Computer Security Symposium 2017
23 - 25 October 2017

個人の嗜好で識別を行う画像認証方式

持田達範 †　稲村勝樹 †

概要：近年パスワード認証や指紋認証など，登録されている個人特定用のデータを用いた認証方式が普及している．これらの認証方法の問題点としては，その特定データが一定期間変動しないことや，そのデータが流出した場合に不正に認証が行われてしまうことである．そこで，認証時の登録された特定情報を設定せずに，人間の性格的な情報から個人での認証を可能とする方法を検討し，本論文では個人の嗜好の特徴から個人を認証する方法を提案する．技術的には，コンピュータから生成された毎回異なる画像を見た時の個人の嗜好の特徴を機械学習によって抽出を行い，その特徴から個人の認証を行う．

キーワード：個人認証，画像認証，機械学習

Image-based Authentication Method by an Individual Liking for User Identification

Tatsunori Mochida †　Masaki Inamura †

Abstract: Recently, authentication methods using registered personal identification data such as password authentication and fingerprint authentication have been widely used. However, There is a problem with these authentication methods, which means that certain data does not fluctuate for a certain period of time and that unauthorized authentication occurs when data leaksIn this paper, we will consider how to enable individual authentication from person's characteristic without setting specific information registered when performing authentication. Furthermore, we propose a method to authenticate individuals from the characteristics of personal taste. As a technical aspect, features of preference are extracted by machine learning when viewing different images generated from a computer. Our method certify individuals based on their characteristics.

Keywords: Authentication, Image-based Authentication, Machine Learning

1. はじめに

近年，パスワードによる個人認証方式に様々な課題が提示され，それに代わる認証方式の研究・提案が行われている．その中の一つとして画像認証方式があり，これは画像内から得られる情報を鍵として認証を行う手法である．画像認証の主な方式としては様々あり，登録画像の再認による方法，画像内の特定の位置を鍵とするもの，画像に示されている人やものから文字記憶を再生・再認するものなどがある．

まず登録画像の再認による方法について，この方式はあらかじめ定められた画像をユーザーに記憶させる．ユーザーに画像を記憶させた後，認証時に複数枚の画像の中からユーザー登録時に設定した画像を選択させる．もしユーザーが認証の鍵とする画像を選択できれば認証成功，選択できなければ認証失敗というものである．具体例としてニーモニックガード[1]や合わせ絵[2]などが挙げられる．画像内の特定の位置を鍵とするものして，Passlogix[3]，PassPoints[4]がある．また，画像を基に文字記憶を再生・再認するものの例としてなぞなぞ認証[5]やCAPTCHA[6]などがある．

しかし，それらの認証方式の問題点としては画像そのものや特定の情報を，認証を解除する鍵として扱うことである．それらの情報は一定期間変動しないため，その情報が流出した際にパスワード方式の認証と同じく，不正に認証が行われてしまうことである．

本稿では，画像認証時における認証の鍵となる情報が流出した際，その情報を使用して不正に認証を行われることを回避するために同じ画像を使用せず，認証時に使用した鍵となる情報が流出しても特定の個人だけを認証できる手法を提案する．具体的にはコンピュータに毎回異なる画像を複数生成させ，個人を認証する際その画像の中でもっとも好みである模様の画像を選択させ，それをコンピュータに学習をさせる．認証を行う際に被認証者が本人であるか，学習時と同様にランダムな模様の画像を生成し選択させる．選択した画像と学習データを照らし合わせ，その適合率から個人を判別する方法を提案する．個人を特定する画像認証の研究において，ランダムな画像を使用した画像認証は存在しない．また今回提案する認証方法は，指紋認証を行う際などに使用する特殊なものを必要としないため，コストを多く必要とせずに実装が行える．

† 東京電機大学理工学部情報システムデザイン学系
Division of Information Systems and Design, School of Science and Engineering, Tokyo Denki University.

本論文では，2 章に関連研究について概要を説明し，3 章にて本論文で使用する手法についての解説を行う．4 章では本論文で提案する手法を用いた実験の手順の提示，実験結果のまとめを行い，5 章で今回の実験についての考察を行い，6 章で本論文のまとめを行う．

2. 関連研究

2.1 画像認証

人間の脳は単純計算やシンボル処理よりも，画像や音声などを使用するパターン情報処理の方が得意であると言われている．昨今はその特性を利用し，特定の文字列を鍵にするのではなく，代わりに画像を鍵として本人認証を行う「画像認証」というものが存在する．そこで，この章では主に画像を用いて個人認証を行う先行研究について論ずる．ニーモニックセキュリティが開発したニーモニック認証[1]では，コンピュータによって用意された数十枚の画像の中にユーザーが登録した画像を数枚含めランダムに配置する．それらの画像の中からユーザーが登録したものを選択できれば認証成功となる．また，画像内の特定の位置を認証の鍵情報として用いる手法もあり，Passlogix を例として挙げると，これは画面に表示される画像（部屋の写真など）に含まれる家具などのオブジェクトを，あらかじめ指定した任意の順で選択を行う．そのオブジェクトを選んだ順番を鍵として認証を行うものである．

しかし，上記の認証システムだと認証時の画面に必ず同じ画像が表示されてしまうため，何度も認証を繰り返すうちに出現頻度の高い画像が鍵であることがわかってしまう．このような問題を防ぐために高田哲司氏らはあわせ絵[2]という手法を考案した．認証時にコンピュータが提示した画像を選択する点ではニーモニック認証と同様であるが，あわせ絵では提示される画像の中にユーザーが登録した画像が含まれないことがある．その場合はユーザーが選択すべき画像がない旨を回答できるため，上記の問題が解決できる．これらのように，画像認証と言われる研究分野では，何か意味を持つ画像や人に関係する画像が認証の鍵として使われる場合が多い．

2.2 既存研究での問題点

2.1 章で論じた通り，画像認証はパスワードの認証に使われるような，ユーザーに無関係な情報を鍵として扱われることがなく，そのユーザーであれば再認できる情報を使われるため，利用者が覚えやすいという利点があるが，その反面，認証を不正に突破できてしまう問題点も存在する．その問題点は主に 2 つ存在する．一つ目に覗き見攻撃に脆弱な点である．この攻撃に対してパスワード認証も脆弱であることは変わらないが，悪意のある者に攻撃をされた場合，ユーザーが設定している鍵となる画像が攻撃者も知っている情報であった場合，画像のため文字より脆弱であることはないが，認証を突破しやすくなってしまう．次の問題点としては推測攻撃に対して脆弱な点である．画像認証でユーザーが鍵とする画像は，ユーザーの好き嫌い，趣味，関連人物が使用されることが多い．そのため，その人をよく知る人物が攻撃者であった場合，その人物の公言している情報から認証に使用されている画像を推測し，不正に認証を行われてしまう可能性がある．推測攻撃に対して，画像認証時のガイドラインにて「公言している情報，持ち歩いている情報ばかりを鍵としない」など警告がなされているが，それでも一部でユーザーに関係のある画像が鍵として使用される以上，認証の強度は弱くなってしまうと考える．

3. 個人の嗜好による識別

3.1 識別方法の概要

本章では，個人の嗜好を用いて本人であるか否かの識別を行う画像認証方式について説明を行う．本方式は，前章で述べられた画像認証を行う際で鍵となるデータの流出，推測攻撃に対して不正に認証が行われてしまう問題点を解決するため，今回のシステム構築を行うことを目的とする．

画像認証時に限らず，認証時の覗き見攻撃の対策としては，正面以外から見た場合画面を暗くする，認証に使用するキー配置やオブジェクトをランダムに設置するなどが考えられる．我々は，この攻撃の対策として認証時に鍵とするデータをシステムにより再度同じデータを使わせないことにより解決した．本論文にて提案する画像認証方式であれば，認証時に使用される画像が 1 度より多く使用されないため，認証時に鍵となるデータが覗き見されることにより情報が流出しても問題がないと言える．また本提案システムは正当な認証対象者の嗜好を機械学習によってトレースを行い，攻撃者の思考判断と，正当な認証対象者の思考の差異から本人であるかどうかの識別を行う．

しかし，色を認証の要素として使う上である問題が発生する．その問題とは人の性格により好きな色が推測できてしまう点である．実際に松田氏らの研究によって，パーソナリティ特性と嗜好色の関連性があることがわかっている[7][8]．我々はこの問題に対して，認証時の色の判別の精度を上げることができれば問題がないと考えた．その理由としては色の感じ方が個人によって違い，例えば A 氏にとって感じた赤色が B 氏にとっては A 氏と同じ赤だと感じられない場合があるからである．それを裏付けることとして，Israel Abramov らの研究[9]によって，色覚は男性ホルモンであるテストステロンによって差異が出る可能性が高いことが示されている．テストステロンの値は男女によって顕著に差が出るが，同性同士でも個人差が出てくる．このため，同性同士であっても他人と同じ色を感じることは難しいと考えた．また個人の色覚の差異は生物学的な問題でもあり，正常色覚を持つ者においても色感覚が異なるという研究結果[10]が出ている．ここに写真の明暗によって同色である色

を異なると錯覚する「色の恒常性」，老化による色覚の変化[11]（しかし，これは認証時の本人拒否の問題に繋がってしまう）などの要素も加わってくれば色の選択が複雑になるため，他人の好きな色を予測することができても好きな色を選択することは難しいと考えた．本論文ではこれらのことにより元来の画像認証方式に対する推測攻撃の脆弱性を補う方法を提案する．

3.2 システム構成の手順

本論文の提案するシステムでは任意のユーザー1 人に対し，複数枚それぞれ模様が違う画像を提示した中で，当人が選択した好きな画像を用いてディープラーニングによる機械学習を行う．それによりそのユーザーの好きな画像の特徴の抽出を行う．画像の特徴抽出が十分にできた後，先ほどと同様の方式でユーザーに画像を選択させる．この時，ユーザーにランダムに提示される画像の中で，ユーザーから抽出した嗜好の特徴を基に，コンピュータではどの画像をユーザーが選ぶかを予測させる．その後，抽出した特徴と選択された画像の特徴がどれほど一致するかによって個人の認証を行う．

本節では，以上の認証方式に必要な手法の解説を行う．個人の嗜好の特徴を抽出するための画像生成方法については 3.2.1 節，画像の特徴の抽出方法としては 3.2.2 節，3.2.3 節，特徴の学習方法について 3.2.4 節，個人認証時の評価基準については 3.2.5 節に示す．

3.2.1 画像の生成

本節では画像認証，個人の嗜好を学習するための画像の生成方法を説明する．以下にその手順を示す．

(1). 正方形の図形を用意し，それを縦横 600 ずつに分割し，白で埋めた(RGB 値(255,255,255))画像 P を作成する．

(2). 1~60000 までのランダムな数字を， 画像 P の全てのピクセルに割り当てる．

(3). 今回生成する模様は円形， 直角二等辺三角形， 正方形の 3 種類とし，大きさは任意のものとする．

(4). 画像 P に割り当てられたランダムな数字の中で 3 以下の数字の場合，その場所を模様が生成される中心とする．この画像は 36 万ピクセルからなるため，この過程で生成される図形の期待値は 18 個となる．(今回の判断基準として，15~20 個前後の模様から判断を行うことを目的としたため) ．

(5). 画像 P の中に数字の 1 が含まれている場合，周辺に円形を描画し，2 の場合は直角二等辺三角形，3 の場合は正方形を描画する．

(6). 生成される画像の色相は RGB 値の要素全てが 0~255 までのランダムな値で構成されるものとする．

(7). 以上の定義を基に生成した画像の例としては以下のようなものとなる(図 1) ．

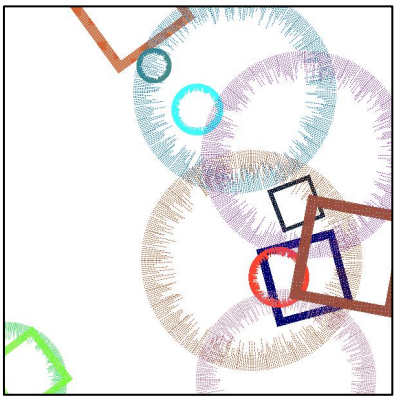

図 1 コンピュータによる生成画像

3.2.2 色相のヒストグラム比較

今回提案する認証手法では，画像からいくつかの特徴点を抽出し，保存されている教育データと，認証時に選択された画像データの比較を行う．そのデータにどれだけの差分があるか計測することが主となる．そのため，この節では 3.2.1 節より生成された画像から，画像の特徴である，色相の割合の導出方法を示す．

3.2.1 節で生成した画像を A とする．色相の割合の導出方法として，まずは画像 A から白成分である RGB 値(255,255,255)を除く．その処理を施したものを RGB 値に分割し，それぞれの値を 0~255 で表す．色成分の分解後，横軸を RGB 値，出現頻度を縦軸としてプロットを行なってヒストグラムを作成する．実際に図 1 を用いてヒストグラム化したものが以下の図となる(図 2) ．

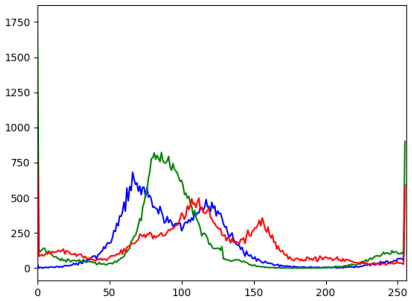

図 2 色相のヒストグラム化

画像 A のヒストグラムの作成後，認証したいユーザーがあらかじめ選んでおいた教育データから生成したヒストグラムと，画像 A のヒストグラムの色相がどれほど一致するか計算によって求める．この計算には画像処理・画像解析機能を持つライブラリである OpenCV[12]を用いて複数のヒストグラム同士を照らし合わせることにより，この比較を行った際の色相の類似度を計算する．

3.2.3 特徴量の比較

色相の類似度とともに，今回は画像の形状を表す，特徴点の抽出を行なったうえ，複数の画像の特徴量の比較を行う． この特徴量の抽出は，ORB(Oriented FAST and Rotated BRIEF[13])のアルゴリズムを用いて行う．このアルゴリズムを用いて図 1 の画像の特徴量を抽出した結果は以下のようになり，図 1 の画像に対して追加された点が ORB によって特徴と判断された部分である(図 3)． あらかじめ選んでおいた教育データの特徴量および，3.2.1 節より生成された画像(これを A とする)の特徴量の抽出をこの ORB のアルゴリズムを用いて行う．

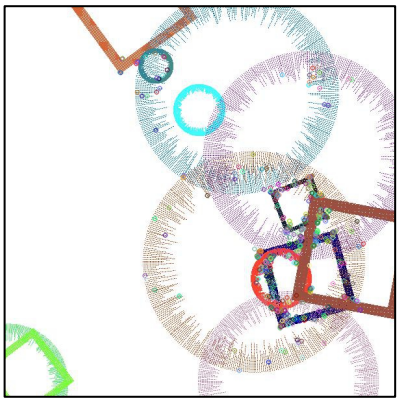

図 3 特徴量の抽出

特徴量を抽出した後，色相の比較と同様に類似度の計算を行う．上記で求めた 2 つの特徴量に対して OpenCV[12]を用いて比較を行う．この比較を行った際の比率を類似度とし，比較される対象の特徴量が近似的であるほど画像同士が類似であるといえる．

3.2.4 嗜好の学習

本節では今回認証に使用する嗜好の学習データの収集方法について説明を行う．今回提案を行う認証方式では，ただ単純に登録ユーザーの好む画像を集めるのではなく，好みの画像がなかった場合，別のどのような画像を選ぶかも重要となる．そこで教育データの収集時は以下のような流れとなる．

(1). コンピュータが 3.2.1 節の方法で複数の画像を生成し、ユーザーに提示する．
(2). 登録ユーザーはその中で好きな 1 枚を選ぶ．
(3). コンピュータは選ばれた 1 枚の画像を 9 分割し，どの部分が好きかをユーザーに選択させる．
(4). ユーザーは画像の中の好きな部分を選択する．
(5). コンピュータは最初に選択された画像，その画像の好きな部分の情報を記録する．

ここまでの流れを 1 セットとし，これを任意の回数行なうことにより学習データを収集する．

3.2.5 個人判別の評価値の算出

本論文では認証の際に複数の画像が提示されるため，3.2.3 節，3.2.4 節の計算を行った際，複数の類似度を得ることができる．この類似度の数列を Sn とし，その数列を要素とする集合を S とする．本節では類似度の数列 Sn が与えられた際，個人判別の評価値へ変換する方法を以下に示す．この方法の目的は Sn 内の最大値を 1 とし，最小値を 0 と表すこと，および最大値と最小値の以外の要素の，その数列の中での点数化(0<x<1)を行うことである．

(1). 数列 Sn から Sn の最小値である min(Sn)の減算を行い，S'n を作る．

$$S'n = Sn - min(S)$$

(2). S'n 全てを要素とする集合を S'とし，その S'n の中での最大値を max(S')とする．S'n の要素全てに，max(S')のマイナス 1 乗を乗算することにより，Sn の最大値を 1 としたものを S"n とする．

$$S''n = S'n \times max(S')^{-1}$$

(3). この手順で作成した S"n を個人評価値とする．

4. 嗜好による画像認証実験

4.1 実験手順

今回の実験は，以下の手順で行った．

1. 被験者 A を登録ユーザーとし，3.2.4 節を基に 6 枚の生成された画像から A の教育データを 250 セット収集した(図 4，5) ．
2. 1 節目で収集した教育データを基に， ランダムに生成された 6 枚の画像に対して，色相の比較，特徴点の比較を行い，コンピュータ側で個人判別の評価値を計算した後，被験者 A~E に好きな画像を選択させる(図 4) ．
3. 2 節で選択された画像の，個人判別の評価値を"First"と呼称し，それぞれ記録する．
4. 1 節目で収集した教育データを基に，2 節で選択された画像を 9 分割し，9 枚の画像に対して，色相の比較，特徴点の比較を行う．コンピュータ側で個人判別の評価値を計算した後，被験者 A~E に好きな画像を選択せる(図 5) ．
5. 4 節で選択された画像の，個人判別の評価値を"Second"と呼称し，それぞれ記録する．
6. 2~5 節をそれぞれ 10 回繰り返す．

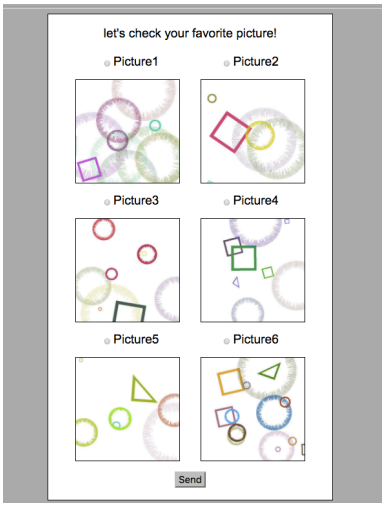

図 4 画像選択画面

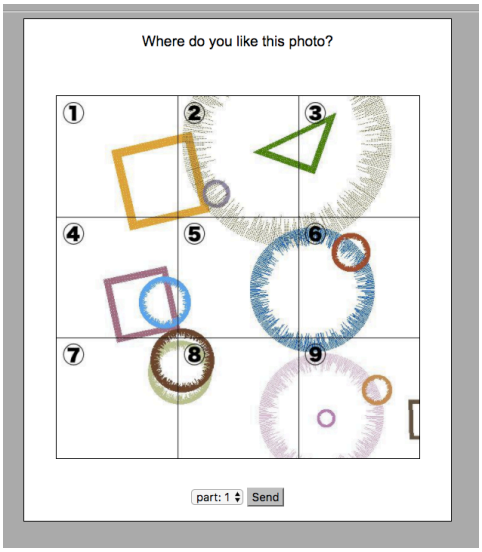

図 5 画像の好きなパーツの選択画面

4.2 実験結果

4.1 の手順で実験を行なった結果，表 1~表 5 の結果が得られた．

表 1 被験者 A 実験結果

実験回数	A			
	First		Second	
	色相比較率	特徴比較率	色相比較率	特徴比較率
1	0.0000000	0.9403744	0.8321040	0.0868058
2	1.0000000	0.8746213	1.0000000	0.1372721
3	1.0000000	0.6295305	1.0000000	0.0086782
4	0.3627634	0.4870289	1.0000000	0.0000000
5	0.9095405	0.3187679	1.0000000	0.0000000
6	0.7893693	0.5888574	0.9565779	0.1621121
7	0.4871460	1.0000000	0.9010468	0.1103095
8	0.6049778	0.2411805	0.5179245	0.4241425
9	0.9675651	0.9014976	0.6352162	0.0868598
10	0.3054138	0.1248170	1.0000000	0.0000000
平均	0.6426776	0.6106675	0.8842869	0.1016180

表 2 被験者 B 実験結果

実験回数	B			
	First		Second	
	色相比較率	特徴比較率	色相比較率	特徴比較率
1	0.3244462	0.4677857	0.6970131	0.0445913
2	1.0000000	1.0000000	0.0754517	0.4592951
3	0.9215464	0.4223858	0.9903385	0.1704693
4	0.0000000	0.3489415	0.1955136	0.1056090
5	1.0000000	0.0000000	0.3874613	1.0000000
6	0.4053643	0.2900587	0.0000000	0.0141087
7	0.1809001	0.4944674	0.9877020	0.2013833
8	0.1464353	0.0000000	0.0941844	0.0000000
9	0.6893209	1.0000000	0.8648855	0.0855410
10	0.2575618	1.0000000	1.0000000	0.2219224
平均	0.4925575	0.5023639	0.5292550	0.2302920

表 3 被験者 C 実験結果

実験回数	C			
	First		Second	
	色相比較率	特徴比較率	色相比較率	特徴比較率
1	0.9247008	1.0000000	0.8692106	0.0276535
2	1.0000000	0.0000000	1.0000000	0.0428566
3	0.8799968	0.0677869	0.7859918	0.1786281
4	0.1029839	0.0404397	0.3766203	0.2005589
5	1.0000000	1.0000000	1.0000000	0.2888091
6	0.3945680	0.3757513	0.5920080	0.0349400
7	0.6915613	0.8767106	0.5422335	0.7394425
8	0.0747461	0.6623473	0.6464816	0.0010779
9	0.0000000	0.0000000	0.1662078	0.8290992
10	0.4317347	0.7866624	0.7800221	0.0000000
平均	0.5500292	0.4809698	0.6758776	0.2343066

表 4 被験者 D 実験結果

実験回数	D			
	First		Second	
	色相比較率	特徴比較率	色相比較率	特徴比較率
1	0.0803599	0.4117576	1.0000000	0.2395592
2	0.0000000	0.2853689	0.8754665	0.1068838
3	0.9247361	0.0608621	0.9339122	0.1012872
4	0.9126125	0.1854113	0.7235870	0.1386177
5	0.8752839	0.0510763	0.8883453	0.1083087
6	0.2848462	0.5254782	0.8047698	0.5088230
7	0.3715160	0.9401077	0.0627781	0.3376008
8	0.1827795	0.0196956	1.0000000	0.0249326
9	0.7490480	1.0000000	1.0000000	0.0410634
10	0.6452600	0.0522302	1.0000000	0.1648863
平均	0.5026442	0.3531988	0.8288859	0.1771963

表 5　被験者 E　実験結果

実験回数	E			
	First		Second	
	色相比較率	特徴比較率	色相比較率	特徴比較率
1	0.00000000	1.00000000	0.95825671	0.42319779
2	0.39006259	1.00000000	0.67621166	0.02383561
3	0.00000000	1.00000000	0.59254581	0.04082949
4	0.00000000	0.16331899	0.12010436	0.00612129
5	0.29563758	0.37200907	0.75847296	0.00000000
6	0.32568008	0.95639394	0.92507679	0.09929787
7	0.33092286	1.00000000	0.35232218	0.20121473
8	0.00000000	1.00000000	0.42164639	0.14624325
9	0.00000000	0.94054743	0.82369420	0.00000000
10	0.19632734	0.50909535	1.00000000	0.16783961
平均	0.15386304	0.79413648	0.66283311	0.11085796

5. 考察

表 1 は被験者 A の学習データ 250 セットを使用して個人判別を行い, 表 2~5 は A とは他人の関係である人物で A と同じ条件下で個人判別を行なった結果である．A に対する実験結果である表 1 と，A 以外に対する実験結果である表 2~5 を比較してみる．

表 1 は First で色相, 特徴量の評価値を 6 割取れているが, 表 2~4 の First, Second ともに評価値が約 5 割という結果になった．E の結果である表 5，First の特徴量の評価値に関しては，約 8 割となっているが，対し色相の評価値が 2 割以下となっている．これらのことから，今回の実験結果を基に認証の基準を First の場合は色相, 特徴量の判別値をそれぞれ 6 割以上の場合に本人と仮定した場合，嗜好による認証が可能である可能性を見出せた. Second の場合, 表 1~5 全ての特徴量の判別値がほぼ 1 割~2 割となっている．今回の実験の仕様上，Second の場合は好きな画像の中から 1/9 の大きさにされた画像を選ぶこと，また，模様として使用したものが 3 種類しかないため，選択する画像の特徴にあまり差がなかったことが起因していると考えられる．しかし色相の判別値の差は顕著であり，表 1 と表 4 以外の色相比較率が 8 割以下という結果となった．ここで，表 1 と表 4 の First の結果に注目すると, 表 4 は表 1 の First の結果と色相，特徴量の差が大きく開いている．以上のことから，今回の結果を基に First の閾値を色相比較率, 及び特徴比較率を 0.6 以上, また Second の色相比較率の閾値を 0.85 以上，特徴比較率を認証に含めないことにより，A と A 以外の人間を判別できる可能性があることが判明した．

以上の結果より，本提案手法を用いることで，情報が固定されている画像やパスワードなどを用いることをせず，個人の感性による認証が行える．また，模様の種類を増やすことにより，認証時の特徴量の判別値の算出精度を向上させることができるとの考察を与える．

6. まとめ

本稿では，機械学習と筆者らが考案した手法を利用することにより，個人の判別の実験を行なった．その結果，認証の精度を上げられる可能性を見出すことができた．

今後の課題としては本稿の提案手法の精度の向上，老化による色覚変化の問題の対策，実用が可能にするためにシステムの処理速度の向上，システム設計の見直しを今後の課題として挙げる．

参考文献

[1] Mnemonic Security Inc. 最強の本人認証ソフトウェアニーモニックガード，http://www.mneme.co.jp/mne/

[2] 高田哲司，小池英樹「あわせ絵：画像登録と利用通知を用いた正候補選択方式による画像認証方式の強化法」, 情報処理学会論文誌，Vol.44，No.8，2003 年 8 月

[3] Paulson，L.D.:TakingaGraphicalApproachtothePassword, Computer，Vol.35，pp.19(2002).

[4] Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A.andMemon, N.:PassPoints:DesignandLongitudinalEvaluationofaGraphicalPasswordSystem，Int.J.Human-ComputerStudiesVol.63, pp.102-127(2005).

[5] 増井俊之.パスワードとの闘い-悩まない認証インタフェースをめざして.情報処理学会 2009 年夏のプログラミングシンポジウム，September2009.

[6] TheCAPTCHAnet(online), http://www.captcha.net/ , 2017 年 7 月 28 日アクセス.

[7] 松田 博子，名取 和幸，破田野 智美 「嗜好色とパーソナリティ特性との関係 ： 色のイメージと向性」(研究発表,第 44 回全国大会発表論文集) P.338

[8] 松田 博子，名取 和幸，破田野 智美 「嗜好色とパーソナリティ特性との関係 2 : 色のイメージと情動性」(研究発表,第 45 回全国大会発表論文集) P.258

[9] Israel Abramov, James Gordon, Olga Feldman and Alla Chavarga：Sex and vision II: color appearance of monochromatic lights (Abramov et al. Biology of Sex Differences 2012, 3:21).

[10] 北原健二 「色覚の分子生物学」(会誌「光学」 26 巻 5 号（1997 年 5 月）P.240)

[11] Marilyn E. Schneck, Gunilla Haegerstrom-Portnoy, Lori A. Lott, and John A. Brabyn : Comparison of Panel D-15 Tests in a Large Older Population (Optometry & Vision Science: March 2014 - Volume 91 - Issue 3 - p 284–290)

[12] OpenCV team 「OpenCV library」,<http://opencv.org/> 2017 年 7 月 28 日アクセス.

[13] Rublee，Ethan;Rabaud，Vincent;Konolige，Kurt;Bradski, Gary:ORB:anefficientalternativetoSIFTorSURF(2011).