外線カメラで手形状を撮影し、指の本数や種類などの情報で認証する方式である。手形状は指の種類や指の本数などの情報パラメータを撮影し、特徴量を抽出され、照合する。

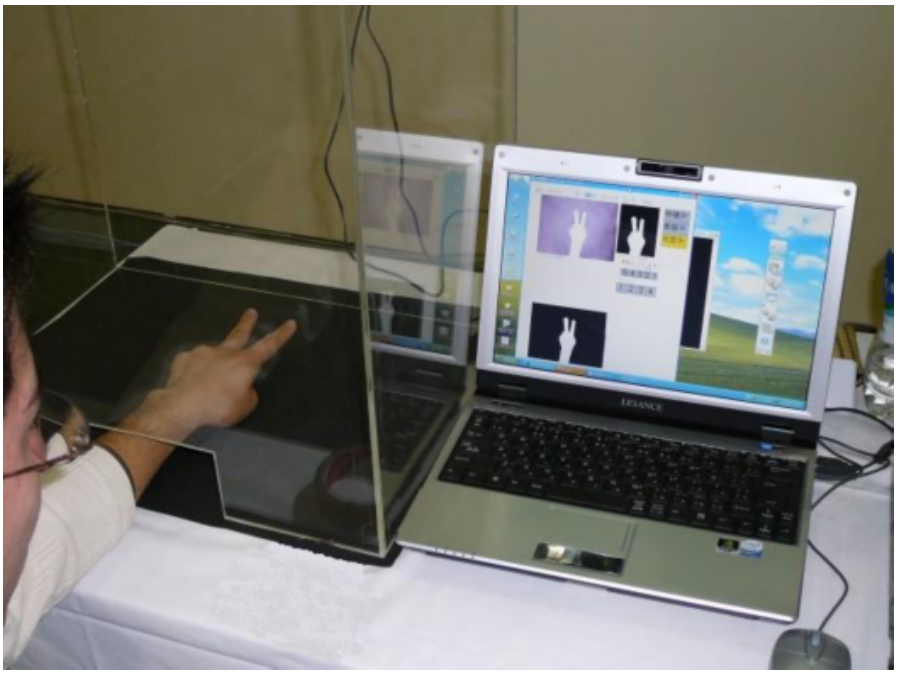

図５　実験環境（文献[４]より引用）

実験は図５のように行う。赤外線カメラにおいて、撮影し、手の部分と背景を二値化する。手の部分は白において表示し、他の部分は黒において表示する。手の部分を切り出し、正規化され、図６の画像を取得できる。

図６　正規化された画像　（文献[４]より引用）

画像の白ピクセル数が全ピクセル数に対して１/２以上または１/２０以下の場合は手が正しく撮影されていないと判断し、破棄する。図７のように、取得された画像で左上からＸ軸方向にピクセル単位でラスタ走査し、白ピクセルが始めて連続して５個続いたＹ軸をＡ、２０個続いたＹ軸をＢとする。ＡとＢの中間に在る走査線をＣとする。人差し指から小指までの幅はＣ上の一番最初と一番最終にある白ピクセルの座標差である。

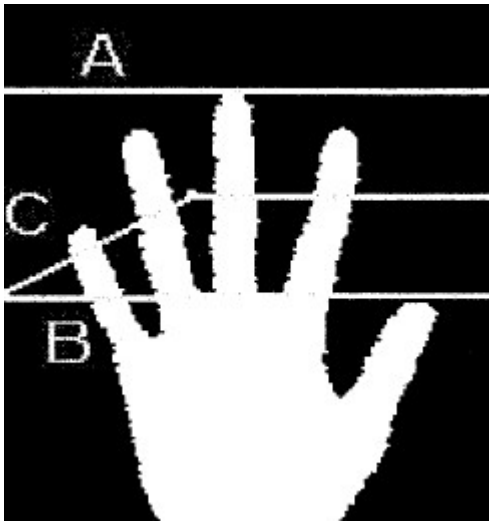

図７　走査線（文献[8]より引用）

図８のように指の太さはＣ上にある白ピクセルの個数を１/４である。

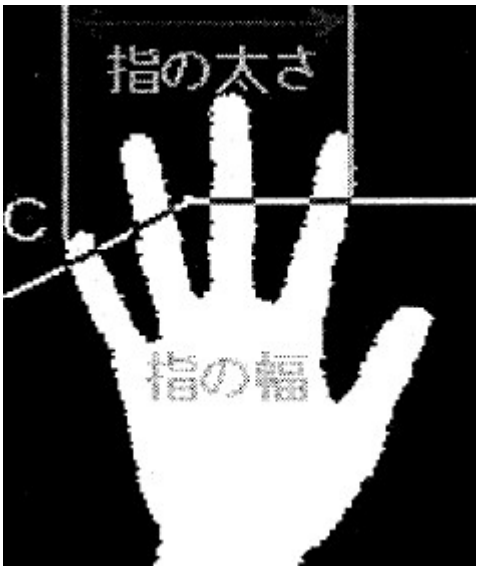

図８　　指の太さ（文献[8]より引用）

図９と図１０のようにＡとＢの幅の差により小さいのは閉じている、逆に開いている。ＡとＢは設置できるため、出ている指が０本または１本の場合には定義出来ないので結果は表示しない。でも、判定は可能である。

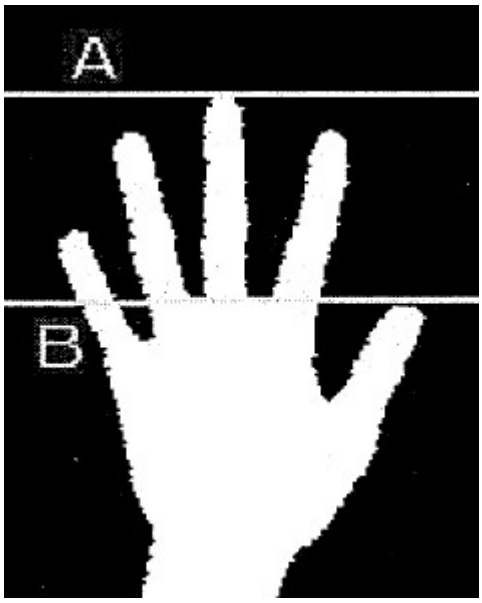

図９　指が開いている時
（文献[４]より引用）

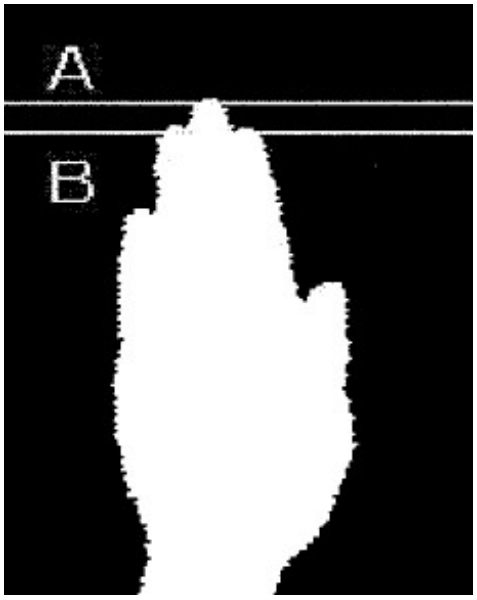

図１０　指が閉じている
（文献[４]より引用）

指の本数の認識について、図１１と図１２のように、手の重心から走査線Ｄをする。指が開いている時にＣと先程登録された指の４本指の太さで親指以外の指は何本が出るか判断し、走査線Ｄから白い部分が何個かを判断し、親指が出るかとかを判断できる。指が閉じている場合に、Ｃと先程登録された指の４本指の太さで親指以外の指は何本が出るか判断し、走査線Ｄから白ピクセルが４本の指より大きいほうが親指は出たと判断できる。

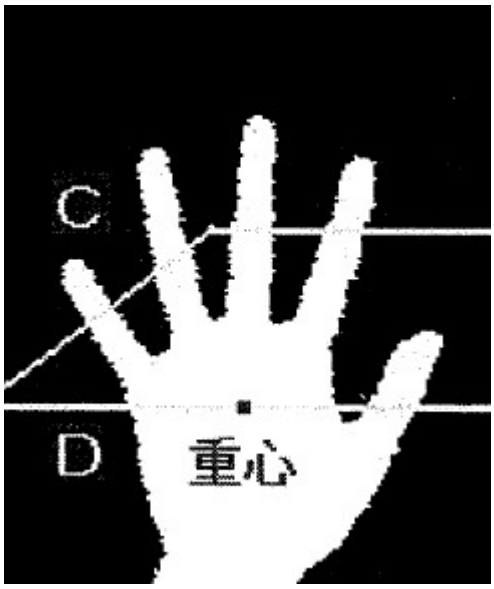

図１１　指が開いている時
（文献[４]より引用）

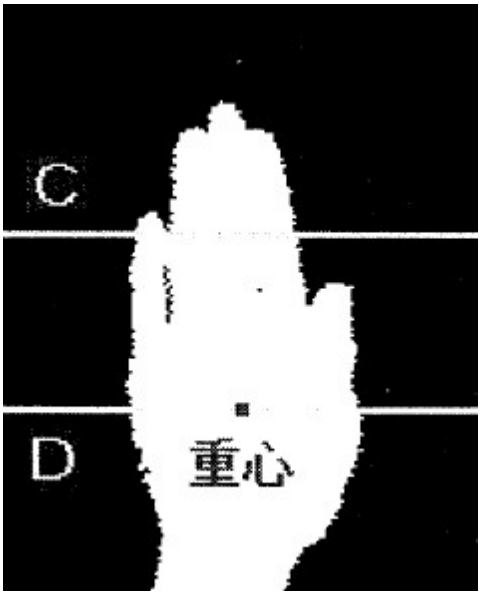

図１２　指が閉じている時
（文献[４]より引用）

指の種類について、図１３のように走査線Ｃで各指の座標を決定し、図１４のように座標の位置で手の領域が等分できる場合に小指が出ると判断し、各指が出るかとかも判断でき、図１５のようなひとつ領域だけがちいさすぎる場合は小指が出ないと判断し、各指が出るかとかも判断できる。等分できない場合に、図１６のように各指から隣の指との座標差や登録した各指の座標と比較し、判定できる。指が閉じている場合に図１７のようにＦ、Ｅの差と指の太さで出る指が判断できる。

図１３　指の座標
（文献[４]より引用）

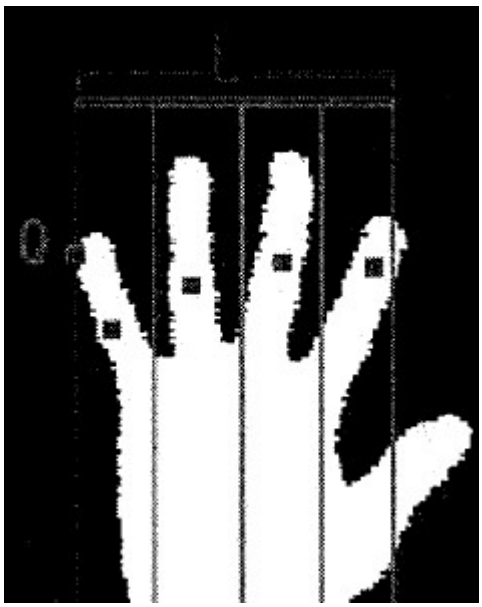

図１４　小指が出る場合
（文献[４]より引用）

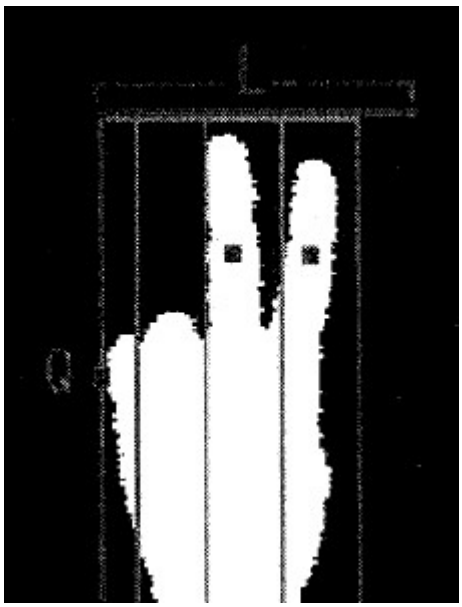

図１５　小指が出ない場合
（文献[４]より引用）

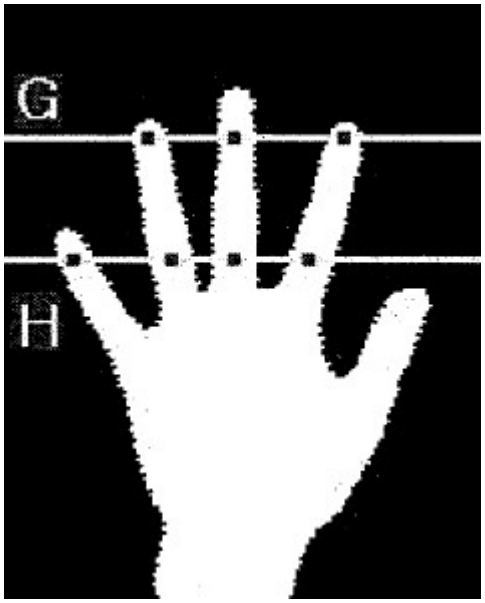

図１６　等分できない場合
（文献[４]より引用）

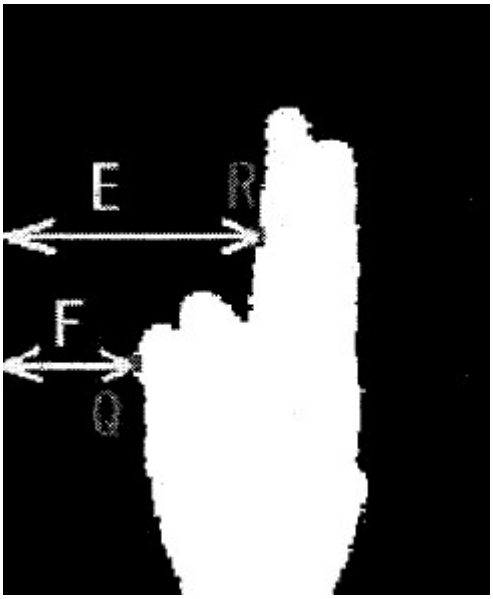

図１７　指が閉じている場合
（文献[４]より引用）

この方式における実験を行って、基本的な認証はできた。指定した手形状を認証されて、心理的な抵抗は少ないが、認証率が主流な生体認証より低いと考えられる。

第 4 章　要素技術

4.1　マニューシャ

マニューシャは図１８のような指紋隆起線の分岐点と端点である。

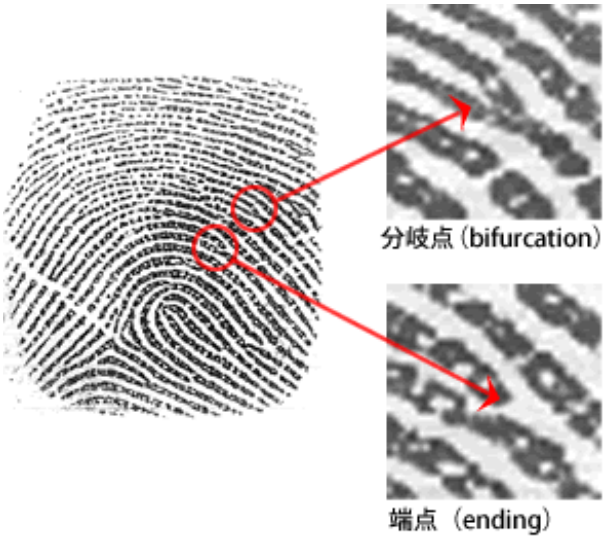

図１８　マニューシャ

今回の実験ではマニューシャに基づく指紋認証を利用する。マニューシャ座標と角度のデータを用いて、照合された類似度で認証を行う。

4.2　NIST Fingerprint Image software2（ＮＦＩＳ２）

NFIS2 は指紋のマニューシャの抽出、指紋形状の分類、マニューシャでの照合と指紋画像品質の判別という四つ機能がある。今回はマニューシャの抽出とマニューシャでの照合を利用し、実験が行う。

4.2.1 mindtct

mindtct パッケージは入力する指紋を解析し、マニューシャを自動的に検出する。指紋画像についてのマニューシャ情報を抽出し、マニューシャファイルを出力する。出力されたファイルが８つあるが、今回は xyt ファイルだけ利用する。

mindtctパッケージでマニューシャを自動出来に検出する例は図１９のように表す。検出されたマニューシャは赤い点を付け、表現する。

図１９　赤点を付けるマニューシャ
(2012 年 12 月研究室で測定, mindct を用いた)

mindtct パッケージで抽出された xyt ファイルは表３のように示す。

表３　mindtct パッケージで抽出された xyt ファイル
（2013 年 1 月研究室で測定, mindct を用いた）

番号	x	y	角度
３８	２０５	２３６	１７
４３	２７６	２３６	１８
４５	２４７	２４７	２０
４６	２９７	２３６	１８
４７	３１４	２３６	１７
４８	２１８	２３７	１６
５０	２８９	２４０	１９
５３	２８８	２３４	２０
５４	２７８	２３７	１８

示された表３のデータは左から右までがマニューシャの番号、x 座標の数値、y 座標の数値とマニューシャに対応する隆起線の角度とする。しかし、マニューシャの番号はノイズを除く前に取ったから、最後まで出力するのは連続しない。xyt ファイルでは数値の量が大きいから、表の中には一部だけ示した。残りの示していない部分のは省略する。

角度の定義は図２０のように表す。角度は対応する隆起線の方向の値である。その値は０から３１までの３２段階で示す。角度は各 11.25° に１が増える。

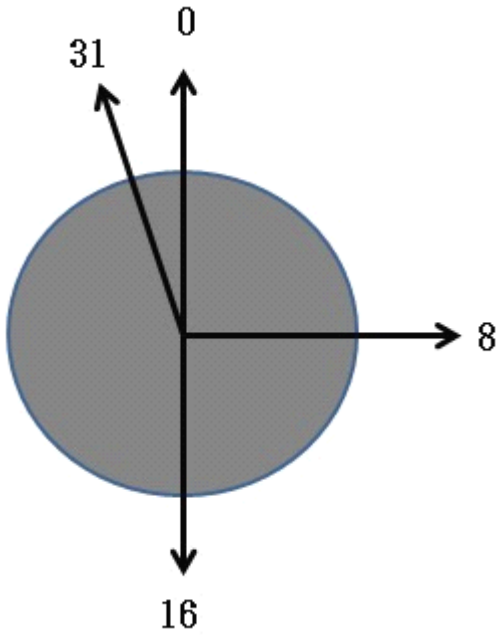

図２０　角度の定義

4.2.2 Bozorth3

Bozorth3 パッケージは、二つの指紋画像の xyt ファイルの類似度を評価する。指定した閾値 τ での認証精度を求められる。今回は mindtct パッケージで抽出された xyt ファイルが Bozorth3 パッケージに入力し、類似度評価をマッチングスコアとして出力する。マッチングスコアは[0,550]の数値を出力し、大きい方が指紋は「近い」と判断する。望月らの研究[7]により、同一指紋の場合は他画像であってもマッチングスコアは 120 であるが、他人の指紋同士の平均として、マッチングスコアは 40 ぐらいである。今回の実験はマッチングスコアが[0,10,20,30,40,50,60,70,80,90,100,110,120,130,140]15 個の閾値 τ の場合において本人拒否率(FRR)と他人受入率(FAR)を求める。

第５章　実験と評価

5.1　実験目的

第４章で述べた mindtct パッケージと Bozorth3 パッケージを用いて、単一の指に対して、本人拒否率(FRR)、他人受入率(FAR)と認証精度を求める。この精度に基づいて、２本指を組み合わせて認証した場合の理論的に見積る本人拒否率(FRR)、他人受入率(FAR)と認証精度を求める。

5.2　使用機材

指紋を撮影するために、図２１のような Digital Persona 社の指紋リーダー“U.are.U”を利用した。

図２１　指紋リーダー“U.are.U”
(2013 年１月研究室で撮った, iPhone 5 を用いた)

5.3 実験概要

5.3.1 単一指の評価

指紋リーダーで単一指の指紋画像を撮影し、mindtct パッケージと Bozorth3 パッケージを用いて、指定した各閾値での本人拒否率(FRR)、他人受入率(FAR)と認証精度を求める。

5.3.2 単一と複数の比較

5.3.1 の結果を用いて、理論的に見積る複数指の指紋の指定した各閾値での本人拒否率(FRR)、他人受入率(FAR)と認証精度を求めて、比較する。

5.4 実験方法

5.4.1 単一指の他人受入率(FAR)

１７名の被験者で、実験を行う。被験者は指紋リーダーで一人ずつ各指をスキャンし、mindtct パッケージを用いて、xyt ファイルを得る。被験者の中から１名を選び、各指を残り１６名一人ずつ各指に対して、Bozorth3 パッケージで入力した xyt ファイルのマッチングスコアを得る。[0,10,20,30,40,50,60,70,80,90,100,110,120,130,140]15 個の閾値 τ の場合において他人受入率(FAR)を求める。

5.4.2　単一指の本人拒否率(FRR)

被験者一人だけに対して、一つの指を選び、1001 回スキャンし、同様にして、一つ指紋と残り 1000 個の指紋を照合し、マッチングスコアを得る。15 個の閾値τの場合において本人拒否率(FRR)を求める。他人受入率(FAR)と本人拒否率(FRR)を用いて、同じ閾値での認証精度を求める。

5.4.3　理論的に２本指と単一指の比較

5.4.1 と 5.4.2 の結果を用いて、２本指に対する理論的に見積る他人受入率(FAR)、本人拒否率(FRR)と認証精度を求める。単一指に対する本人拒否率(FRR)の確率が P の時に、２本指の確率は式 $P'=1-(1-P)^2$ により求められる。他人受入率(FAR)も同様である。その結果から２本指の認証精度も求められる。３つの結果で単一指と２本指比較する。

5.4.5　実験結果

表４　単一指の FAR

(2013 年 1 月研究室で測定, Bozorth3 を用いた)

閾値τ	0	10	20	30	40	50	60	70
FAR	1	0.100625	0.003125	0	0	0	0	0
閾値τ	80	90	100	110	120	130	140	
FAR	0	0	0	0	0	0	0	

表５　単一指の FRR

(2013 年 1 月研究室で測定, Bozorth3 を用いた)

閾値τ	0	10	20	30	40	50	60	70
FRR	0	0	0.005	0.055	0.25	0.655	0.903	0.984

閾値 τ	80	90	100	110	120	130	140	
FRR	0.999	1	1	1	1	1	1	

表６　単一指の認証精度

(2013 年 1 月研究室で測定, Bozorth3 を用いた)

FAR	1	0.100625	0.003125	0	0	0	0	0
FRR	0	0	0.005	0.055	0.25	0.655	0.903	0.984
FAR	0	0	0	0	0	0	0	
FRR	0.999	1	1	1	1	1	1	

表７　２本指の FAR

(2013 年 1 月研究室で測定, Bozorth3 を用いた)

閾値 τ	0	10	20	30	40	50	60	70
FAR	1	0.191124609	0.006240234	0	0	0	0	0
閾値 τ	80	90	100	110	120	130	140	
FAR	0	0	0	0	0	0	0	

表８　　２本指の FRR

(2013 年 1 月研究室で測定, Bozorth3 を用いた)

閾値 τ	0	10	20	30	40	50	60	70

FRR	0	0	0.009975	0.106975	0.4375	0.880975	0.990591	0.999744
閾値 τ	80	90	100	110	120	130	140	
FRR	0.999999	1	1	1	1	1	1	1

表９　２本指の認証精度

(2013 年 1 月研究室で測定, Bozorth3 を用いた)

FAR	1	0.100625	0.003125	0	0	0	0	0
FRR	0	0	0.009975	0.106975	0.437	0.8805975	0.990591	0.999744
FAR	0	0	0	0	0	0	0	
FRR	0.999999	1	1	1	1	1	1	

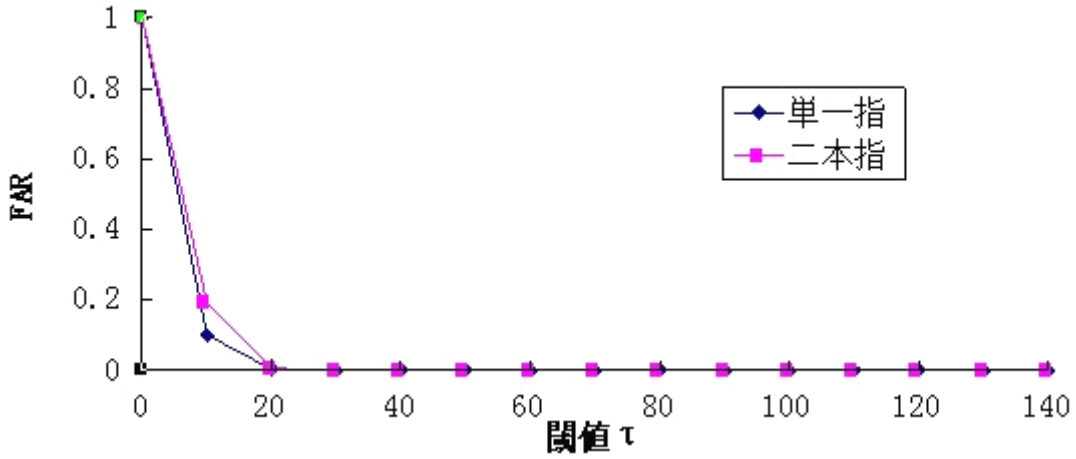

図２２　　単一指と二本指 FAR の比較
(2013 年 1 月研究室で測定, Bozorth3 を用いた)

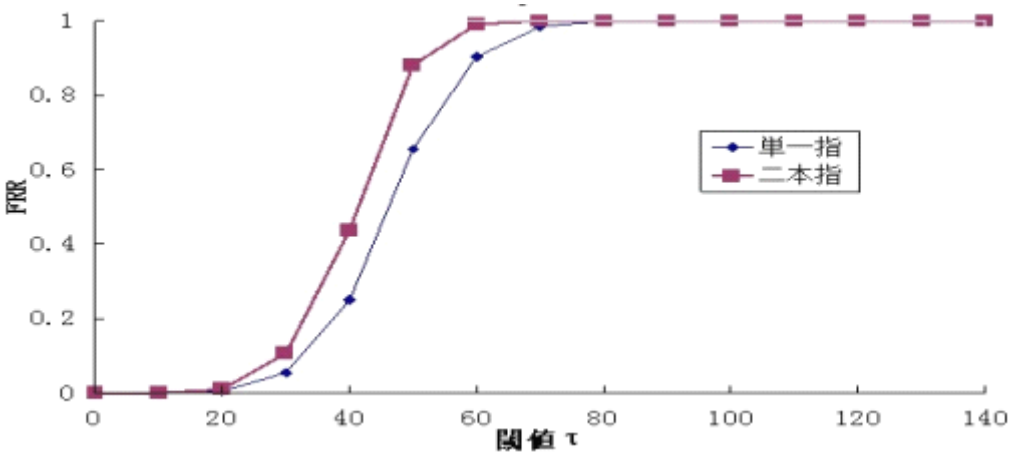

図２３　　単一指と二本指 FRR の比較
(2013 年 1 月研究室で測定, Bozorth3 を用いた)

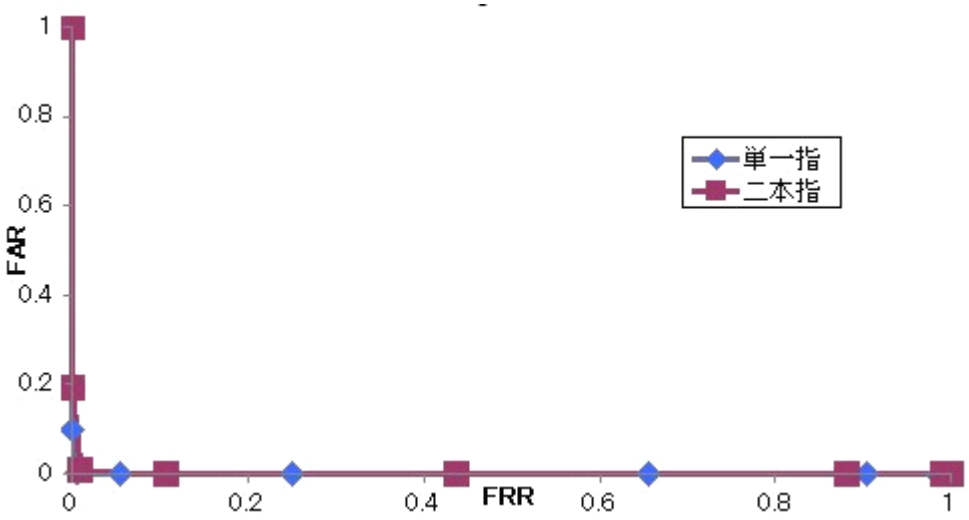

図２４　　単一指と二本指認証精度の比較
(2013 年 1 月研究室で測定, Bozorth3 を用いた)

表４、表５、表６は単一指の FAR、FRR と認証精度を示し、表７、表８と表９は二本指の理論的に見積る FAR、FRR と認証精度を示した。この結果で次の図２２、図２３と図２４を書いた。

5.5　実験評価

１７名の被験者の指紋を指紋リーダーでスキャンし、要素技術を用いて、実験を行い、単一指に対する本人拒否率(FRR)と他人受入率(FAR)と認証精度を求めた。確率の計算で二本指の理論的に見積る確率を求め、単一指と比較した。２本指の場合は同閾値の場合に単一指より FRR が上がって、FAR が下がる。

第６章　　結論と今後の課題

6.1　結論

本研究では、主流の指紋認証より安全性が高い認証方式を探し、二本指を組み合わせた認証方式を提案し、理論的な結果と単一指の認証結果を比較し、二本指にすることで、同閾値の場合に単一指より FRR が上がって、FAR が下がる。

6.2　今後の課題

今後の課題としては、二本指に対して、実験を実装する。理論的な結果と比較し、認証精度と安全性を検討し、この提案の有用性を考察する。

参考文献

[1] 松本　勉　「金融取引における生体認証について」　金融庁・第９回偽造キャッシュカード問題に関するスタディグループ　2005.

[2] 小林 哲二　「複数の指紋で暗証番号を表現する個人認証」情報処理学会シンポジウム論文集　p.175　2003.

[3] 小林　哲二　「個人認証用の指紋と暗証番号の入力方法についての検討」電子情報通信学会　2003 年度総合大会講演論文集, A-7-25, p.198, March 2003.

[4] 大野　敬弘,他　「手形状認識によるセキュリティキー入力システムに関する研究」情報通信学会（IPSJ）p.293 2008.

[5]佐藤公則 他　「手の形状を利用した非接触セキュリティキー入力システムの開発に関する研究」バイオメトリクスと認識・認証シンポジウム,IEICE p.19 2009.

[6] 菊池　浩明　他　「直交基底指紋への参照度を特徴量とした安全な生体認証プロトコル」　暗号と情報セキュリティシンポジウム,SCIS p.2F4-3　2009.

[7]望月「指紋認証におけるマニューシャ変動の調査」, 東海大学 2009年度卒業論文,2009.

[8] 国分佑樹　他「同時押し認証:暗証番号認証の改善を目指した一つの試み」,情報処理学会シンポジウムシリーズ,IPSJ　p. ROMBUNNO.1F-4　2012.

謝辞

本研究では多く方々のご指導とご協力を頂きました。大変感謝しております。

特に東海大学情報通信学部通信ネットワーク工学科教授菊池浩明教授に最大な感謝を申し上げます。大変迷惑を掛けて、有難うございました。

そして、ご指導を頂いた情報理工学部情報科学科内田理准教授にも感謝を申し上げます。

まだ実験に協力下さった菊池研究室と内田研究室の様様と留学生達にも感謝を申し上げます。