社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2009－DPS－138 (14)
2009－CSEC－ 44 (14)
2009／3／5

打鍵署名を利用したパスワード認証の強化について

山村直也†, 鈴木隼人‡, ラシキア城治‡
†中京大学大学院 情報科学研究科
‡中京大学 情報理工学部

あらまし

パスワード認証はユーザＩＤとパスワードを利用し、ユーザ認証で最も一般的な手法であるが、パスワードの漏洩など問題が多い。パスワード認証を強化するために生体認証が注目されている。生体認証は身体的特徴と行動学的特徴を利用した認証の2つにわかれる。身体的特徴を用いた認証は各々ユニークな特徴を用いた認証であり、いくつか実用化されたシステムがあるが、信頼できるシステムはコストがかかる。打鍵署名は行動学的特徴の一種である。特別な機器を必要としないが、打鍵の変動が激しく特徴を捉える事が難しい。

本研究ではパスワード認証を改良し、パスワードと打鍵を利用した認証システムの研究をする。打鍵は特別なハードウェアを使用しないためパスワードとの組み合わせが有用な認証技術である。いくつかの手法を提案し、従来の手法と比較する。本研究の実験結果は提案システムの高い信頼性を示した。

User Verification Based on Keystroke and Password Information

Naoya Yamamura†, Hayato Suzuki‡, and George Lashkia[1]‡
†Graduate School of Computer Sciences, Chukyo University
‡School of Information Science and Technology, Chukyo University

Abstract

Use of login names and passwords is the most common mechanism to control user access to computer systems. However, this mechanism is no longer adequate and we need to investigate more advanced safeguards against unauthorized access to computer resources. Biometrics, the physical and behavioral characteristics that make each of us unique, are a natural choice for identification. Some systems have been developed based on physiological traits, but reliable systems require expensive hardware and software. Keystroke dynamics, which is a behavioral trait, is a good sign of identity, and it does not require a specialized hardware. However, unlike other access control systems based on biometric features, keystroke analysis has not led to techniques providing an acceptable level of accuracy. In this paper we investigate authentication systems that use keystroke dynamics in conjunction with passwords to improve security of passwords. We present a few original methods, discuss their properties, and compare them with conventional methods. Empirical results suggest that our approach can provide a secure and sufficient easy to use access control system.

1. 背景・目的

パスワード認証とはIDと対になるパスワードをキーボードより入力し、設定したIDとパスワードの組み合わせが一致していれば認証されるシステムである。しかし、推測しやすいパスワードの設定やクラッキングなどにより、他人に漏洩しやすいという問題がある。

パスワード認証を強化するため生体認証が注目されている。生体認証には指紋や網膜、虹彩などのように身体的特徴を用いて認証を行う方法と、筆跡や声紋、打鍵などのように行動学的特徴を用いて認証を行う方法がある。身体的特徴を用いた認証は専用の機器が必要なため、コストがかかる事や生体情報を利用するため、万が一偽造されてしまった場合、本人であっても認証データを変更できない事が問題である。行動学的特徴を用いた認証は普段の行動や振る舞いをパターン化し、認証に利用するが、変動しやすくパターンを捉えるための認証ルールの作成が難しい事が問題点である。打鍵署名は行動学的特徴に属する認証手法の1つであり、キーボードなどから入力する時に打鍵時間を取得し、ユーザプロファイルを形成し、ユーザプロファイルからリファレンス署名を生成する。ユーザプロファイルと認証時のデータのマッチングを行う事によって認識を行う手法である。認証時のデータをテスト署名と呼ぶ。パスワード認証のようにある瞬間だけ打鍵時間を取得し、認証を行うシステムである「静的認証」とユーザのタイピングを常に監視しなりすまし検出などを行

う「連続認証」の2つにわかれる。キーボードを用いて認証を行うためPCの認証には自然な選択であるといえるが、体調などによって打鍵が大きく変動してしまうため認証が難しい事が問題である。

本研究ではパスワードを入力する時にキーの入力時間を取得し、取得した入力時間も認証データとして加える事により、パスワード認証を強化し、万が一パスワードが漏洩した場合でも容易に認証されないシステム構築を目指す。

先行研究の多くは認証ルールに属性と定数を比べるpropositional ruleを使用している。多くのデータマイニングの場面でpropositional ruleは良い結果を示すが、変動の大きな打鍵時間を扱うには不十分である。そこで、本研究ではrelational ruleを生成する。relational ruleはキー間の関係を捉えるルールを生成するため打鍵時間の変動の大きさに対応できる。さらに本研究では[4]で示すようにリズムが重要であると考える。リズムを意識したタイピングを行い、リズムを検出する事によりユーザの識別を明確に行えるようにする。以上の改善によって、よりロバストでセキュアなシステム構築を目指す。

2. 先行研究

打鍵署名の先行研究は[2-4]などがある。[2]はログイン時にだけ認証を行う静的認証のための手法である。ユーザが「ユーザ名、パスワード、姓、名」を入力した時の時間データを取得する。使用する時間データはdigraph(あるキーを押してから次のキーを押すまでの時間)である。初回に数回タイピングを行い、時間データを取得し、リファレンス署名を生成する。認証を行いたい時に取得した時間データをテスト署名とする。リファレンス署名とテスト署名とをL1ノルムを用いて比較し、認証する。しかし、[2]は入力された打鍵時間を直接閾値と比べるpropositional ruleを生成するため、打鍵署名のように変動の激しさを捉えきれない。よって精度は本人が拒否される確率が13.3%、他人を受け入れてしまう確率が0.17%と他人は拒絶するが、本人であっても認証出来ない確率が高くなってしまっている。ユーザIDとパスワードの他に姓、名といった情報も必要とするため、ユーザの利便性を損なう恐れがある。

[3]はタイピングを常に監視し、長いテキストを扱う連続認証を行うための手法である。ユーザの全てのタイピングの打鍵時間を取得する。時間データとしてtrigraph(あるキーを押してから2つ隣のキーを押すまでの時間)を取得する。過去の時間データの属性を小さい順に並び変えたデータからリファレンス署名を生成し、認証する時の時間データの属性を小さい順に並び変えたデータをテスト署名とする。リファレンス署名とテスト署名の比較にはtrigraph属性の位置の違いを利用する。2つの時間データの差の求め方を図 1に示す。[3]はrelational ruleを生成するため、打鍵の変動に対してロバストであるが、連続認証であるため、長いテキストを必要とする。

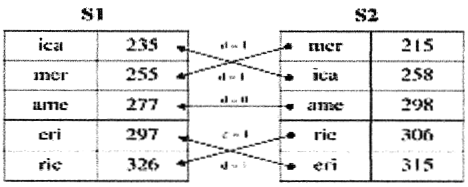

図 1. 距離の求め方

[4]は[2]の手法を用いてリズムを意識したタイピングの実験の結果、精度が改善したためリズムを意識したタイピングの有効性を示した。

打鍵署名を商用利用した例として、アメリカのAdmitOne Securityあり、トータルセキュリティソリューションとして打鍵署名を利用したセキュリティ製品を提供している[1]。AdmitOne Securityは打鍵署名を静的認証として使用し、ログインなどのユーザ認証に利用している。

3. 提案手法

本研究では1回分のdigraphを1個ベクトルであると考える。打鍵時間ベクトルから特徴抽出処理を行い、特徴ベクトルに変換する。特徴ベクトルを認証に使用する事によって、打鍵時間の変動に対応する。つまり、n文字の打鍵時間はn次元のベクトルであると考える。また、リズムを意識したタイピングを行う事で打鍵の変動を抑え、精度の向上を図る。本研究で提案する手法では以下の手順にそって認証を行う。認証の流れを図 2に図示する。

1. ユーザ登録時に数回のタイピングを行い、ユーザプロファイルとして保持する
2. 認証時に入力したユーザIDとパスワードが一致するかをチェックする

3. 認証時に取得した時間ベクトルを特徴抽出ユニットに通して、特徴ベクトルに変換する。この時の特徴ベクトルをテスト署名とする
4. ユーザプロファイルに保持された時間ベクトルを特徴抽出ユニットに通して、特徴ベクトルにする。この時の特徴ベクトルからリファレンス署名を計算する
5. リファレンス署名とテスト署名を比べる事によって認証を行う
6. 認証に成功した場合、取得した時間ベクトルをユーザプロファイルに加える

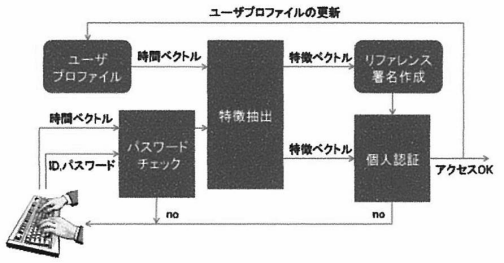

図 2. 認証手順の流れ

本研究では特徴抽出、個人認証処理が異なる6つの手法を提案する。

最初の2つの手法はordinal measure法[5]を利用して認証を行う。取得した時間ベクトルの各属性の順位付けを行い、ランクベクトルを得る。以下に例を示す。[president]がパスワードであり、時間ベクトルが以下の通りの時、

(624, 257, 881, 698, 148, 185, 1760, 222)

ランクベクトルは以下のようになる。

(5, 4, 7, 6, 1, 2, 8, 3)

ランクベクトルを特徴ベクトルとする。ordinal measure法は2つのランクベクトルを比較するために利用する。2つの時間ベクトル π_1, π_2 から以下の式を用いてベクトル S を作成する。

$$S^i = \pi_2^k \quad k = (\pi_1^{-1})^i$$

π_1^{-1} は π_1 の逆行列であり、$0 \leqq i,k \leqq n$ である。ベクトル S から2つの時間ベクトルの差を以下の式を用いて算出する。

$$d = |S^i - i|$$

d が2つの時間ベクトルの差を数値化した値出る。認証ではこの値を用いる。

最初の提案手法はユーザプロファイル内の時間ベクトルとテスト署名でordinal measureによる比較を行い、ベクトル間の差の平均を求める。平均が閾値以下かどうかによって認証を行う。ユーザプロファイルのイメージを深めるために、時間ベクトルを図 3、特徴ベクトルを図 4に示す。以降、本手法をM1とする。

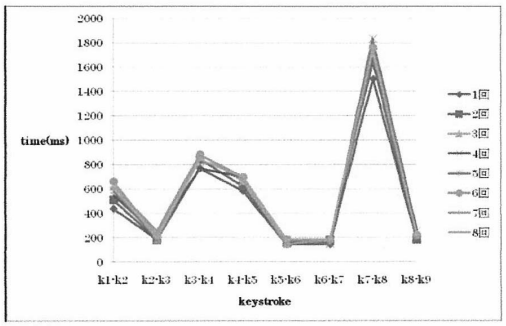

図 3. ユーザプロファイルの時間ベクトル例

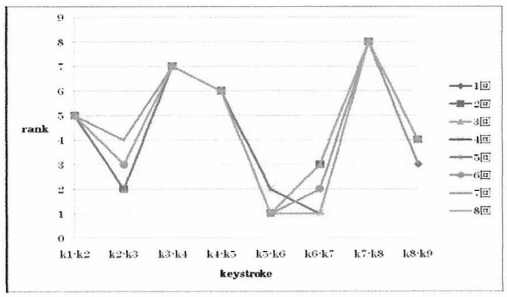

図 4. M1の特徴ベクトル例

提案手法２は最初に時間ベクトルの属性間の差を求め、差ベクトルからランクベクトルを作成し、特徴ベクトルとする。その後はM1と同様の手法で認証を行う。提案手法２での特徴ベクトルを以後はM2と記す。

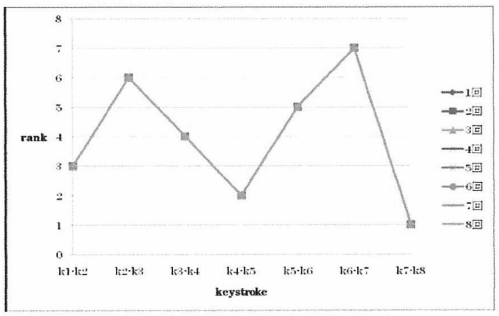

図 5. M2の特徴ベクトル例

提案手法３、４、５は個人認証処理ではユークリッド距離を用いる。つまり、ユーザプロファイルのデータとテストデータの比較をユークリッド距離によって行う。

提案手法３は離散化手法であるequal interval width法を利用する。最初に時間ベクトルを差ベクトルに変換し、差ベクトルを同じ大きさのボックスで分割する。分割した時のボックスの数を離散値とする。equal interval width法によって離散化された値を特徴ベクトルとする。離散化例を図6に示す。以降、M3と記す。

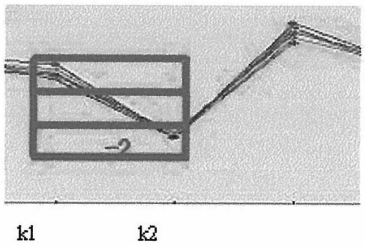

図 6. Equal interval width法による離散化例

提案手法４は時間ベクトルの比率を以下の式によって求め、比率を特徴ベクトルとする。

$$sum(T)=\sum_{i=0}^{n} t_i \qquad f_i=\frac{t_i}{sum(T)}$$

時間ベクトル$T=(t_1,t_2,\ldots,t_n)$とする。

提案手法４での特徴ベクトルの例を図 7に示す。以降、本手法をM4と記す。

提案手法５はランクベクトルの比率を利用する。最初に時間ベクトルをランクベクトルに変換し、M4と同様に比率を求め、特徴ベクトルとする。以降、M5と記す。

提案手法６はヒストグラムを利用する。時間ベクトルからヒストグラムを作成し、特徴ベクトルとする。ユーザプロファイルとテスト署名のヒストグラムをカイ2乗検定による比較する事で、認証を行う。生成されるヒストグラムの例を図 8に図示する。(以後、M6と記す。)

様々な打鍵署名に対応するため、複数の手法を組み合わせてより良い精度を目指すための手法を2つ提案する。1つ目はユーザプロファイルを作成した後に数回分のvalidationデータを用いて最も精度が良くなる手法を導く。以降の認証には導かれた手法を用いる。以降本手法をCFと記す。2つ目はmajority vote法を用いる。認証を行う時に全ての手法を並行して適応し、認証結果の多数決をとる事によって認証を行う。つまり、手法が６つあった場合は、３つ以上の手法で認証が成功した場合に、本人であると認証された事にする。本手法を以降DSとする。

また、本研究では打鍵の変動を緩和するために平滑化処理としてガウシアンフィルタを適応する。ガウシアンフィルタとは、中央部分に近いほど大きな重みを与える加重平均フィルタの一種である。中央部に平均を持つようなガウス分布を考え、このガウス分布に従うように重みを与えたフィルタの事である。

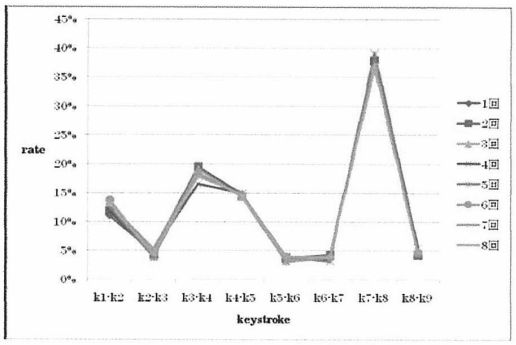

図 7. M4の特徴ベクトル例

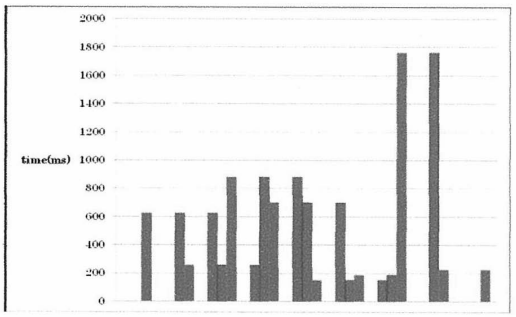

図 8. M6にて生成するヒストグラムの例

4. 実験

評価実験の前に、提案手法の閾値をチューニングするためとガウシアンフィルタの検証を行うために基礎実験を行った。基礎実験の結果、ガウシアンフィルタは適用する方が良い手法と適用しない方が良い手法がある事が分かり、M4とM6は精度が向上するためガウシアンフィルタを適用するが、それ以外の手法は適用しない事とする。

基礎実験の結果を元に評価実験を行った。評価実験は提案手法の性能を評価するために10人の学生に協力を仰ぎ、行った。実験は4週間かけて行い、リズムを覚えていられるかを調べるための実験を行った。リズムを意識したタイピングを行うために鈴木氏が作成したリズム学習支援ソフトを利用した。本ソフトはリズム作成機能とリズム学習機能がある。また、3つのカテゴリに分けて行った。カテゴリ1は英字、数字を含む一般的なパスワード、カテゴリ2はATMのようにキー同士が近く短いパスワードであり、リズムを意識したタイピングをお願いした。カテゴリ3はリズムを意識せずにタイプしたパスワードである。精度はFAR(本人拒否率)とIPR(他人受入率)を用いて測る。鈴木氏のリズム作成ソフトの有効性を図るため本ソフトを使用しない実験1と使用する実験２の2つの実験を行った。FARの実験として各カテゴリにつき、1日、10回タイピングを１週間に３日行い、全体では2週間行い、合計で1800回のタイピングを行った。IPRの実験として10人の学生が１人につき各カテゴリにつき、ランダムに３人選び、10回のタイピングを行い、全体として900回侵入を試みた。実験前に数時間、リズムを意図的につけたタイピングを著者の指導のもと練習してもらい、リズムは既存の音楽などから選んで作成した。

実験2は本研究で作成したリズム学習支援ソフトを使いリズムの学習、作成を行う実験であり、実験１と同じ要領でFAR及びIPRの実験を行った。実験前に実験1と同じく数時間のソフトによる練習を行った。

実験1、2共にリズムの練習は実験開始前1回のみとし、実験途中での練習はないものとする。本研究では先行研究として良く知られている[2]とrelational ruleを生成する[3]を比較対象とする。本実験では[2]、[3]と提案手法のM1、M2、M3、M4、M5、M6と複合手法DS、CFを対象とする。CFは先行研究も含めた多数決をとり、DSはvalidationデータを8件とする。閾値の算出には基礎実験で算出した閾値を利用する静的閾値決定手法とユーザプロファイルを作成する時にvalidationデータを用いて手法ごとに本人が最も認証される中で最も値が小さくなる閾値を算出する。算出した閾値にα値を加算した値をユーザの閾値とする動的閾値決定手法の2通りの方法が考えられる。本研究では両手法を検証した。また、リズムの学習ができているかを検証するため練習直後のデータのみを使用した実験も行った。実験1の静的閾値決定手法を用いた結果を表 1、表 2に示す。M6だけは動的閾値決定手法の結果も示す。表 1はFARを、表 2はIPRをそれぞれ示す。表の精度はM6が実験1の動的閾値決定手法を用いた精度、それ以外は実験1の静的閾値決定手法を用いた精度を記している。[2]ではFARは5%以下、IPRは1%以下が許容できる範囲であるとしている。本研究でも[2]の許容範囲を利用して精度を確認する。カテゴリ1の[3]、静的M6、CFのFARが許容できる範囲であり、カテゴリ2のM2、M6のFARとカテゴリ3の[3]、M6のFARも許容できる。IPRはカテゴリ1の[2]、M3、CF、カテゴリ２の[2]、M3は許容できる範囲である。

5. 考察

閾値の決め方には動的閾値決定手法と静的閾値決定手法の2通りが考えられる。本実験の結果、動的閾値決定手法は静的閾値決定手法と比べ精度が悪くなっている。動的閾値決定手法はFARの精度だけで判断しており、FARとIPRはトレードオフの関係があるため、FARもしくはIPRのどちらかに偏ってしまっていると考えられる。しかし、M6は精度が良くなっており特にカテゴリ2でFARが4.36%、IPRが9.09%と比較的良い精度を示した。この事からもM6はATMなどのシステムで効果が期待できる。静的閾値決定手法でもM6が最も精度が良かった。複数の手法を組み合わせる手法はDSよりCFの方が良い精度を示した。これは、より良い手法は動的に変化していくためであると考えられる。また、リズム学習支援ソフトを利用した実験2は実験1に比べて精度が悪かった。実験１は元から親しみのあるリズムを使用し、実験２は新しくリズムを作成しリズムの学習を行ったものであり、リズム学習支援ソフトを用いたリズムの学習が不十分であったと考えられる。しかし、練習直後の10回分のみを利用した精度は実験2の精度が実験1と比べて優れていた。カテゴリ2では特に精度が向上した。カテゴリ2はパスワードが短いため特にリズムを意識したタイピングが難しい事からも学習支援ソフトは有効である事を示している。

6. まとめ

本研究では、打鍵署名を利用してパスワード

表 1. FAR

Data Category	[2]	[3]	M1	M2	M3	M4	M5	M6 静的	M6 動的	CF	DS
1 (all keys)	53.22% ±35.22	3.92% ±4.15	13.07% ±18.46	11.69% ±19.55	34.28% ±27.44	5.01% ±3.13	38.93% ±37.73	3.35 ±6.11	5.30% ±11.01	3.94% ±4.74	6.53% ±8.67
2 (PIN)	61.00% ±29.61	7.21% ±8.48	9.42% ±18.02	0.24% ±0.64	76.47% ±27.52	44.93% ±29.15	66.34% ±31.21	61.94 ±27.42	4.36% ±3.29	35.05% ±26.13	8.69% ±17.73
3 (free style)	16.40% ±12.23	3.39% ±4.08	18.45% ±31.40	14.00% ±32.62	27.25% ±20.20	17.81% ±9.01	38.00% ±38.73	6.24 ±3.68	3.48% ±2.87	9.79% ±10.04	5.47% ±5.37

表 2. IPR

Data Category	[2]	[3]	M1	M2	M3	M4	M5	M6 静的	M6 動的	CF	DS
1 (all keys)	0.00% ±0.00	23.94% ±31.49	13.80% ±18.66	15.06% ±19.07	0.00% ±0.00	1.05% ±1.67	34.29% ±39.22	4.86 ±7.70	2.57% ±4.87	0.57% ±1.40	15.44% ±20.60
2 (PIN)	0.00% ±0.00	61.58% ±18.46	48.28% ±20.37	64.52% ±19.61	0.00% ±0.00	4.53% ±10.41	4.60% ±10.72	1.70 ±4.51	9.09% ±11.81	2.27% ±6.01	43.56% ±25.89
3 (free style)	12.43% ±22.00	73.88% ±23.94	50.98% ±33.93	65.81% ±28.97	25.30% ±34.12	18.34% ±14.67	56.32% ±46.18	22.73 ±26.70	27.96% ±28.81	19.58% ±17.91	63.41% ±30.83

認証を強化する事に主眼を置いた。relational ruleを生成する6つの手法を提案した。打鍵の変動を緩和するために平滑化手法であるガウシアンフィルタの適用を検討した。また、複数の手法を組み合わせる事によって精度の向上を図った。本研究では動的閾値決定手法と静的閾値決定手法の2手法を用いて実験を行い、両手法の有効性を検証した。

評価実験ではパスワードを3つのカテゴリに分け、10人のユーザに対して、長期間にわたる実験を行った。静的閾値決定手法を用いて先行研究の[2]、[3]と精度比較を行い、先行研究より優れ、M6は比較的長く、リズムを意識したタイピングを行った場合に許容できる範囲の精度を示した。複数の手法を組み合わせる事でより精度が向上する事を示した。動的閾値決定手法はあまり良い精度を示さなかったが、カテゴリ2のM6は良い精度を示した。この事からM6の動的閾値決定手法の効果は期待できる。また、評価実験により一定のリズムを長期間にわたって保持し続けられる事を示した。これらにより、認証システムのセキュリティを高めるために長いパスワードを使用する選択を行う代わりに、比較的短いパスワードにリズムを加える事でよりセキュリティを高められる事を示した。また、パスワードの長さが限られているシステムでは特に有用である。しかし、カテゴリ2は精度を許容できる範囲にまで改善出来ていないため、短いパスワードに特化した認証ルールの作成が今後の最大の課題である。また、リズム学習支援ソフトは長期間にわたってリズムを定着させるには至っていない。そのため、さらなる改善が必要であると考えられる。

参考文献

[1] AdmitOne Security, http://admitonesecurity.com/

[2] Joyce R, Gupta G:Identity Authentication Based on Keystroke Latencies, Communication of the ACM, Vol.33, No.2 (1990) 168-176

[3] Bergadano F., Gunetti D., Picardi C. : User Authentication through Keystroke Dynamics, ACM Transactions on Information and System Security, Vol 5, Issue 4, (2002) 368-397

[4] 小越康弘, 日名田明, 広瀬貞樹, 木村春彦 : 打鍵間時間を基にした認証システムのリズム打鍵による改善, 情報処理学会論文誌, Vol.44, No.2 (2003) 397-400

[5] Bhat D. N., Nayar S. K. : Ordinal Measures for Image Correspondence, IEEE Trans, PAMI vol.20, No.4 (1998) 415-423

[6] Dymitr Ruta, Bogdan Gabrys : Classifier Selection for Majority Voting, Information Fusion , Vol 6, Issue 1, (2005) 63-81