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

2008－GN－68（11）
2008 / 5 / 23

非整数次フーリエ変換を利用したサーバーへの指紋情報登録に関する一検討

岩井 玲子† 吉村 博幸††

†千葉大学工学部 〒263-8522 千葉市稲毛区弥生町 1-33
††千葉大学大学院工学研究科 〒263-8522 千葉市稲毛区弥生町 1-33
E-mail: †reiko@tu.chiba-u.ac.jp ††yoshimura@faculty.chiba-u.jp

あらまし 近年，指紋認証による個人識別は身近なところで増加している．例えば，パソコンの自動ログインやオフィスでの入退室管理，勤怠管理などである．指紋認証では，個人の指紋情報を１度サーバーに登録してしまえば，パスワードのように覚える必要もなく，紛失する心配もない．しかし，サーバーに登録した指紋情報が漏洩してしまった場合，パスワードのように変更することができない．そこで，指紋情報を登録する際に，他者から解読できないよう暗号化されるのが望ましい．本研究では，非整数次フーリエ変換を利用した暗号化方法を提案し，その基本的特性について解析を行った．

キーワード フーリエ変換，暗号化，生体認証，指紋，周波数解析方式

Study on registration of fingerprint information with a server by use of the fractional Fourier transform

Reiko IWAI† Hiroyuki YOSHIMURA††

†Faculty of Engineering, Chiba University 1-33 Yayoi-cho, Inage-ku, Chiba, 263-8522 Japan
††Graduate School of Engineering, Chiba University 1-33 Yayoi-cho, Inage-ku, Chiba, 263-8522 Japan
E-mail: †reiko@tu.chiba-u.ac.jp ††yoshimura@faculty.chiba-u.jp

Abstract Recently, the personal identities by the fingerprint authentication have been increasing everywhere, for example, in the automatic logging into a PC, the access control and the diligence & indolence management in an office, and so on. In the fingerprint authentication, the fingerprint does not have to be remembered and there is no worry to be lost like a password, if once the information is registered with a server. The fingerprint, however, cannot be changed like a password if the information leaks out from the server. Therefore, the coding is necessary not to be able to be decoded by another person. In this study, we use the fractional Fourier transform to the method of coding, and analyze the fundamental properties.

Keyword Fourier transform, Coding, Biometrics, Fingerprint, Frequency analysis method

1. はじめに

指静脈や指紋といった，各人の持つ生体情報によって個人を識別するシステムは，さまざまな分野で使われている．しかし，生体情報は個人の固有情報であるため，パスワードのように自由に変更することができない．そのため，生体情報は人からはノイズにしか見えない画像に変換（暗号化）されサーバー内に登録されている場合が多い．

図 1 に，暗号化の一手法である，周波数解析方式の一例を示す．横方向に指紋の位置を，縦方向に指紋の凹凸（画像の濃淡）をとると，切り出された指紋画像は 1 ラインの波形とみなすことができる．この波形を解析することにより，ラインごとの離散フーリエ変換スペクトルを得ることができる．

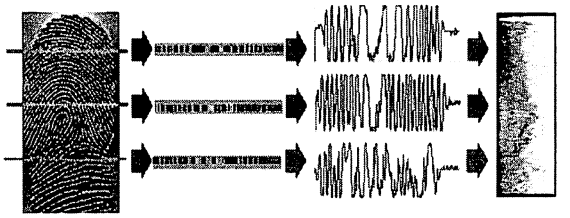

図 1　周波数解析方式の一例[1]

本研究では，新たな指紋画像暗号化の手法を検討するとともに，より解読されにくいサーバーへの登録情報を生成するため，通常のフーリエ変換の代わりに非整数次フーリエ変換を適用する手法を提案する．具体的には，指紋画像を一次元の有限矩形波と見なし，その非整数次フーリエ場の諸特性を解析する．さらに，非整数次フーリエ場の強度分布の逆非整数次フーリエ場の諸特性について解析する．

2. 非整数次フーリエ変換を利用したサーバーへの指紋情報登録手法の提案

図 2　指紋画像

図 2 に，指紋作成ツール[2]を用いて作成した指紋画像を示す．縦 336 画素，横 240 画素のビットマップ形式で構成されている．また，図 2 の指紋画像の 140 ライン目と 200 ライン目に相当する箇所の断面（濃淡）波形を，図 3 に示す．

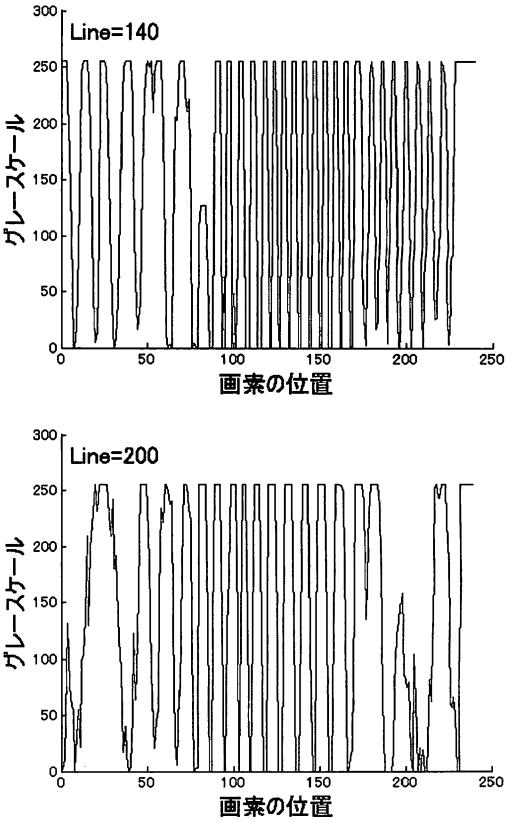

図 3　指紋の断面（濃淡）波形

図 3 において，指紋の断面（濃淡）波形は，縦軸に 0 から 255 の数値で表わされるグレースケールをとり，横軸に指紋画像の横軸方向 240 画素中の位置をとり，表わされている．図より，指紋画像の 140 ライン目の断面波形は 200 ライン目の断面波形に比べて変動が激しく，指紋の隆線と溝の間隔が狭くかつ各々の幅が狭くなっていることがわかる．

このように，指紋の断面波形は指紋画像のラインにより異なっているため，個人個人の指紋情報をサーバー内に登録しておくためには，指紋画像の全てのラインから断面波形の情報を得る必要がある．

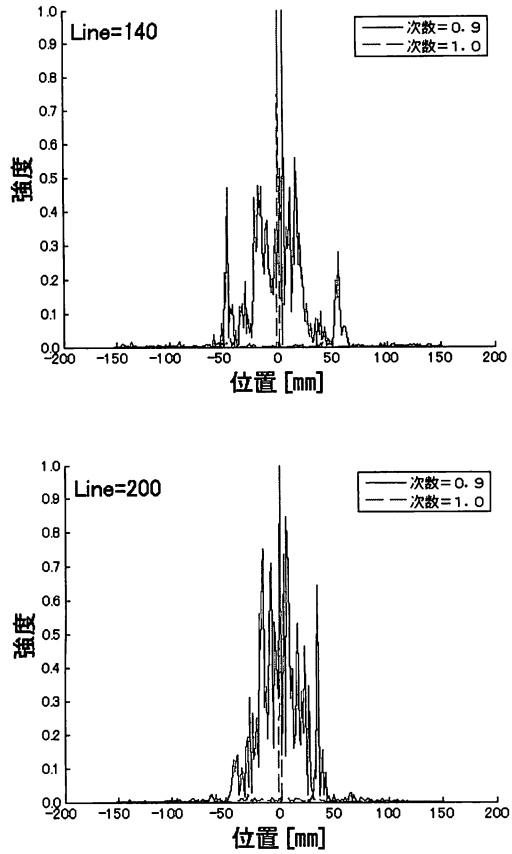

図 4　指紋の断面波形の
非整数次フーリエ場の強度分布

次に，図 3 で示した図 2 の指紋画像の 140 ライン目と 200 ライン目に相当する箇所の断面波形を，次数 1.0 と 0.9 で非整数次フーリエ変換した結果を，縦軸に強度，横軸に位置をとり図 4 に示す．これより，同じ断面波形を異なる次数で非整数次フーリエ変換して得られた結果は，お互いに異なることがわかる．また，断面波形が異なっても通常のフーリエ変換した結果には顕著な差異は見られないが，非整数次フーリエ変換した結果には顕著な差異が見られることがわかる．

以上の結果を踏まえて，本研究では指紋画像を一次元の有限矩形波とし，サーバーへの登録情報を生成するため様々な次数の非整数次フーリエ変換を行い，非整数次フーリエ場の諸特性を解析する．さらに，サーバーへの登録情報を復元できなくするため，登録情報として非整数次フーリエ場そのものではなくその強度分布を登録するようにし，逆非整数次フーリエ変換を行っても元の指紋画像が復元されないことを確認する．

3. 非整数次フーリエ変換とは

フーリエ変換を一般化した概念として 1980 年に，非整数次フーリエ変換（Fractional Fourier transform：以降 FRT）が導入された．一次元入力データ $u_0(x_0)$ の FRT は次式にて定義される[3]．

$$F^{(P)}[u_0(x_0)] = \int u_0(x_0)\exp[i\pi(x_P^2 + x_0^2)/(s^2\tan\phi)] \times \exp[-i2\pi x_p x_0/(s^2\sin\phi)]dx_0. \quad (1)$$

ここで，$\phi = p\pi/2$，p は FRT の次数，s はスケール因子を示す．

一次元入力データ $u_0(x_0)$ として，指紋画像の任意のラインにおける断面（濃淡）波形（図 5 (a)）と，それをモデリングした有限矩形波（図 5 (b)）を使用した．ここで，指紋の全幅：19 mm，指紋の凹凸の数：38×2 個，サンプリング数：2^16 点である．一例として，図 5 (b) を FRT した結果を図 6 に示す．

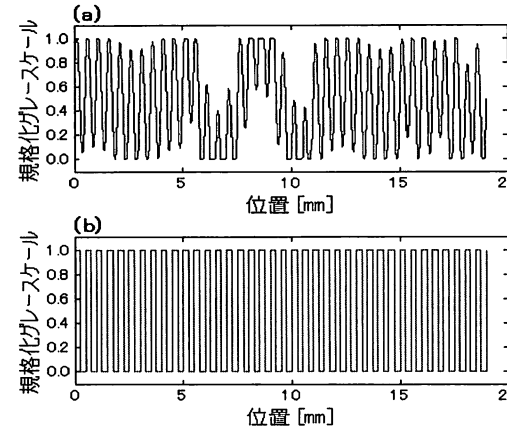

図 5 入力データ (a)指紋の断面波形，(b)有限矩形波

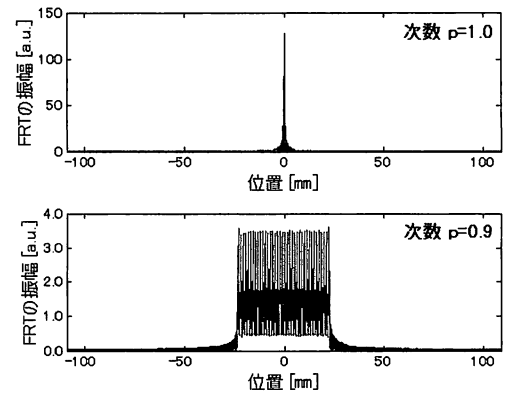

図 6　非整数次フーリエ場の振幅分布

図の上段は次数 p が 1.0 の，下段は次数 p が 0.9 のフーリエ場の振幅分布を示しており，特に前者は通常のフーリエ変換した結果に相当する．両図を比較することにより，フーリエ変換の次数 p の値が小さくなると，波形の Peak 値が著しく下がる一方，波形の幅が広がることがわかる．

4. 指紋画像の非整数次フーリエ場とその自己相関関数特性

FRT の次数 p を 1.0～0.1 まで 0.1 刻みで変化させ，それぞれの次数のフーリエ場の自己相関関数を求めた．縦軸に規格化した自己相関関数の振幅，横軸に位置をとり，一例として，次数 p が 1,0 および 0.9 の FRT の結果に対する自己相関関数の規格化振幅分布を図 7 に示す．両図を比較することにより，フーリエ変換の次数 p の値が小さくなると自己相関関数の幅が広がることがわかる．

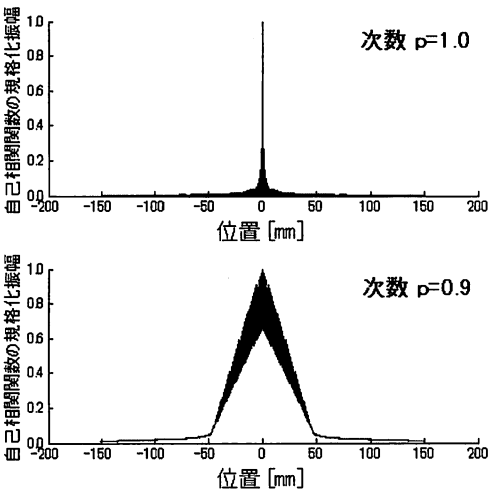

図 7　非整数次フーリエ場の自己相関関数

そこで，得られたそれぞれの次数の自己相関関数の規格化振幅分布の包絡線の半値全幅に着目し，縦軸にその半値全幅，横軸に FRT の次数 p を取り，解析した結果を図 8 に示す．なお図中で，「指紋画像」は入力データとして図 5 (a)を，「矩形波」は図 5 (b)を用いた場合の結果を示す．

これより，自己相関関数の包絡線の半値全幅の次数 p 依存性は入力データがいずれの場合であっても同じ傾向を示しており，次数 p が減少するにしたがって半値全幅が累積的に広がっていくことがわかる．

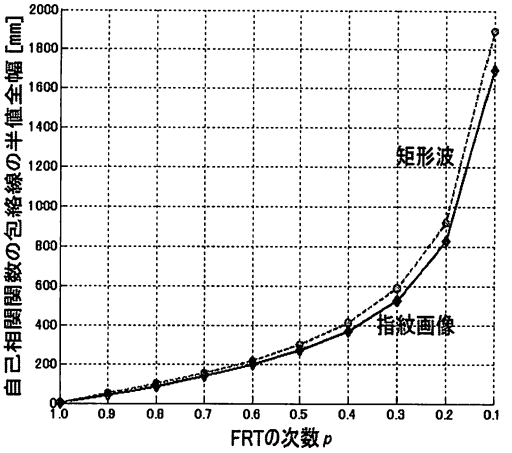

図 8　自己相関関数の包絡線の半値全幅の特性

5. 異なる次数の非整数次フーリエ場の相互相関関数特性

次に，FRT の次数 p が 1.0 の場合のフーリエ場と，次数 p が異なる場合のフーリエ場(具体的には p が 0.99, 0.95, 0.9, 0.8, 0.7, 0.5 の場合）の相互相関関数を求めた．縦軸に相互相関関数の振幅，横軸に位置をとり，一例として，入力データを有限矩形波（図 5 (b)）とした場合の次数 1.0 と 0.9 の相互相関関数，および次数 1.0 と 0.5 の相互相関関数の結果を図 9 に示す．これより，FRT の次数の差が大きくなると相互相関関数の Peak 値が下がる一方，相互相関関数の幅が広がることがわかる．

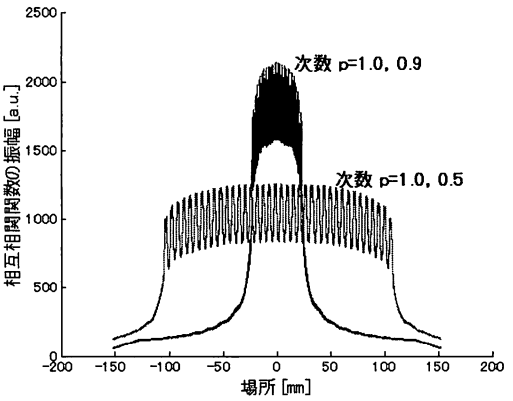

図 9　非整数次フーリエ場の
相互相関関数の振幅分布

そこで，得られた相互相関関数の Peak 値に着目し，

縦軸に相互相関関数の Peak 値，横軸に FRT 1.0 次との次数差 Δp をとり，解析した結果を図 10 に示す．

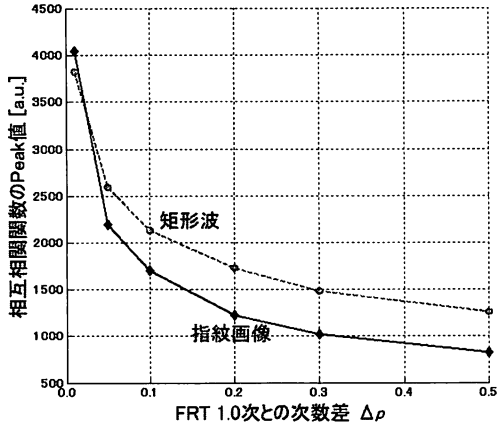

図 10　相互相関関数の Peak 値の特性

これより，相互相関関数の Peak 値の次数差 Δp 依存性は入力データがいずれの場合であっても同じ傾向を示しており，次数差 Δp が大きくなるに従って，Peak 値が急激に下がっていくことがわかる．

以上，４節および５節では，指紋画像の非整数次フーリエ場の特性を解析することにより，指紋画像の非整数次フーリエ場は次数が異なると顕著に異なることがわかった．これにより，指紋画像の各々のラインに対してフーリエ変換の次数を暗号化して非整数次フーリエ場をサーバーに登録することにより，他者が元の指紋画像に復元することが著しく困難にできることが明らかになった．

次節では，指紋画像の復号化を全く行えないサーバーへの登録手法を提案する．

6. 指紋画像と逆非整数次フーリエ場の相互相関関数特性

入力データとして有限矩形波（図 5 (b)）の全幅のみを 3 倍にしたものを図 11 に示す．ここで，指紋の全幅：57 ㎜，指紋の凹凸の数：38×2 個，サンプリング数：2^16 点である．このデータを入力データとすることにより，逆 FRT を行った際の結果が正しく得られるようにした．

まず，図 11 に示された有限矩形波を入力データとし，次数 p が 1.0，0.99，0.95，0.9，0.8，0.7，0.5 で FRT を行い，その強度分布（絶対値の二乗）を導出する．これにより，非整数次フーリエ場から位相情報がなくなるため，サーバー登録時のデータ量が半減する．また，この強度分布に対して逆 FRT を行っても，元の矩形波に戻らないことが予想できる．

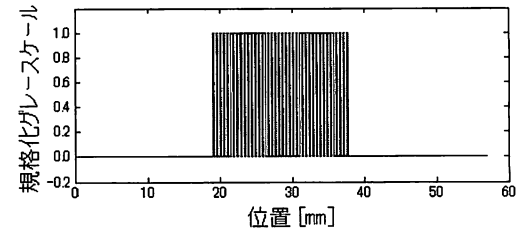

図 11　全体幅を広げた入力データ（有限矩形波）

一例として，縦軸に FRT の強度，横軸に位置をとり図 12 に示す．

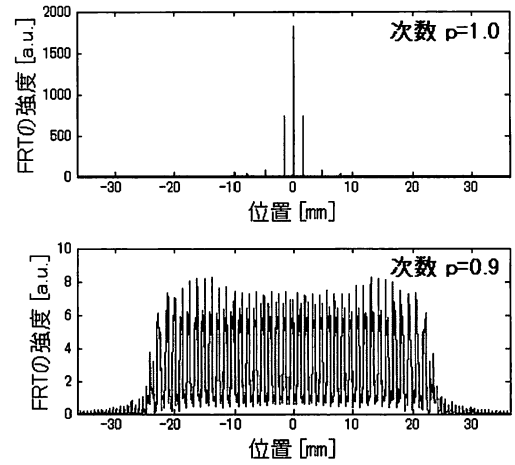

図 12　非整数次フーリエ場の強度分布

図の上段は次数 p が 1.0 の，下段は次数 p が 0.9 のフーリエ場の強度分布を示している．これより，図 6 に示した非整数次フーリエ場の振幅分布の結果と同様に，フーリエ変換の次数 p の値が小さくなると，波形の Peak 値が著しく下がる一方，波形の幅が広がることがわかる．

次に，図 12 に示された，それぞれの波形に対して逆 FRT を行うことにより得られた結果の規格化振幅分布の例を図 13 に示す．

図 13 では，縦軸に規格化振幅，横軸に位置をとり，上段に次数 p が 1.0 の，下段に次数 p が 0.9 の場合の規格化振幅分布が示されている．これより，図 11 の矩形波入力データと比較しても明らかなように，非整数次フーリエ場の強度分布に対して逆 FRT を行っても元の指紋画像と明らかに異なり，指紋画像を復元できないことがわかる．

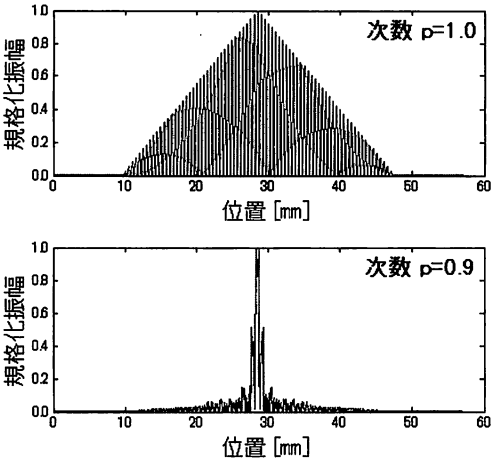

図 13　非整数次フーリエ場の強度分布に対する逆 FRT の振幅分布

次に，図 13 で示した結果と図 11 で示した元の指紋画像（有限矩形波）との差異を定量的に解析するために，両者の相互相関関数を求めた．特に，相互相関関数の振幅分布の包絡線の半値全幅を求めるため，最大振幅値で規格化した結果を図 14 に示す．

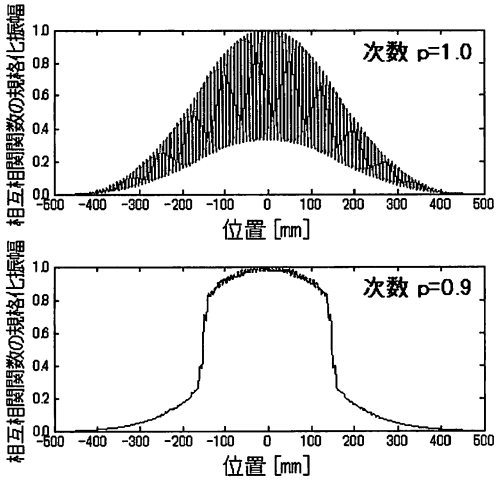

図 14　有限矩形波と逆 FRT の振幅分布の相互相関関数

図 14 では，縦軸に相互相関関数の規格化振幅，横軸に位置をとり，上段に次数 p が 1.0 の，下段に次数 p が 0.9 の場合の結果が示されている．これより，次数 p が 1.0 の結果より 0.9 の結果の方が相互相関関数の包絡線の半値全幅が狭くなることがわかる．

そこで，それぞれの次数に対する相互相関関数を求めた結果より，相互相関関数の規格化振幅分布の包絡線の半値全幅を求めた．縦軸に規格化した相互相関関数の包絡線の半値全幅を，横軸に FRT の次数を取り，解析した結果を図 15 に示す．

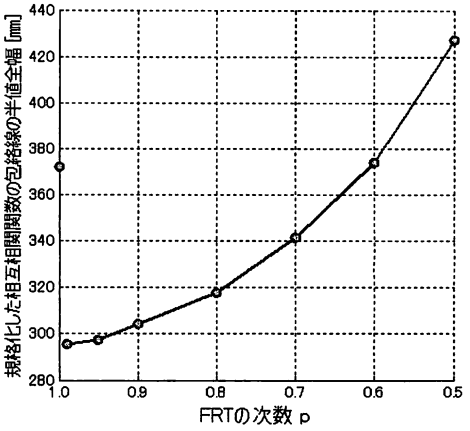

図 15　規格化した相互相関関数の包絡線の半値全幅の特性

図より，非整数次フーリエ変換の次数 p の値が 1.0 の場合を除き，次数 p の値が小さくなるにしたがって半値全幅が広がっていくことがわかる．しかし，次数 p が 1.0 と 0.6 の場合の半値全幅の値は同等であることがわかる．

7. まとめと今後の課題

本研究では，FRT を用いた指紋画像暗号化の可能性を検討するため，指紋画像の非整数次フーリエ場の諸特性を解析した．その結果，非整数次フーリエ場はその次数が異なると顕著に異なることが明らかとなった．これにより，指紋画像のラインごとにフーリエ変換の次数を任意に変更することにより，他者から解読されにくいが元の指紋画像に復元できる暗号化が容易にできることが示された．また，サーバー登録時のデータ量を半減し，かつ復号化が行えない指紋画像登録情報を作成するための方式についても検討した．

今後は，指紋画像の暗号化においてランダムノイズを重畳させることを考え，FRT を利用した画像の暗号化手法についてさらに検討を進めていく．

文　献

[1] 吉嶺達樹　“バイオメトリクス認証の動向と周波数解析法，” Interface, pp.62-68 (2005.3).

[2] DVD of the SFINGE Software Tool, D. Maltoni *el al.*, “Handbook of Fingerprint Recognition,” Springer-Verlag, 2003.

[3] F. J. Marinho and L. M. Bernardo, “Numerical calculation of fractional Fourier transforms with a single fast-Fourier- transform algorithm,” J. Opt. Soc. Am. A, Vol.15, No.8, pp.2111-2116 (1998).