Evaluation and Implement of Fuzzy Vault Scheme using Indexed Minutiae

Hiroaki Kikuchi, Yasunori Onuki and Kei Nagai

Abstract—Juels et. al proposed a fuzzy vault scheme that extracts secret from inexact biometric information. However, typical feature extracted from fingerprint, called minutiae, is assumed to tolerate against re-ordering minutiae. In order to address the issue, we propose a new scheme of fuzzy vault for fingerprint that assigns identification number to all minutiae and chaff (fake minutia) and determines correct order in greedy short distance algorithm. We evaluate the accuracy and the performance of the proposed scheme in comparison to some of existing schemes.

I. INTRODUCTION

Biometric information, e.g. facial image, iris and blood vessel, has been widely used for user authentication in many application contexts. The biometrics can not be replaced, or altered and hence it is highly reliable information than the conventional password or PIN. The template of biometric information stored in database, however, has a risk to be disclosed by malicious administrator for the server. Nowadays trusted party is hardly to be assumed in open and distributed network environment.

For protection biometric template, Juels and Sudan proposed an interesting cryptographical protocol, called fuzzy vault in [1], and fuzzy commitment in [2]. The idea is to add random noise to genuine one and somehow discard it by valid users who learns valid biometric information but not exactly same to the biometric feature in enrolment. The randomly generated noise, called chaff, prevents malicious or curious administrator from extracting private information stored in database.

An implementation of the fuzzy vault scheme is not so trivial because feature of biometric information is fragile and not stable in most cases. For example, characteristic information in fingerprint image, called minutiae, may be slightly moved, or be lost in extraction processes. Hence naive error handling technique such as the error-collecting code is not able to simply apply these.

Uludag et. al proposed a fuzzy vault scheme for fingerprint using line-based feature of biometric information in [3]. In the system, edge directions and minutiae directions, which may vary but not be lost, are used. To deal with recover the uncertainty, they use the LaGrange interpolation technique in which a polynomial is represented out of a limited number of points on the polynomial. They shows their scheme improves accuracy of some of existing system [4] based on experimental system.

The drawback of the Uludag’s approach, say secret-sharing approach, is its complexity in decoding. It necessary to test all possible combinations chosen t out of n candidates, where t is the order of polynomial and n is number of characteristics and spoils performance if n became large.

In this paper, we propose a new fuzzy vault scheme using indexed minutiae. The main idea is to assignment of identification to both of genuine and chaff minutiae so that re-ordering is made possible, which then allows efficient error-collecting code to be used to resolve the uncertainty of biometric information. We implement our proposed scheme and evaluate the accuracy and the performance in comparison to some of existing schemes.

II. PREVIOUS WORKS

A. Fuzzy Vault Scheme

Alice has a secret key in a vault $R$ using her biometric information $A$. She chooses polynomial $p(x)$ with her secret information as constant, e.g., $p(0)$, and computes the projections of the polynomial, $p(A)$, for the elements of $A$. Adding random elements, called chaff, that do not lie on $p$, fuzzy vault $R$ is defined by

$$ R = \{(a_i, p(a_i)) \mid a_i \in A\} \cup \{(r_j, s_j) \mid s_j \neq p(r_j)\}. $$

Bob, using a newly extracted biometric information $B$, can unlock the vault $R$ only if $B \cup A$ is large enough. He can locate many points in $R$ that lie on $p$. Using error-correction coding, e.g., Reed-Solomon code, it is assumed that he can reconstruct $p$. The security of fuzzy vault is based on the infeasibility of the polynomial reconstruction problem. According to analysis in [1], given vault $R$ of size $r$, there are possible

$$ \frac{\mu^q k - t}{3} \left( \frac{n}{7} \right)^t $$

combination for $\mu > 0$ to choose $t$ valid elements in $R$. For instance, to choose $t = 22$ elements out of a group of order $q = 10^4$, there are possible $2^{86}$ combinations, which is infeasible to compute.

III. PROPOSED SCHEME

A. Overview

We propose a new scheme of fuzzy vault with indexed minutia, for which rearrangement of minutia is performed and thus error collection with the Reed-Solomon code is made possible to the arranged minutia. The error-collecting
approach allows better performance for dealing with unstable behavior of minutiae than the secret-sharing approach made by Uldag[3] since no exhaustive search for possible combination of valid minutia is required in the error collecting steps.

In enrolment, a genuine fingerprint image is scanned and feature A, typically list of coordinate of minutiae, is extracted. All minutia are assigned an identification number, called index, and then mixed with random fake minutia, called chaff, to be a fuzzy fingerprint R for fingerprint. For a given index, there are several candidates of minutia which contains one valid minutia and few chaff, making it impossible to choose all valid minutiae out of chaff data except the correct user who has rescanned feature B and can guess almost all coordinate of valid minutia A in R.

B. Reed-Solomon(RS) code

Reed-Solomon is an error-correcting code, with \( \ell \)-bit blocks, defined over \( \text{GF}(2^\ell) \), which ensures \( t \)-bit error-collection, i.e., \( \ell \)-bit error collection. Given \( n \) blocks, including \( k \) information blocks and \( 2t \) redundant blocks, we have

\[ n = k + 2t. \]

C. LaGrange interpolation

LaGrange algorithm reconstruct \( v \)-order polynomial from arbitrary \( v + 1 \) points on the polynomial. Given \( f(x_1), \ldots, f(x_v), f(x) \) is computed by

\[ f(x) = \sum_j \lambda_j(x)f(x_j), \]

where

\[ \lambda_j(x) = \prod_{\alpha \neq j} \frac{x - \alpha}{j - \alpha}. \]

D. Indexed Fuzzy Vault Scheme

Our scheme consists of an enrolment step, or locking, and an authentication step, or unlocking.

E. Enrolment Step

Step 1.Let A be an extracted feature (minutiae) of the form \((a_1, a_2, \ldots, a_n)\), where \(a_i\) is a coordinate \((X_i,Y_i)\) for \(i\)-th minutia.

Step 2.Perform Reed-Solomon encoding with polynomial \(p(x)\) for A and obtain a codeword \((y_1, y_2, \ldots, y_n)\) that conceals secret information \(s\). Let \(R\) be a set of \(n\) valid minutiae of the form

\[(i, x_i, y_i)\]

where \(i\) is an index for \(i\)-th minutia and the corresponding piece of codeword \(y_i\).

Step 3.For \(i = n + 1, \ldots, r\), add random chaff such that \(x_i \not\in A\), \(r_i \not\equiv y_i \mod n\) as

\[ R \leftarrow R \cup \{(i \mod n, x_i, r_i)\}. \]

Note that \(r = |R|\) is the size of vault, which determines security parameter of the scheme. Given index \(i\), there are \(r/n\) elements in \(R\), including \(r/n - 1\) chaff. Also note that \(R\) may be randomly ordered so that valid minutia and chaff are indistinguishable.

F. Authentication Step

Valid user leans a newly extracted feature \(B = \{b_1, b_2, \ldots, b_n\}\) and thereby obtains \(Q\) as following steps.

Step 5.For \(i = 1, \ldots, n\), find \(j\) such that Euclid distance \(d(x_i, b_i)\) is the shortest distance for all \(x_i\) such as \(j \equiv i \pmod n\), where distance is defined with 2D coordinate \(X, Y\) as

\[ d(x_i, b_i) = \sqrt{(X_j - X_i)^2 + (Y_j - Y_i)^2}. \]

Add \(j\)-th element to \(Q\) as

\[ Q \leftarrow Q \cup \{(i, x_i, y_j)\}. \]

Since \(r \gg n\) holds, there always exists \(j\) for any \(i\).

Step 6.Perform re-ordering elements in \(Q\) for index and then decode codeword \(y_1, y_2, \ldots, y_n\) according to Reed-Solomon algorithm.

Step 7.Extract secret information \(s\) from the corrected codewords. For user authentication, using the shared secret \(s\) between valid user and a server, appropriate protocol can be applied, e.g., challenge-and-response.

IV. EXPERIMENTAL RESULT

A. Environment

Table I shows the experimental environment. We investigate accuracy for several fraction of chaff to be added to vault. A chaff ratio is defined by \(r/n\), where \(r\) is total number of element in \(R\) and \(n\) is the number of valid minutiae. For instance, chaff ratio \(r/n = 2\) and \(n = 22\) means that 22 chaffs are added to \(R\).

<table>
<thead>
<tr>
<th>item</th>
<th>specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>fingerprint scanner</td>
<td>Digital Persona U.are.U4000</td>
</tr>
<tr>
<td>software</td>
<td>Digital Persona Gold SDK 2.5.0</td>
</tr>
<tr>
<td>error correcting code</td>
<td>Reed-Solomon</td>
</tr>
<tr>
<td>feature extraction</td>
<td>NIST NFIS2 [5]</td>
</tr>
<tr>
<td>number of minutiae n</td>
<td>22</td>
</tr>
<tr>
<td>block size (\ell) [bit]</td>
<td>10</td>
</tr>
<tr>
<td>error collection [bit]</td>
<td>(\ell t)</td>
</tr>
</tbody>
</table>

B. Accuracy

We evaluate the accuracy of the proposed scheme with False Acceptance Ratio (FAR) and False Rejection Ratio (FRR) where 50 genuine fingerprints and random imposter fingerprints are used. In the proposed scheme, chance to cheat verifier as genuine user depends on chaff ratio, \(r/n\), and hence we estimate FAR using random guess of valid minutiae out of \(r/n\) candidates.
Error collection is one more factor to determine overall accuracy of the system. With $t$-blocks error collection ($\ell t$-bit error collection), less than $t$ miss choices out of $n$ elements can be recovered through error-collection step and thus a false rejection can be prevented. On the other hand, random guess is likely to be succeeded as $t$ increases. Therefore, we may clarify the optimal $t$ to resolve the tradeoff between FAR and FRR.

Figure 1 shows FAR and FRR with respects to $t$, error collection block size, where $r = 2n$. Figure 2 illustrates FAR and FRR in terms of chaff ratio, $r/n$, with fixed $t = 6$. Combining both results, we illustrate the relationship between FAR and FRR in Figure 3.

The best accuracy $FAR = 0$ and $FRR = 0.02$ achieves at chaff ratio $r/n = 2$ and $t = 6$ block error collection code. If adversary learns any partial information such as statistics, small number of valid minutiae, the FRR might be worse.

\begin{equation}
T(n) = a e^{\beta n} \leq \frac{n^t}{t!} \leq \frac{n^t}{t}
\end{equation}

for processing time in [3]. We illustrate the processing time in figure 5.

\begin{figure}[h]
\centering
\includegraphics[width=\columnwidth]{fig1}
\caption{Accuracy with respects to $t$-block error collecting code}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=\columnwidth]{fig2}
\caption{Accuracy with respects to chaff ratio $r/n$}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=\columnwidth]{fig3}
\caption{Correlation between FAR and FRR}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=\columnwidth]{fig4}
\caption{Processing Time with respects to $t$-block Error Collecting Code}
\end{figure}

V. CONCLUSION

We have proposed a new fuzzy vault scheme for fingerprint that introduces an indexed minutiae for re-ordering and applies greedy approach to chose the shortest distance to the new extracted feature. Experiments shows at the peak performance $FAR = 0, FRR = 0.02$ with processing time 530 [ms], which concludes that the error collection approach is advanced than secret sharing approach as high redundancy (error collection).

\textbf{Acknowledgement}

The authors gratefully acknowledge the contribution made by Mr. Yusuke Takahashi, who has graduated from Tokai University.
Fig. 5. Performance in [3] and the proposed scheme

Fig. 6. Minutiae Distribution

REFERENCES


