

# レーザー誘起クラックを応用した 個人認証装置の試作とその性能評価

時田 大作\*, 渡辺 一弘\*

A performance evaluation of identification module  
for personal identification method using laser-induced crack

Daisaku TOKITA\*, Kazuhiro WATANABE\*

Various personal identification methods have been so far used for one of the indispensable elemental technologies to offer more secure social services. This paper describes a practical scheme of a newly developed personal identification method which combined laser-induced crack and speckle pattern as a basic operational principle. A possible scheme has been investigated in terms of the key location accuracy, the image processing time required for pattern matching, and a compact design of ID reader, resulting in its performance evaluation. Additionally, the identification accuracy is statistically evaluated by introducing the same way as conventional biometric identification to determine the security level of the method for services of interest. As a result of this evaluation experiment, the false rejection rate (FRR) and the false acceptance rate (FAR) have been discussed for 300 identification keys created by an ID writer. Prospective picture of this method has been demonstrated by practical performances of the ID reader which are the key location accuracy of  $\pm 10\mu\text{m}$ , the image processing time  $\leq 0.62$  second, and the high identification accuracy with  $\text{FRR} \leq 1\%$  and  $\text{FAR} \leq 0.0067\%$ .

**Key Words:** Personal identification, practical performance evaluation, Laser-induced crack, Speckle pattern

## 1. はじめに

近年、個人認証技術は各種のサービスを構築する上で重要な要素技術の一つとなっている。一般的に個人認証の手法はその対象により3種類に分類されている。(1)パスワードや暗証番号のような本人しか知り得ない情報を対象とした記憶による認証、(2)印鑑やカードなどの本人の持つ所有物による認証、(3)指紋<sup>1)</sup>や虹彩<sup>2)</sup>といった身体的特徴や、声紋<sup>3)</sup>、筆跡<sup>4)</sup>などの本人の動作を対象とした生体情報による認証の3種類であり、現在までに様々な認証手法が開発されている。所有物による認証では偽造に対して脆弱であり、磁気ストライプカードはスキミングにより簡単に偽造されてしまう。偽造に強いといわれるICカードであっても、内部の情報を読み出す様々な攻撃法が存在し、カード情報が流出した場合には容易に偽造されてしまう。また、生体情報による認証は偽造に強いとされているが、生体情報は第三者による不同意収集が可能なものも多く、そこから生体情報を模した人工物を作成することで認証されてしまう

ことがある。実際に指紋認証においては、ゼラチンで作製したグミ性人工指により認証されることが確認されている<sup>5)</sup>。

筆者らはレーザー加工とスペckルパターンを用いた個人認証手法を提案し<sup>6)</sup>原理的に可能であることを実証した。この手法では、短パルスレーザーにより透明部材内部にレーザー誘起クラックを生成し、その不規則な形状を認証の対象となる認証キーとしている。これらのパターンは偶発的に生成されるので複製は不可能である。認証キーから得られるスペckルパターンを解析・照合することで個人の識別を行なう。すなわち、この手法は原理的に偽造不可能な認証キーを用いることで、従来の認証手法の弱点であった偽造に対して非常に高い耐性を有する安全な個人認証手法を実現している。また、認証の対象となるクラックのような3次元ランダム位相物体をレーザー加工により簡便に作成するという利点<sup>6)</sup>を有している。

本論文では、この偽造不可能な認証手法を実用化する上で必要な条件を検討するために、認証装置を試作し、その性能を評価した。試作した装置は、実用性を考慮し小型化可能な構成を有している。特に、重要と考えられるものは認証キーの設置の再現性およびそれに関連した画像処理技法の工夫である。また、画像処理に要する時間も認証精度を維持した上で十分に短いものでなくてはならない。

\* 創価大学大学院工学研究科 八王子市丹木町 1-236

\* Graduate School of Engineering, SOKA University,  
1-236, Tangi, Hachioji  
(Received February 5, 2009)

更にこの種の認証手法では、認証精度によってセキュリティーレベルや利用するサービスが決定されている<sup>7)</sup>。そのためこの手法においても認証精度は、実用にあたって重要な意味を持ち、生体情報による認証と同様の評価を行なう必要がある。本研究では、比較的現実性のある認証キーの設置精度 ( $\pm 10 \mu\text{m}$ )、認証時間 (0.62 秒以下)、が可能となり、あわせて高い認証精度 (本人拒否率 = 1%, 他人受容率 = 0.0067%以下) が達成され、実用化の指標を明らかにすることができた。

このレーザー誘起クラックの認証キーは、携帯するという意味ではカードなどの利便性と同一程度といえる。一方、耐偽造性を極めて高めたことにより認証精度の評価は、カードのようにデジタル数値の照合によるものとは異なる。すなわち複製不可能な不規則な画像データを照合することによりおこなうもので、生体情報による認証の処理過程と同じになる。生体情報の認証では常に正しい認証がされるとは限らないので、誤った認証が起こる確率により精度の評価が行なわれている。

## 2. 認証原理と精度評価方法








### 2.1 認証原理

本認証手法は内部にクラックを誘起した透明アクリル部材を認証の対象である認証キーとした所有物による認証である。アクリルは、高い透明度と耐衝撃性を有する非結晶性の高分子材料である。このアクリル部材の内部に強力な短パルスレーザーを集光照射した場合、光強度が高まることで多光子吸収が発生し、表面を傷つけることなく集光点近傍のみが選択的加工される<sup>8)</sup>。このとき発生するクラックはアクリル部材の局所的な結合力の差により、同一の照射条件で加工を行なっても、同一の形状となることはない。そのため、認証キーの意図的な複製が困難である。この認証キーから得られるスペックルパターンとあらかじめ取得しておいたパターンとを照合することで個人を識別する。

スペックルパターンは、レーザーのような可干渉性の光を粗面などに照射した際の反射光や透過光中に現われるランダムな粒状模様であり、簡便な光学系で取得することができるという特徴を持っている<sup>9)</sup>。認証キーを粗面と見立てて参照光を照射した場合、照射されたレーザーはクラックにより複雑に屈折、散乱することでスペックルパターンを形成する。形成されるスペックルパターンは、クラックの形状に依存してそれぞれ異なるパターンとなる。これらのパターンの照合により認証キーを識別することで、個人を認証している。

認証手法において、利便性、認証性、耐偽造性は互いにトレードオフの関係にあり、それぞれに一長一短がある。本手法は、偽造不可能な認証キーを用いることで、従来手法の欠点であった偽造に対して非常に耐性の高い安全な認証を提案している。また、ランダムな干渉パターンであるスペックルパターンからは、クラックの形状を推測することは困難であり、パターンの流出に対しても優れた安全性を有している。その一方で、前述のとおり認証キーを携帯することから利便性は所有物による認証と同程度でありながら、認証精度の評価は、生体情報による認証と同様に確率的な認証となっている。つまり本手法の認証精度は、カードのような所有物による認証

Table 1 False rejection rate (FRR) and false acceptance rate (FAR) of each biometric identification.

Biometric information	FRR[%]	FAR[%]
 Fingerprint	1.0	0.01
 Palmprint	0.1	0.1
 Face	5	5
 Iris	10	$1.0 \times 10^{-6}$
 Voiceprint	10	10
 Signature	5	5
 Vein	1.0	0.01

ではなく、生体情報による認証と比較を行なうのが適当であり、同様の評価を行なう必要がある。

### 2.2 認証精度評価方法

生体情報による認証では、認証の対象となる生体情報は、終生不変、万人不同の性質を持つ指紋や虹彩のような身体的特徴と声紋や署名のような行動的特徴が用いられている。しかしながら、これらのパターンは入力時の環境や本人の状態、リーダーへの入力の仕方などによって、取得するたびにわずかながら変化してしまう<sup>10)</sup>。その結果、パターン照合の結果にばらつきが生じ、本来認証すべき本人を拒否してしまう場合や、拒否すべき他人を認証してしまう誤認証が発生する。これらが発生する確率をそれぞれ本人拒否率 (False rejection rate: FRR) と他人受容率 (False acceptance rate: FAR) としている。FRR は手法の利便性を示し、FAR は手法の安全性を示す値であり、この二つの値により認証精度が評価されている<sup>11)</sup>。また、FRR と FAR は認証閾値により値が変化し、互いにトレードオフの関係にある。

生体情報による認証では、手法ごとに FRR, FAR が異なる値をとる。Table 1 に一般的に用いられている生体情報による認証の FRR と FAR を示す<sup>12)</sup>。生体情報による認証において、最もセキュリティーレベルが高い手法は虹彩認証である。虹彩認証は FAR が  $1.0 \times 10^{-6}\%$  と他の手法に比べてきわめて低い値を示しているが、FRR は 10% と高くなっている。汎用的に用いられている指紋認証や静脈認証での FRR, FAR はそれぞれ 1%, 0.01% である。本手法は広汎な運用を想定しており、その実用には汎用性の高い認証精度が必要である。そのため、少なくとも、生体情報による認証において汎用的に用いられている程度以上の精度があれば、本手法は実用上十分な汎用性を持つといえる。

FRR と FAR の評価は、複数の被験者から生体情報を取得し認証を行なうことでそれぞれの値を算出する。このとき問題となるのが照合に用いるサンプル数である。米国のバイオメトリクステストセンタによると、信頼度 95% において、サンプル数  $S$  で評価可能な

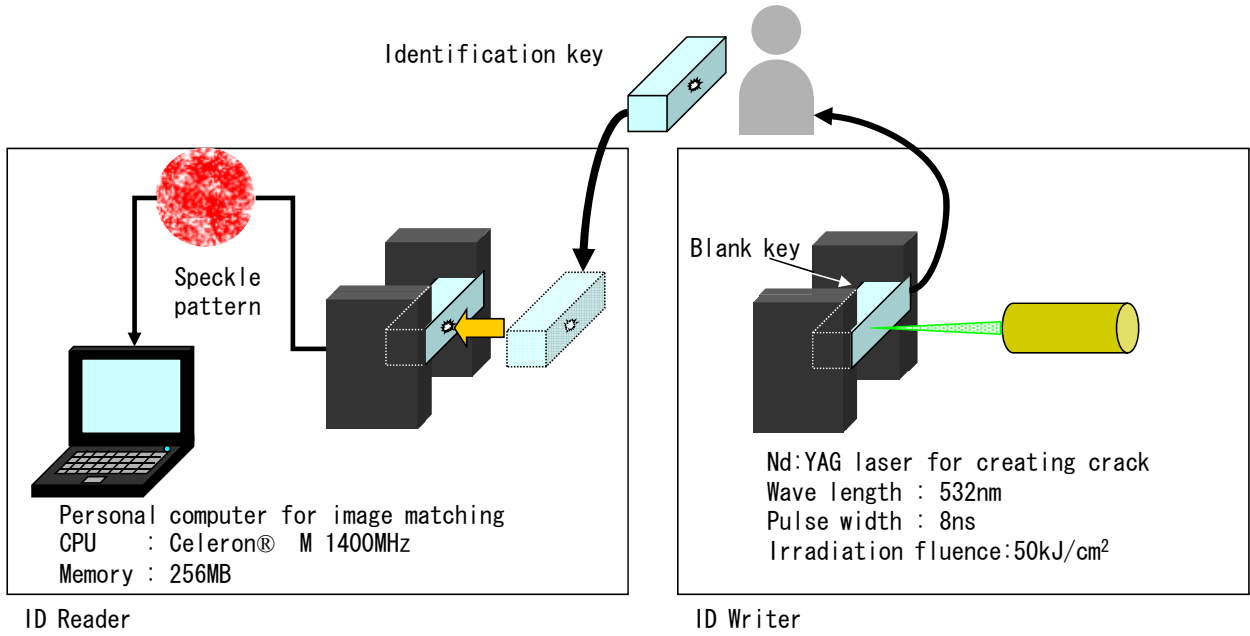


Fig.1 Conceptual diagram of identification system

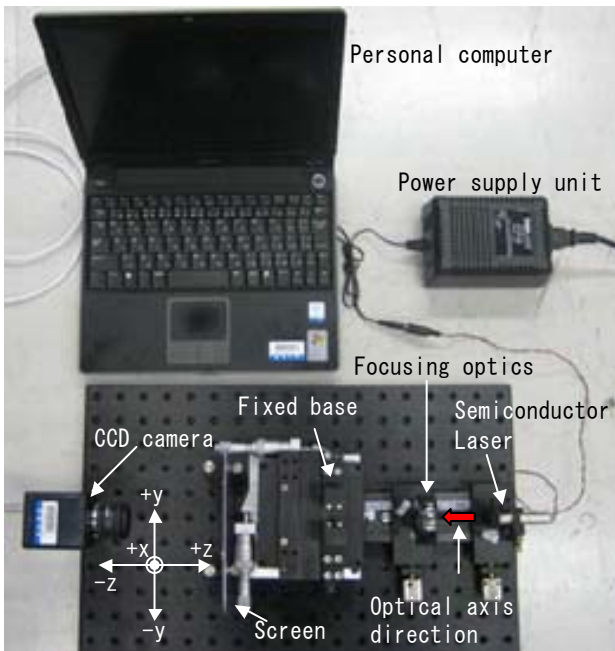


Fig.2 Experimental apparatus.

FRR と FAR の評価限界値はそれぞれ

$$FRR = 3/S \quad (1)$$

$$FAR = 6/S(S-1) \quad (2)$$

で表される<sup>13,14)</sup>。これらの式から、評価したい FRR, FAR に必要なサンプル数を計算することが可能である。本手法の有用性を示すために汎用的に用いられている指紋認証や静脈認証と同程度の

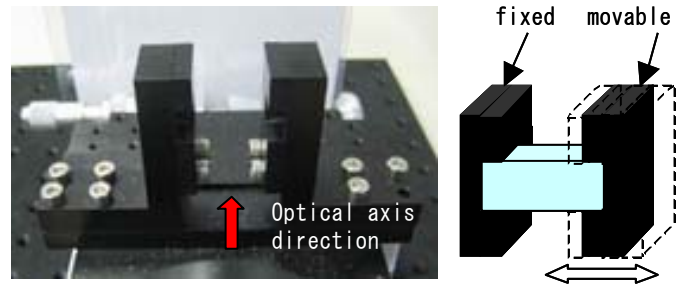


Fig.3 Structure of fixed base.

FRR=1%, FAR=0.01%程度を目標として精度を評価する。これらの FRR および FAR の評価に必要なサンプル数は、それぞれ 300 サンプルと 246 サンプルである。そこで本評価実験においては 300 サンプルの認証キーを作成し評価を行なう。

### 3. 認証装置

Fig.1 に本研究室で開発した個人認証手法のシステム構成図を示す。本認証システムは透明アクリル部材 (ブランクキー) にクラックを生成することで認証キーを作成する IDライターと、認証キーからスペckルパターンを読み出し、パターン照合を行なう IDリーダーで構成されている。本論文では認証装置として IDリーダーを試作し、その性能を評価することで、認証手法の実用化の条件を検討する。

IDライターにはクラック生成用のレーザーとして Nd:YAG レーザー (波長 532nm, パルス幅 8ns) を用いた。出力されたレーザーは、集光光学系により照射エネルギー密度 50 kJ/cm<sup>2</sup> で集光照射され、透明アクリル部材の内部にクラックを生成する。クラックは一箇所ごとに一回の照射により生成している。クラックは部材内部の任意の位置に、任意の数だけ生成することが可能であり、簡単に 3次元ランダム位相物体を生成することが可能である。

作成された認証キーから IDリーダーによってスペckルパターンを取得し、そのパターンを照合により認証キーは識別される。す

なわち、IDリーダーによって最初のスペックルパターンを取得した時点で、IDライターでクラックを生成された部材は認証キーとして登録される。クラックの生成位置はライターとリーダーで共有され、秘匿されており、それにより登録時のリーダーの照射位置条件がクラックのどの部位に照射しているかという点で秘匿されることになる。Fig.2に実際に本研究で試作したIDリーダーの構成を示す。参照光には実用面を考慮し、小型の半導体レーザー（波長635nm、出力1mW）を用いた。出力光は集光光学系によりスポットサイズ16 $\mu\text{m}$ で集光されクラックに照射される。これにより表面状態の影響を可能な限り除去している。本研究の特長は、ライターとリーダーはクラックの位置座標を共有しており、一種の秘匿条件となっていることである。したがって、リーダーの固定台と光学系はその位置座標を再現するように初期の段階で調整されている。これにより、決められた方向でキーを固定台に押し付けることにより、認証キーは常に同一の位置に参照光が照射されるように固定台に固定される。本実験では、アクリル部材の個々の大きさのバラツキを吸収するために、Fig.3に示したような固定台の長手方向の一方を固定側とし、他方を可動側として設けた。認証キーの保持は、固定側の側面と底面に認証キーを沿わせるように押し付け、その後可動側の位置を手動で調節して押し付けを補助した。固定側の側面、底面、端面からの距離はライターの条件を保存しており、その条件を秘匿する。照射された参照光はクラックで複雑に屈折、散乱され後方の半透過スクリーン上でスペックルパターンを形成する。このパターンはスク

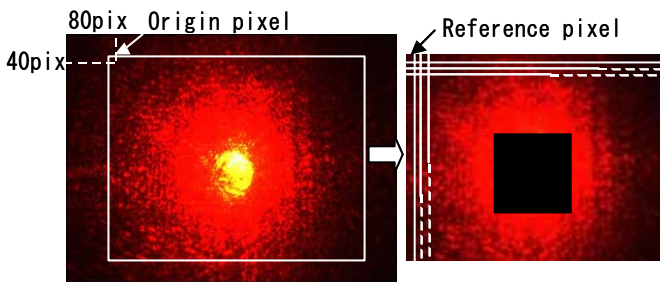


Fig. 4 A sample of template image.

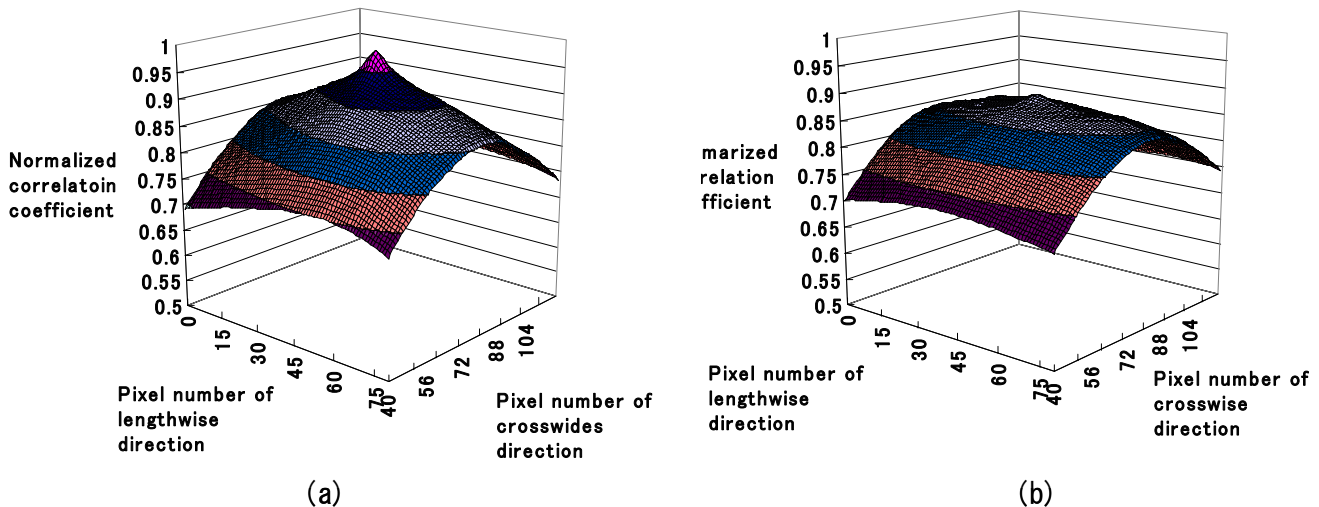


Fig. 5 Distribution of normalized correlation coefficient in the case of (a) same sample matching (b) different sample matching.

リーン背面より ARTRAY 社製 30 万画素 CCD カメラ (640pix $\times$ 480pix) で撮像される。スクリーン上に出現するスペックルパターンにおける個々の斑点の大きさは0.5mm $\sim$ 1.2mmであった。CCDカメラ1pixはスクリーン上の0.066mm四方を撮像しているため、十分にスペックルを撮像することが可能である。撮像されたパターンはPCに転送され、パターン照合処理が行なわれる。PCには一般に市販されている Celeron $\text{\textcircled{R}}$  M 1.4GHz, Windows $\text{\textcircled{R}}$  2000 搭載のものを用いている。照合プログラムは、結果の表示に柔軟性を持たせるために Microsoft 社製の「Visual C++ 6.0」で構築した。これによりパターンの取得から照合、判定までの一連の認証過程を自動で行なうことが可能になる。

#### 4. IDリーダーの性能評価

##### 4.1 画像照合方法

本手法の実用化に必要な条件の検討するために認証装置としてIDリーダーを試作し、認証に必要な時間と認証キーの設置位置精度によりその性能を評価する。本手法はテンプレートマッチング法により入力パターンとテンプレートパターンの類似度を算出する。スペックルパターンは参照光の照射位置がずれた場合、出現位置が移動するとともにパターンを変化させるという性質を持つ。そのため同一サイズの画像による一回の照合では、類似度が低下し正しく識別を行なえない可能性がある。そこで本研究ではFig.4に示すような入力されるパターンよりも小さいテンプレートパターンを用いる。テンプレートパターンは、入力パターンの上を移動させながら画像照合が行なわれる。テンプレートパターンは640pix $\times$ 480pixの画像の一部を500pix $\times$ 400pixに切り取ったものを用いている。切り取りは元画像の左上端の画素より横方向に80pix、縦方向に40pixの位置から切り取ったものであり、この画素を基準座標 (Original pixel) とする。また、テンプレート画像の左上端の画素を参照画素 (Reference pixel) としている。これまでの研究から、出現するスペックルパターンは中心部分の輝度が非常に高いパターンになることが分かっている。この高輝度の部分により、テンプレートパターンと入力パタ

ーンの類似度が高くなることが予想される。そこで、高輝度の中心部分を除去したテンプレートをを用いることとした。スペckルパターンはクラックの結像とは違い、屈折や散乱により参照光の波面が乱された結果、複雑に干渉することで現われるランダムな粒状模様である。3次元ランダム位相物体の全体もしくは、一部に照射しようが乱された波面の影響は粒状模様のすべての領域に反映されているので、中心部分を除いてもクラックの唯一性を利用するという本手法の理論的根拠が失われるものではない。評価関数にはテンプレートマッチング法において一般的に用いられている正規化相関係数を用いた<sup>15)</sup>。正規化相関係数は1~1の間の値をとり、1に近いほど2パターン間の類似度が高いことを示す。

テンプレートパターンを入力パターン上で移動させながら照合を行なった際に得られた相関値の分布を Fig.5 に示す。入力パターンが 640pix×480pix、テンプレートパターンが 500pix×400pix であることから、参照画素を入力パターン上の座標 (0,0) から (139,79) までの間で移動させながら、合計 11200 回のマッチングを行なった。Fig.5(a)は認証されるべき同一の認証キーから取得されたパターン同士の照合、Fig.5(b)は拒否されるべき別々の認証キーから取得したパターン同士の照合の結果である。認証されるべき照合の結果、相関値は基準座標の近傍の局所領域において急峻なピークを示しているのに対して、拒否されるべき照合では、ピーク値とその他の照合に大きな相関値の差が確認できない。また、一組分の照合である 11200 回のマッチングに必要な時間は 72 秒であった。

Table 2 に相関値のピークが得られた領域とその平均値を示す。20 個の認証キーを作成し、総当りで 400 組の照合を行なった。同一

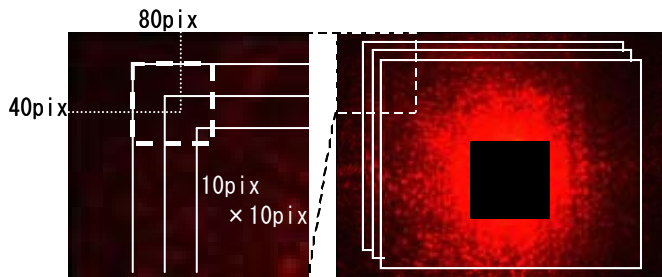


Fig. 6 Matching domain.

Table 2 Frequency of template image position shown strongly correlate at each domain.

Template image		10 × 10pixel domain around the origin pixel		Other domain	
		Frequency	Normalized correlation coefficient	Frequency	Normalized correlation coefficient
Unprocessed template	same sample	20/20	0.982	0/20	0
	different sample	265/380	0.822	115/380	0.820
Processed template	same sample	20/20	0.969	0/20	0
	different sample	214/380	0.723	166/380	0.728

認証キーから得られたパターン同士の照合は 20 組、異なる認証キーから得られたパターン同士の照合は 380 組である。使用したテンプレートは、画像を加工し中心部分を除去したものと、加工を行わない 2 種類を用いた。照合の結果、2 種類のテンプレートパターンのどちらを用いても、認証されるべき照合と拒否されるべき照合のピーク値の平均には大きな差があることが確認された。中心部分を加工したテンプレートを用いた場合にその差は大きくなり、未加工のテンプレートを用いた場合が 0.161 に対して、加工したテンプレートを用いた場合には 0.244 であった。また、認証されるべき同一認証キーから得られたパターン同士の照合では、テンプレート画像によらず基準座標を中心とした 10pix×10pix の局所領域でピーク値が検出された。拒否されるべき照合においても同様の領域でピークを検出することが多かったものの、それ以外の領域においてもピークが現われ、その割合は中心部分を加工したテンプレートの場合のほうが高くなっている。このことから、Fig.6 に示した基準座標を中心とした 10pix×10pix の領域で参照画素を移動させ照合を行なうことで認証精度を落とすことなく、照合時間を短縮可能である。

作成した 20 個の認証キーを用いて、照合領域を限定した照合を行なった結果を Fig.7 に示す。縦軸に正規化相関係数を示し横軸にテンプレートパターンを取得した認証キーの番号を示す。グラフには、中心部分を加工したテンプレートと未加工のテンプレートを用いた場合それぞれの拒否されるべきサンプル同士の平均値をプロットしている。たとえば Sample number 1 は認証キー-1 から得られたテンプレートとそれ以外の認証キー-2~20 の入力パターンとの照合の平均値である。これらの照合の結果、テンプレートを加工することにより相関値が平均的に 0.098 低下し、照合領域を限定することで一組の照合に必要な時間を 72 秒から 0.62 秒まで短縮することができた。照合時間が、1 秒以下であることから実用にあたって十分に現実的な時間で照合が行なえることが確認された。

#### 4.2 固定位置精度

本手法において、正確な認証を行なうには常に同一位置に参照光を照射することが重要である。参照光の照射位置は、認証キーの固

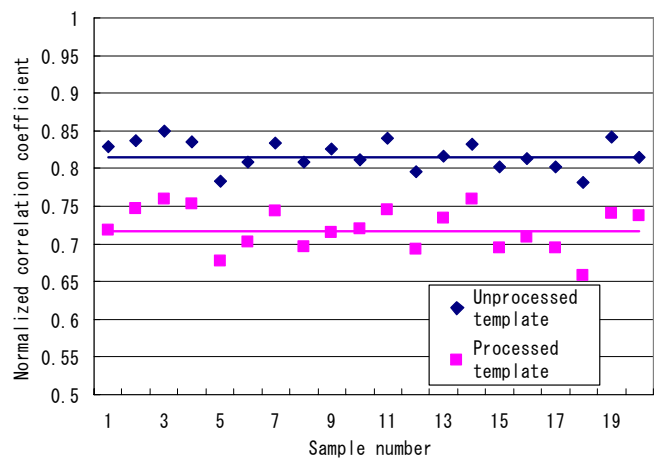


Fig. 7 Result of matching experiment in the case of two template image.

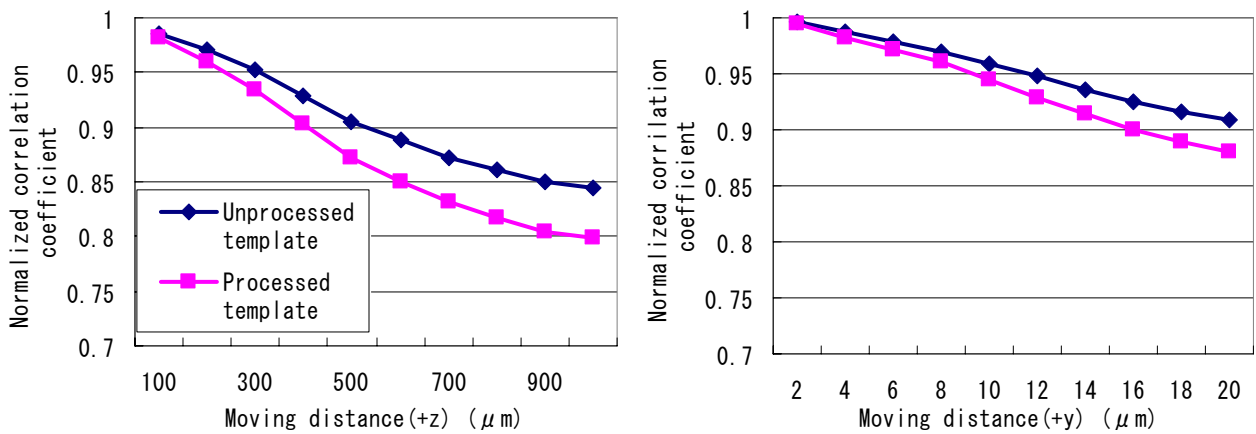


Fig.8 Results of moving experiment (a)in the optical axial direction (+z)  
(b)in the opposite optical axial direction (+y).

定位置やレーザー発振機や光学系の設置位置などによって変化する。これまでの研究では、認証キーの固定位置精度を検査することで照射位置の許容性に関する検討を行なった。

Fig.8 に認証キーを移動させながら照合を行なった場合の移動距離と相関値の結果を示す。Fig.8(a)は光軸方向(±z)に移動させた結果、Fig.8(b)は光軸に対して垂直な方向(±y)に移動させた場合の結果である。縦軸に正規化相関係数を示し、横軸に移動距離を示している。グラフには中心部分を加工したテンプレートをを用いた場合と未加工のテンプレートをを用いた場合をプロットしている。

グラフから、相関値は z 方向に対して緩やかに減少しているのに対して、y 方向の移動に対しては急激な減少を示している。中心部分を除いたテンプレートをを用いた場合は、当然ながら位置ずれによる相関値の減少がやや顕著である。本実験では、参照光をスポットサイズ 16 μm まで集光し照射しており、レイリー距離は 333 μm となっている。実験結果から認証閾値を 0.93 とした場合、z 方向はレイリー距離程度の ±300 μm、y 方向はスポットサイズの半分程度、±10 μm の移動で認証が不可能になることから、認証リーダーにはこの程度の設置精度が必要である。つまり、あえて 3次元ランダム位相形状の一部のみを利用し集光条件を秘匿することにより、唯一性を高め、認証リーダーそのものの複製を困難にしている。この程度

の精度はキーを一定の力で押し付ける程度の固定機構により十分に達成することが可能である。

## 5. 認証精度評価実験

本手法の実用性を示すために認証精度の評価を行なう。本実験では実際に複数の認証キーを作成し、そこからスペックルパターンを取得し照合を行ない、認証閾値を設定することで FRR と FAR を算出する。認証キーの生成数は 300 サンプルとし、このときの評価限界値はそれぞれ、FRR=1%、FAR=0.0067%である。

認証の対象となる認証キーには 10mm×10mm×30mm の透明アクリル角柱の内部にクラックを生成したものをを用いた。クラックは認証キーごとに 1~10 箇所 ID ライターを用いて生成する。生成位置は平均的なクラックの長さが約 90 μm であったことから、参照光の照射位置を中心に 120 μm×120 μm の範囲でランダムに決定している。ただし、参照光照射位置に確実にクラックが存在するように、20 μm×20 μm の範囲に最低でも 1 箇所は生成する。深さはアクリル部材の表面から 1mm の位置とした。生成したクラックは固定台の固定側に押し付けられる側面から 11mm、底面から 2mm の近傍の位置を中心としており、本実験ではその位置に参照光が照射されめいりようなスペックルパターンが得られるように固定台の位

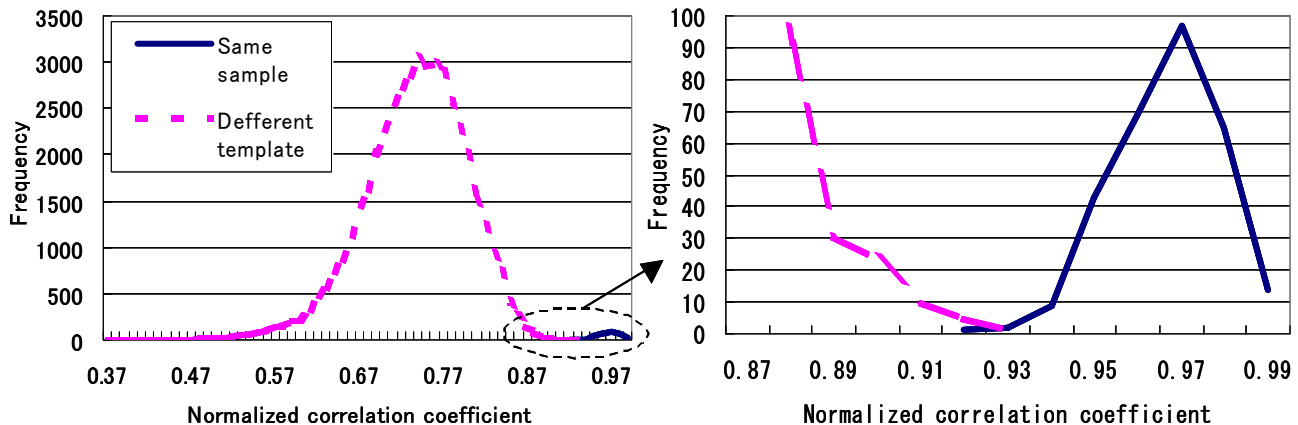


Fig.9 Distribution of matching experiment result.

置を最初に調整し、その後のこのような位置調整は一切行なわれない。

作成した認証キーから ID リーダーによりテンプレートパターンと入力パターンを各一枚ずつ取得し、パターン照合を行なう。その際、各キーのスペックルをテンプレートとして取得する際には最初に固定側に沿わせ、その後可動側で軽く押し付けるのみで位置固定を行っている。その後、同じキー同士また異なるキーと同様に固定し、数百回にわたり照合実験を行った。同一キーならばこの方法で認証が可能である。照合に際しては、認証キーA から取得したテンプレートパターンと認証キーB から取得した入力パターンの照合と、その逆に認証キーB から取得したテンプレートパターンと認証キーA から取得した入力パターンの照合は、ほぼ同一の結果が得られると考えられる。前述の(2)式においてもこの事は考慮されているため、本実験においても(2)式に従いどちらか一方の場合において照合を行なう<sup>13),14)</sup>。

照合の結果を Fig.9 に示す。このグラフにおいて、縦軸は度数を示し、横軸は正規化相関係数を示している。破線のプロットは拒否されるべき、異なる認証キーから得られたパターン同士の照合の結果であり、実線のプロットが認証されるべき同一の認証キーから得られたパターン同士の照合の結果である。このグラフから同一の認証キーから得られたサンプル同士の照合結果は0.92~0.99の範囲に局在している。一方で、異なる認証キー同士から得られた照合は0.37~0.93 という広い範囲に分布していることがわかる。また、これらの二つの分布は互いに重なり合う部分を持ち、その部分を拡大したのも Fig.9 に示してある。このような重なりあう部分を持つために認証閾値を設定した場合に本人拒否や他人受容が起きることとなる。本実験の結果からは認証閾値を0.92~0.94 に設定することが可能であることがわかる。この範囲に閾値を設定した場合の FRR と FAR を Table 3 に示す。この表から、すべての閾値においておおむね目標とした FRR=1% と FAR=0.01% を達成していることが確認できた。また、閾値 0.93 において FRR, FAR とともに評価限界値を下回ったことから、本手法は評価限界値以下の精度を持った認証手法であることが確認された。

## 6. おわりに

本論文では、レーザー誘起クラックを用いて偽造に対して極めて高い耐性をもつ認証装置を試作しその性能を評価し、個人認証手法の実用化の可能性を示した。本研究で試作した ID リーダーは、半導体レーザーの採用により、450w (幅) × 200h (高さ) × 200d (奥行) mm 程度の比較的小型なリーダーとなった。試作したリーダーによる性能評価において、認証キーの設置位置精度とそれに関連した画像処理技法を検討した。その結果、認証キーの設置位置精度は ±10 μm 程度のまでの許容性を持つことが確認され、機械的固定機構の設計指針を与えている。また、画像処理は現実的な時間で照合することが要求される。照合領域を限定することで、認証精度を維持しつつ実用に供しうる程度の 0.62 秒での照合が達成された。本研究では、画像処理には汎用 PC を用いてソフトウェア処理をしているが、この処理をハードウェア化することで、照合時間を更に短縮することが可能である。

また、試作したリーダーを用いて、生体情報による認証の精度と

Table 3 FRR and FAR of each threshold

Threshold	0.92	0.93	0.94
FRR [%]	0	0.33	1.00
FAR [%]	0.016	0.002	0

同様に FRR と FAR を用いて評価した。実験では実際に 300 サンプルの認証キーを作成し、リーダーによる照合実験を行なった。その結果、認証閾値を 0.93 に設定した場合に算出された値が評価限界値を下回ったため FRR=1%、FAR=0.0067%以下の精度を持つ認証手法であることが確認された。この値は、現在汎用的に用いられている指紋や静脈による認証と同等程度以上の精度であることから、本手法が実用上、十分汎用的な精度を持つ手法であることが示された。以上により原理的に偽造が不可能な安全性の高い認証手法を提案し、ある程度の現実性をもたせて実現することができた。

本手法で用いる認証キーは所有物と同様に通常の使用のなかで損傷や劣化が発生しうる。本手法は、運用において認証キーの寿命の範囲で認証を行なうことを想定している。現在までの研究に用いた限り(数ヶ月)認証に支障となるクラックの進展がないということが顕微鏡観察で明らかになっている。加えて、精度評価実験と同様の認証実験により正規化相関係数が認証閾値 0.93 を超えることも確認された。また、クラックを作り込んで数年間放置をした後のアクリルの表面にも大きな変化が見られていないことから、認証キーが自然のうちに短期間で急激に劣化することはないと考えている。長期的な進展に対しては認証を行なうたびにテンプレートパターンを更新するなどの運用上の工夫により認証キーの寿命を実用上、十分に確保することが可能である。

本研究において ID ライターにより透明アクリル部材に生成したクラックは、3 次元的に広がった形状有している。これらのクラックは光軸方向には 1mm 程度の長さで分布しているため、認証キーには少なくとも 2mm 以上の厚さが必要となる。クラックを生成する際に対象となるアクリルの表面に対して、レーザーを浅い入射角をもって入射させることでアクリルの深さ方向への伸長を抑制し、認証キーに要求される厚さを軽減することができる。以上より、本手法はバルク状の認証キーによる鍵としての利用のみならず、ID カードなどを用いる個人認証を必要とする多くの場面での応用が期待できる。今後、自動的な認証キーの固定機構、テンプレートパターンの保存方法などの検討と、様々な認証の場面での実地試験を行なうことで、現実的で有用な認証手法が確立できるものと考えられる。

謝辞 本研究の一部は、文部科学省私立大学学術研究高度化推進事業「私立大学社会連携研究推進事業」(平成 18 年度~平成 22 年度): 研究課題「測位/光神経複合センサノードによるユビキタス・モニタリング・ネットワークの開発とその産業応用への展開」の一環として実施したものである。記して、厚く御礼申し上げます。

また、多大な協力を頂いた、創価大学大学院工学研究科の首藤貴雄氏、佐々木正孝氏、江島春樹氏に深く感謝申し上げます。

## 参考文献

- 1) M.Kawagoe, A.Tojo: Fingerprint pattern classification, Pattern Recognition, **17**-3, 295/303 (1984)
- 2) J. Draugman: How iris recognition works, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, **14**-1, 21/30 (2004)
- 3) 松井 知子, 黒岩 眞吾: 音声による個人認証技術の現状と展望: 今, なすべきことは何か!, 電子情報通信学会誌, **87**-4, 314/321 (2004)
- 4) 吉村 ミツ, 吉村 功: 筆者認識研究の現段階と今後の動向, 電子情報通信学会技術研究報告. PRMU, パターン認識・メディア理解, **96**-141, 81/90 (1996)
- 5) 山田, 松本, 松本: 指紋照合装置は人工指を受け入れるか, 電子情報通信学会技術研究報告. ISEC, 情報セキュリティ **100**-213, 159/166(2000)
- 6) 時田, 齋藤, 櫻田, 石井, 渡辺: 透明部材内部に生成したパルスレーザー光学的損傷からのスペckルパターンによる個人認証手法の開発, レーザー研究, **35**-4, 259/264 (2007)
- 7) 瀬戸, 磯部, 三村: バイオメトリクス認証技術の精度評価の標準化活動, 電子情報通信学会誌, **83**-8, 624/629 (2000)
- 8) 林 健一: 制御可能な光学的損傷を用いたガラス基盤の内部マーキング, レーザー研究, **28**-1, 40/44 (2000)
- 9) レーザー学会: レーザーハンドブック第2版, 789/800, オーム社 (2005)
- 10) バイオメトリクスセキュリティコンソーシアム: バイオメトリクスセキュリティ・ハンドブック, 329/340, オーム社 (2006)
- 11) 瀬戸 洋一: サイバーセキュリティにおける生体認証技術, 109/131 共立出版 (2002)
- 12) 社団法人日本自動認識システム協会: よくわかるバイオメトリクスの基礎, 2/16, オーム社 (2005)
- 13) 小松, 内田, 坂野, 和田, 池野: バイオメトリクスの精度評価, 計測と制御, **43**-7, 539/543 (2004)
- 14) A. J. Masnsfield and J. L. Wayman: Best Practices in Testing and Reporting Performance of Biometric Devices Version 2.01, NPL Report CMSC 14/02, 1/32 (2002)
- 15) 村松, 小林, 高橋, 清水: テンプレートマッチングにおけるハードウェア化と高速化手法の開発, 電子情報通信学会論文誌, **J83-D-II**-7, 1667/1675 (2000)

## 【著者紹介】

時田 大作 (学生会員)



2004年創価大学工学部情報システム学科卒。2006年創価大学大学院工学研究科情報システム学専攻博士前期課程修了。現在、創価大学大学院工学研究科情報システム学専攻博士後期課程在学中。レーザーによる光情報記録に関する研究に従事。レーザー学会会員。

渡辺 一弘 (正会員)



1976年3月慶應義塾大学工学部電気工学科卒業。81年同大学院工学研究科電気工学専攻博士課程修了。81年より防衛大学校電気工学教室助手、講師、助教授を経て、91年創価大学工学部助教授。現在、創価大学工学部情報システム工学科、教授、工学研究科情報システム専攻教授、工学部長。レーザーの光情報装置への応用、光ファイバセンサ、自律移動ロボットの自己位置認識システム、ユビキタス空間の開発の研究に従事。計測自動制御学会、レーザー学会、電気学会、日本ロボット学会、応用物理学会、可視化情報学会等の会員。(工学博士)