2005－CSEC－31（9）
2005／12／9

Fuzzy Biometric Vault Scheme を用いたテンプレートの安全性対策

大木哲史[†]　赤塚志郎[†]
小松尚久[†]　笠原正雄[††]

近年，バイオメトリック個人認証において注目が集まりつつあるが，登録されたテンプレートが適切に保護されていない場合テンプレートの漏洩により，生体情報の復元やなりすましが行なえる危険性がある．本稿では利用するテンプレートの安全性を高めるための一手法として Fuzzy Vault Scheme を用いた手法を提案する．また，本提案手法に関しては指紋を対象例としてシミュレーションを交え評価する．

Safety of Templates Using Fuzzy Biometric Vault Scheme

Tetsushi Ohki,[†] Shiro Akatsuka,[†] Naohisa Komatsu[†]
and Masao Kasahara[††]

Recently, biometric person authentication has become a spotlight. However, in conventional biometric person authentication systems, each individual's template is stored as it is in the system. Hence, when a registered template is not properly protected, the risk of impersonation using biometric information restored due to template leakage by a third party arises. In this paper we propose a method to improve safety of template using Fuzzy Vault Scheme. In this paper the safety of templates is evaluated by simulation of a fingerprint verification system.

1. まえがき

ユビキタスネットワーク環境に関する議論に伴い，個人認証の必要性に対する関心が高まっている[1)]．個人認証は，1）暗証番号やパスワードなどの本人知識によるもの，2）鍵や IC カードなどの本人の所有によるもの，3）指紋，顔，筆跡，音声などの本人固有の特徴によるバイオメトリック認証，の3つに分類できる[2)]．これらの手段はそれぞれが長所・短所を持ち，どの手段が最も優れているということは言えないため，適用するシステムのリスクや利便性を考慮した上で適用する認証手段を選択する必要がある．

バイオメトリック認証はシステム構築の面からも，また記憶，所持の煩わしさから解放されるなどの利便性の面からも特長があり，入退室管理，ネットワークアクセス等のアクセスコントロール，ネットワークバンキング等のフローコントロール，またサーベランスシステム等トラッキングへの展開が期待されているが，利用者，環境条件，運用条件，生体情報，バイオメトリクス装置といったさまざまな要素において脆弱性が存在しており，それぞれの脆弱性への対策が今後の展開への重要な課題となっている[3)]．

そこで本稿では，こうした脆弱性のなかでもバイオメトリクス装置に関連するデータ漏洩に着目し，個人テンプレートを暗号化して保管し，個人テンプレートと提示したバイオメトリック情報から秘密情報を生成する方式である Fuzzy Vault Scheme を用い，秘密情報と秘密情報の取得に用いる個人テンプレートをシステムに保管された情報からは復元できない対策を施すとともに，本人のバイオメトリック情報を用いて秘密情報を生成可能とする手法を提案する．

本手法は従来提案されてきた手法と違い，秘密情報は登録したテンプレートと提示したバイオメトリック情報から生成される．このためテンプレートの安全性だけでなく秘密情報の秘匿性にも優れている点を特徴としている．また，テンプレートの形式を問わないため，指紋だけでなく様々なモダリティへの応用が可能である．本稿では，まず Fuzzy Vault Scheme のバイオメトリック認証への応用例として，テンプレート情報と検査符号をペアとする手法について説明する．次

† 早稲田大学理工学部
Science and Engineering, Waseda University
†† 大阪学院大学情報学部
Facluty of Informatics, Osaka Gakuin University

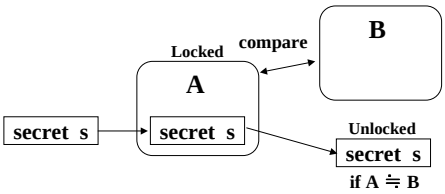

図 1 Fuzzy Vault Scheme の概要

いで提案手法の指紋照合への適用を提案する．さらに指紋照合方式に関しては秘密情報の復元可能性とテンプレート安全性についてシミュレーションを交え考察する．

2. Fuzzy Vault Scheme[4)]

Fuzzy Vault Scheme とは Juels らによって提案された，任意の情報の組を用いてある情報を秘匿する暗号方式の一種である．ここでは Fuzzy Vault Scheme の概要について説明する．隠したい情報 S を任意の情報の組 A を用いてロックする．そして，A と同じ形式の情報の組 B を与え，A と B の大部分が一致すれば S を得ることができる．これがアンロックとなる．Fuzzy Vault Scheme の概要を図 1 に示す．

まず，秘密情報 S と情報の組 A を用意し，S の値を元に，例えば S の値が各次数に対する係数となるような多項式 $P(X)$ を生成する．次に，A の要素 a_i を多項式 $P(X)$ に代入した結果 $P(a_i)$ を求め，a_i とペアにしてロック情報 R とする．また，R に含まれる A の要素の特定を困難とするためにダミーデータを作成してロック情報 R へ加えた後，順番をシャッフルして最終的に保管するロック情報 R とする．

ロックされた情報 S をアンロックするにはロック時に用いた情報の組 A と同様の形式を持つ情報の組 B を用いる．この情報の組 B が R 中に含まれる A の要素とある程度一致すれば S が復元できる．また，復元には誤り訂正符号が用いられるため，情報の組 A と B は完全に一致しなくても S が復元できる．Fuzzy Vault Scheme は以下のような特徴を持つ

- A や B の値は任意に選ぶことが可能
- A や B の並び順を考慮する必要はない
- アンロック時は完全一致ではなく大部分が一致すればよい (fuzziness)
- 隠したい情報 S はシステムに保管しなくてよいため，セキュリティの面で有利である．

また，Fuzzy Vault Scheme は,「多項式復元問題」「ダミーデータの付加」の 2 点によってセキュリティを保っている．多項式復元問題とは，システムに実際に保存されている情報は，$(a_i, p(a_i))$ なる情報の組およびダミーデータのみであり，ここから多項式 $P(X)$ を復元することは困難であるというものである．また，ダミーデータを加えることにより，a_i の予測を困難とし，さらに総当り攻撃に対する耐性をより強く保つことができる．

3. Fuzzy Vault Scheme を用いたテンプレート安全性対策

Fuzzy Vault Scheme のバイオメトリック認証への適用を考える．秘匿したい情報（以下，秘密情報 S）をロックおよび，アンロックする情報としてバイオメトリック情報を用いる．図 2 に示すように，提案手法ではロック時に提示される情報をロック用バイオメトリック情報 A とし，S の要素を係数とする多項式を生成し，生成した多項式（以下，多項式 $P(X)$）を誤り訂正符号器に入力して符号語を得る．得られた符号語（以下，符号語 F）のうち，検査符号部（以下，検査符号 C）の各要素とその要素番号（以下，要素番号 L），バイオメトリック情報 A の各要素をペアとしてシステム内の保管情報（以下，ロック情報 R）へ追加する．さらにダミーとして偽のバイオメトリック情報と検査符号のペアを A および C と重複しない範囲で作成し，作成されたダミーの情報（以下，ダミーデータ D）を R に追加する，最後に R の要素の並びをシャッフルし，これをシステムに登録する情報とする．

アンロック時には登録時と同様にバイオメトリック情報を提示し，これをアンロック用バイオメトリック情報 B とする．R に含まれる全てのペアと B の間でマッチング処理を行い，一致したペアを選択する．一致した全てのペア（以下，一致情報 Q）から検査符号部を抽出し，誤り訂正用の多項式を生成する．生成された多項式（以下，検査多項式 $Q(X)$）を誤り訂正復号器へ入力することにより多項式 $P(X)$ が復号され，またその係数から秘密情報 S_d が生成される．ここで，ロック用情報とアンロック用情報の類似性が高ければ $S = S_d$ となり，そうでなければ $S \neq S_d$ となる．

3.1 ロック処理

$GF(2^m)$ 上の k 個の情報からなる秘密情報 S，n 個の要素からなるロック用バイオメトリック情報 A を考える

$$S = \{S_1, S_2, \ldots, S_{k-1}, S_k\}$$
$$A = \{a_1, a_2, a_3, \ldots, a_{n-1}, a_n\}$$

ここで S の各要素を係数とする多項式 $P(X)$

$$P(X) = S_1 + S_2 X + \ldots + S_k X^{k-1}$$

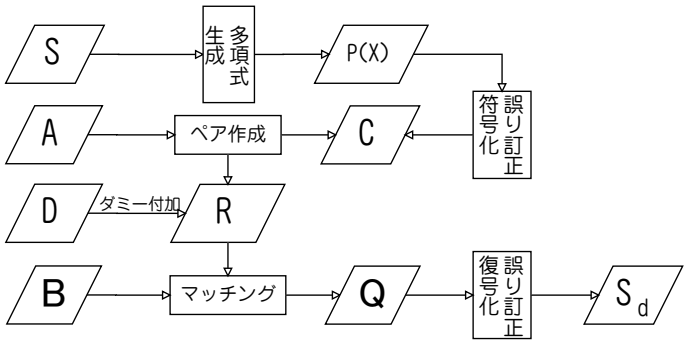

図 2 Fuzzy Vault Scheme を用いたテンプレート安全性対策

を生成する．この $P(X)$ を情報記号とみなして，これを最大距離分離符号である Reed-Solomon 符号（以下，RS 符号）に符号化する．誤り訂正符号は情報符号と検査符号から成るが，このうち検査符号 C を

$$C = C_1, C_2, C_3, \ldots, C_{g-1}, C_g$$

とする．また，C を多項式表現したものを

$$C(X) = C_1 + C_2X + \ldots + C_gX^{g-1}$$

とし，以後 $F \rightarrow F(X)$ といった表記はその情報を $C(X)$ と同様に多項式表現したものとして扱う．RS 符号により $P(X)$ を符号化した符号語 F は，

$$F = (c_1, c_2, \ldots, c_g, S_1, S_2, \ldots, S_k)$$

$$F(X) = X^gP(X) + C(X)$$

となる．ここで，得られた情報のうち情報記号は秘密情報 S を復元される危険性があるので用いないこととし，検査符号 C とロック用情報 A との間でペアを生成する．情報符号は全て消失誤りとみなし，アンロック時にマッチングにより得られる検査符号のみから情報符号を復元する．

また，誤り訂正復号を行うためにはアンロック時に検査符号の要素が正しい並び順で復元されなければならない．このためロック時に A, C の要素に加え，ペアとして保管される検査符号の要素番号（＝対応する次数+1）を示す要素番号 L ($\{L_1, L_2, \ldots, L_i, \ldots, L_g\}$) を保管する．たとえば，ペアとして保管される検査符号が C_5 であれば対応する要素番号 L_i は 5 となる．

ロック用情報 A の i 番目の要素と検査符号 C の i 番目の要素および C_i の要素番号 L_i とのペアを

$$r_i = (a_i, C_i, L_i)$$

のように表記し，ロック情報 R を

$$R = \{r_1, r_2, r_3, \ldots, r_{g-1}, r_g\}$$

とする．検査符号と A の要素を一対一に対応させるため，A の要素数 n はあらかじめ $n = g$ と設定し，検査符号との要素数と同数にしておくこととする．したがって，ロック用バイオメトリック情報を取得する際，正規化等の処理により g 個の情報が確実に得られるようにしておくことが必要である．

3.1.1 ダミーデータの作成

R をそのままシステムに保管した場合 R に含まれる A の予測が容易に可能となるため，ダミーデータを付加して安全性を高める必要がある．ダミーデータは，それ自身がダミーであることが容易に推測できてしまう場合安全性の面から大きな問題となるため，A と同様のデータ形式で作成する．A から作成したペアとダミーデータを合わせて t 個の要素をシステムに保管するとすれば，ダミーデータ D は

$$d_j = (\alpha_j, \beta_j, \gamma_j)$$

$$D = \{d_1, d_2, \ldots, d_j, \ldots, d_{t-g-1}, d_{t-g}\}$$

となる．ダミーデータの量を増やせばマッチングの過程でダミーデータとの誤一致が発生する可能性が高くなる．この際誤一致したダミーデータのペアから正しい検査符号が取得できてはならないため，ダミーデータには検査符号の値が含まれないように注意する必要がある．したがって，ダミーデータ作成時には，次の条件を満たすようなダミーデータを作成する．

$$\alpha_j \notin A,\ \beta_j \notin C$$

$$1 \leq \gamma_j \leq g$$

また，ダミーデータの要素番号に当たる γ_j は，$g+1$ など要素番号の範囲外をとった場合ダミーデータであると容易に判別できるため，要素番号の範囲内（1∼g）を設定しなければならない．

作成したダミーデータをロック情報 R に加える．

$$R = R \cup D$$

$$R = \{r_1, r_2, r_3, \ldots, r_{t-1}, r_t\}$$

$$R = \left\{ \begin{array}{l} r_1, r_2, \ldots, r_{g-1}, r_g \\ d_1, d_2, \ldots, d_{t-g-1}, d_{t-g} \end{array} \right\}$$

また，R をこのまま保管した場合要素の並び順からバイオメトリック情報 A が露見する可能性がある．こ

のため R の要素をランダムにシャッフルした後，最終的な登録データとしてシステムに保管する．

3.2 アンロック処理

アンロック時にはロック時と同様に $n(=g)$ 個の値から成るバイオメトリック情報 B

$$B = \{b_1, b_2, b_3, \ldots, b_{n-1}, b_n\}$$

を提示し，得られた B とロック情報 R との間でマッチング処理を行う．ここで，R の各要素はダミーであるかどうかがわからないため，(x, y, z) なる形式のペアで表現する．したがって R の i 番目の要素 $r_i = (x_i, y_i, z_i)$ となる．B の i 番目の要素 b_i と R の j 番目のペア R_j を比較する場合，

$$if(b_i \ = \ x_j)$$
$$r_j = (a_j, y_j, z_j) \ \ if \ b_i \in A$$
$$Q \leftarrow Q \cup (b_i, y_j)$$

ただし，

$$y_j = C_j, \ z_j = L_j \ \ if \ b_i \in A$$
$$y_j = \beta_j, \ z_j = \gamma_j \ \ if \ b_i \notin A$$

である．マッチングにより T 個のペアが得られたとすると一致情報 Q は

$$Q = \{Q_1, Q_2, \ldots, Q_T\}$$

であり，得られた T 個のペアの検査符号部を誤り訂正復号器へ入力することにより $P(X)$ が復元され，S_d もまた $P(X)$ の係数から生成される．ここで，検査符号 $C_1, C_2, \ldots, C_g$ の最小距離 $\overline{d}$ は

$$\overline{d} = g + 1 \tag{1}$$

で与えられる．ここで，Q に含まれる T 個の要素のうち m 個が $P(X)$ から作成された検査符号であったとすれば，誤り訂正符号により $P(X)$ の係数を正しく復元するためには $k + 2(g - m) + 1 \leq \overline{d}$ なる関係が成り立たなければならない．これを 1 式を用い，m に関する式へ変形すると

$$\frac{k+g}{2} \leq m \tag{2}$$

となり，$P(X)$ の係数を正しく復元し，$S_d = S$ となるためには，$(k+g)/2$ 以上の検査符号がマッチングにより与えられる必要があるということがわかる．一般に提案手法では 2 式を満たすことが必要であるが，個人認証の安全性を高めるためには，g は k に対し適当に大きな値に設定されねばならない．

4. 指紋照合への適用

3 で述べた手法はロック，アンロック用の情報に一般的なバイオメトリック情報を想定した手法であり，適当なパラメータ設定を検討することにより，どのモダリティにも適用可能である．ここでは適用の一例として，指紋照合への適用を提案する．

4.1 特徴点座標を用いない指紋照合方式

本稿では，指紋の特徴としてマニューシャ方式を用いる．マニューシャ方式において，保管すべきパラメータとしては，マニューシャの座標点，端点や分岐点の属性，マニューシャの座標での隆線ベクトルの方向，マニューシャ間の交差隆線数（リレーション），といったものが主に考えられる．これらは 3 章におけるロック用バイオメトリック情報 A の各要素 $a_1 \sim a_n$ として用いることができるが，システムに保管されるデータにマニューシャの座標点が含まれていると，データの漏洩が起こった場合第三者に指紋情報を推測される可能性がある．そこで，本稿では保管対象のマニューシャの位置情報を座標点としては保管せず，指紋の中心点を基準として指紋画像を複数のエリアに分割した後各エリアにインデックスをつけ，分割したエリア内のどこにマニューシャが所属するかの情報のみを保管することとする．これに加え，保管対象のマニューシャが端点・分岐点のどちらであるか，またマニューシャの座標点での隆線方向を併せて保管する．A の i 番目のマニューシャ a_i の端点・分岐点を示す属性を属性値 p_i とし，所属するエリアの番号をエリア番号 W_i，座標点での隆線方向を隆線方向 θ_i とすれば，a_i を構成するデータは以下のように表現できる．

$$A = a_1, a_2, \ldots, a_i, \ldots, a_{n-1}, a_n$$
$$a_i = (p_i, W_i, \theta_i)$$

4.2 検査符号の生成

保管される情報は 1 式で示したとおり C の要素と C_i と C_i 要素番号 L_i，指紋情報 a_i の 3 つの要素からなるペアである．したがって，ロック情報 R に追加されるデータは次式で表される．

$$R = (r_1, r_2, \ldots, r_i, \ldots, r_t)$$
$$\text{ただし}, r_i = (a_i, C_i, L_i)$$

4.3 ダミーデータの生成

3.1.1 で述べたように，ダミーデータの形式は A と同様でなければならない．ダミーデータとロック情報の要素数が合わせて t 個であるとし，ダミーデータを

$$D = (D_1, D_2, \ldots, D_i, \ldots, D_{t-g})$$

ただし，

$$D_i = (\alpha_i, \beta_i, \gamma_i)$$
$$\alpha_i \notin A$$
$$\beta_i \notin C$$
$$1 \leq \gamma_i \leq g$$

のような条件で作成し，ロック情報 R へ追加する．

4.4 アンロック過程

アンロック用指紋情報 B の要素と R との間でマッチングを行う．B の要素 B_i と R の要素 R_j とのマッチングは，属性値 p，エリア番号 W が一致するかどうか，また隆線方向 θ が設定した値（以下，閾値 th）より小さいかどうかを判定することによって行われる．マッチしたと判定したものは一致情報 Q へ追加される．3.2 と同様に Q の i 番目の要素 q_i を (x_i, y_i, z_i) なるペアで表現し，また B の要素を $(\overline{p}, \overline{W}, \overline{\theta})$ なる形式で表すとすれば，マッチング処理は次のような式で示される．

$$
\begin{aligned}
&foreach\ b_i \\
&\ for\ j = 1 \sim t \\
&\ b_i = (\overline{p}_i, \overline{W}_i, \overline{\theta}_i),\ r_j = (x_j, y_j, z_j) \\
&\ if \quad \overline{p_i} = x_j\ and \\
&\qquad \overline{W_i} = y_j\ and \\
&\qquad |\overline{\theta_i} - z_j| < th \\
&\qquad Q \leftarrow Q \cup r_i \\
&\text{ただし，} \\
&\qquad r_i \notin D \qquad if\ b_i \in A \\
&\qquad r_i \in D \qquad if\ b_i \notin A
\end{aligned} \tag{3}
$$

4.5 誤り訂正符号による秘密情報の復元

得られたマッチ情報 Q の全てのペアから検査符号部と要素番号を用いて，検査多項式 $Q(X)$ を生成する．アンロック過程においてダミーデータも含め T 個のペアが一致と判定されたとする．R と同様 Q の要素 q_i はダミーであるかどうかを判断できないため，$q_i = (\overline{x}_i, \overline{y}_i, \overline{z}_i)$ なる形式で示すとすれば，検査多項式 $Q(X)$ は

$$
\begin{aligned}
&Q = (q_1, q_2, \ldots, q_i, \ldots, q_T) \\
&Q(X) = \overline{y}_1 X^{\overline{z}_1} + \overline{y}_2 X^{\overline{z}_2} + \ldots, \overline{y}_T X^{\overline{z}_T} \\
&\text{ただし，} \\
&q_i \ = \ (\overline{x}_i, \overline{y}_i, \overline{z}_i) \\
&\quad = \ \notin D \qquad if\ x_i \in A \\
&\qquad \in D \qquad if\ x_i \notin A
\end{aligned}
$$

となる．生成した $Q(X)$ を誤り訂正復号器へ入力し，多項式 $P(X)$ を復元し，その係数から秘密情報 S_d を生成する．ここで，$Q(X)$ に含まれる T 個の要素のうち $P(X)$ から作成された検査符号の個数（以下，一致数 m）が 2 式で示した $(k+g)/2$ 個以上であれば復号によりロック時に作成した $P(X)$ が正しく復元され，$S_d = S$ となり S もまた正しく復元される．しかし，m が $(k+g)/2$ 個未満であった場合 $S_d \neq S$ となり S は誤った値が出力される．

5. 提案手法の評価

Fuzzy Vault Scheme の指紋照合への適用実験を行なった．指紋照合方式においては各人のマニューシャの数は一定ではなく，また，本人であっても登録時と照合時でマニューシャ数は変化する．このため，登録時に複数の指紋を用い，信頼性の高い n 個のマニューシャを用いることとする．また，検査符号とペアにして保管することを前提とするため，$n = g$ となる．検査符号とロック用指紋情報がペアとして保管されることを考慮すれば，秘密情報の復号に必要な一致数は，秘密情報の要素数 k とロック用指紋情報の要素数 g によって決まる．指紋情報が一定の数以上得られないと仮定すると，秘密情報の要素数 k を減らすことにより，少ない一致数で復号が可能となるが，同時に第三者によるアンロックの危険性も増大することとなる．秘密情報の要素数を増やしていけば本人であってもアンロックできなくなる可能性があるが，第三者によるアンロックの危険性は減少する．この問題は k を一定の数と考え，取得するバイオメトリック情報の数を増減させた場合にも起こる．このようなトレードオフの関係を考慮しつつ，要求されるパフォーマンスに応じて，k, g といったパラメータを設定する必要がある．

横軸に多項式の次数 k を，縦軸にその次数で生成した多項式 $P(X)$ および $S_d = S$ となる確率（以下，復元率）を示したのが図 3 である．マニューシャ取得数 g は 10 個，15 個，20 個の 3 種類に関して調査を行った．その他のシミュレーション諸元を表 5.1 に示す．

図 3 から，多項式の次数を上げるほど本人の復元率が低くなっていることがわかる．$(k+g)/2 < m$ なる関係を考えれば秘密情報の要素数 k が少ないほど，秘密情報の復元に必要な一致数 m が小さくなり，本人の復元率が高くなるとともに，第三者の復元率もまた高くなると考えられる．また，今回の実験においては第三者の復元率は要素数 k が最も少ない場合でも約 0.3 %と低く抑えられている．

5.1 復元率の向上

図 3 の結果では他人の復元率を低く抑えることはできるが，本人の復元率を高く保つためには秘密の要素数 k を 0∼3 程度の小さな値としなければならず，より多くの情報を保管する場合に不都合が生じる可能性がある．ここでは，より多くの情報を保管するための対策の一例として，検査符号の一部をシステムに保管し，一致情報 Q と併せて照合を行う手法を提案する．

まず，ロック時に得られた g 個の要素からなる検査符号 $C = C_1, C_2, \ldots, C_g$ を 2 つに分割し，一方（以下，

シミュレーション諸元

指紋データ	35 名 ×5 枚 (登録 3 枚，照合 2 枚)
特徴点抽出アルゴリズム	NFIS2[5]
取得マニューシャ数	10,15,20 個
隆線方向の量子化レベル	32
回転誤差許容 th	1 レベルまで
走査エリアの大きさ	40×40 pixel

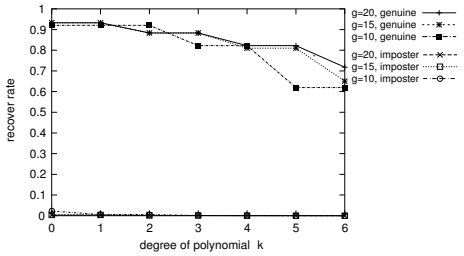

図 3　$P(X)$ の次数 k と秘密情報 S の復元率

分割検査符号 C_a）をシステムにそのまま保管し，もう一方（以下，分割検査符号 C_b）を A とペアにして保管する．またこの場合 A の要素数 n は分割検査符号 C_b と一対一でペアを作成するために，$n = g - \overline{g}$ 個に正規化すべきである．C_a の要素数を $\overline{g}$ 個とすると，

$$\begin{aligned} A &= \{a_1, a_2, \ldots, a_{(g-\overline{g}-1)}, a_{(g-\overline{g})}\} \\ C_a &= \{C_1, C_2, \ldots, C_{\overline{g}}\} \\ C_b &= \{C_{\overline{g}+1}, C_{\overline{g}+2}, \ldots, C_g\} \\ R &= \{r_1, r_2, \ldots, r_{g-\overline{g}}\} \end{aligned} \tag{4}$$

となる．次に 4 章の手順に従い R にダミーデータを加えシャッフルを行う．作成された R に加え C_a をシステムへ保管する．ここで，分割検査符号 C_a が漏洩したとしても C_a の要素数が $(k+g)/2$ 以下であれば C_a のみから S の復元は困難である．アンロック時には 3 式で示すマッチング処理により一致情報 Q が作成され，次いで 4 式により検査多項式 $Q(X)$ が生成される．ここで，得られた検査多項式にシステムから取得した分割検査符号 C_a を付加する．

$$\begin{aligned} Q(X) &= Q(X) + C_a(X) \\ &= \overline{y}_1 X^{\overline{z}_1} + \overline{y}_2 X^{\overline{z}_2} + \ldots, \overline{y}_m X^{\overline{z}_m} \\ &\quad + C_1 + C_2 X \ldots, C_{\overline{g}} X^{\overline{g}-1} \end{aligned}$$

C_a を付加した $Q(X)$ を誤り訂正復号器へ入力し，多項式 $P(X)$ および秘密情報 S を復元する．ここで一致数 m に関する式 $(k+g)/2 <$ はマッチングにより検査符号がいくつ得られれば秘密情報 S が復元できるかという式であると考えられる．したがって，g 個の検査符号のうち $\overline{g}$ 個の検査符号 C_a が必ず得られる場合，一致数 m に関する式は $(k+g)/2 - \overline{g} \leq m$ となる．図 4 は図 3 のマニューシャ取得数 n が 20 個の場合において，システムに保管する検査符号の数 $\overline{g}$ を

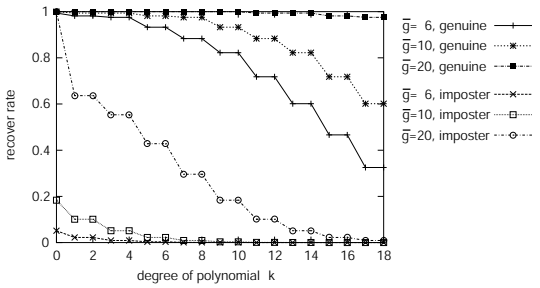

図 4　$\overline{g}$ の付加と S の復元率の関係

6，10，20 個と変化させていった時の復元率である．例えば $\overline{g} = 10$ であれば $g = 30, n = 20, \overline{g} = 10$ なる関係が成り立つ．図 4 と図 3 とを比較すれば，図 4 のほうがより大きい k を設定しても高い復元率での復元が行なわれていることが確認できる．このことから，次数 k を大きくしてより多くの情報を保管したい場合には有効な手法であることがわかる．

6. ま と め

本稿では，バイオメトリック個人認証のシステムの構築においてテンプレートの安全性を確保することが重要であるとの認識から Fuzzy Vault Scheme を用いてテンプレートの安全性を高める一手法を提案した．そして指紋照合方式への適用を行い，秘密情報の要素数 k と検査符号の要素数 g を適切に設定することにより本人であれば高い確率で秘密情報を復元可能であることを確認した．この手法は秘密情報を登録したテンプレートと提示したバイオメトリック情報から生成するため，テンプレートだけでなく秘密情報の秘匿性に優れた手法であると言える．このためバイオメトリクス PKI 等，秘密鍵の保管とユーザ認証を安全に行うことが必要とされる場面での認証方式として期待できる．

参 考 文 献

1) 瀬戸洋一．“ユビキタス時代のバイオメトリクスセキュリティ”．日本工業出版, 2003.
2) 小松尚久．“ユビキタスネットワーク環境におけるバイオメトリック個人認証”．システム/制御/情報,vol.49, Vol. 49,no.4, pp. 119–124, 2005.
3) 社団法人日本自動認識システム協会．“平成 15 年度基準認証研究開発事業, 生体情報による個人識別技術（バイオメトリクス）を利用した社会基盤構築に関する標準化”, 2004.
4) Juels A and Sudan M. “a fuzzy vault scheme”. *proc IEEE Int. Symp. Inf. Theory*, p. 408, 2002.
5) NIST Fingerprint Image Software 2, 2005. “http://fingerprint.nist.gov/NFIS/”.