A Summer Internship Project Report

on

“Fingerprint Biometric cryptosystem combining Error correcting code and modified voronoi neighbour structure”

Carried out at

Institute for Development and Research in Banking Technology,

Hyderabad

Established by ‘Reserve Bank of India’

Submitted by

L. GREESHMA SAI

B.E. Computer Science and Engineering

OSMANIA UNIVERSITY

HYDERABAD

Under the Guidance of

Dr. MVNK PRASAD
Associate Professor
IDRBT, Hyderabad.

Fingerprint Biometric Cryptosystem combining Error Correcting Code and Modified Voronoi Neighbour Structure
CERTIFIACTE

This is to certify that L. Greeshma Sai, pursuing Computer Science and Engineering(C.S.E.) at Osmania University, Hyderabad has undertaken a project as an intern at IDRBT, Hyderabad from June 1st, 2015 to July 15th, 2015. She has done project work on “Fingerprint Biometric Cryptosystem combining Error Correcting Code and Modified Voronoi Neighbour Structure” under my guidance.
I wish her all the best for all her endeavours.

Dr. MVNK Prasad
Associate Professor
IDRBT
Hyderabad
ACKNOWLEDGEMENT

I wish to express my profound gratitude to my Guide Dr. MVNK Prasad for giving me the opportunity to do this project in the Institute for Development and Research in Banking Technology (IDRBT). Without his inspiration, guidance and supervision, it would not have been possible to complete this project. This opportunity of learning about Fingerprint Recognition in Biometric cryptosystems was a boon to me. I would like to add that this short period in IDRBT has added a different facet to my life as this is a unique organisation being a combination of academics, research, technology, communication services, crucial applications etc.,

I am extremely grateful to Dr. MVNK Prasad for his advice, innovative suggestions and supervision. I thank him for introducing me to this excellent area of Digital Watermarking for research. I am thankful to IDRBT for providing such an amazing platform for students, like me, to work. I thank one and all who made this project successful either directly or indirectly.

Last but not the least I would like to thank the trainees at IDRBT for nurturing my confidence.

L. GREESHMA SAI
(OSMANIA UNIVERSITY)
PROJECT TRAINEE
IDRBT, HYDERABAD.
ABSTRACT

Biometric cryptosystems is an emerging technology which combines both biometrics and cryptography. Bio-cryptosystem provides both security and privacy of biometric data. Biometrics is used to secure the system. Because of these features biometric system has received more concentration. Among all methods used fuzzy commitment scheme is a pioneer contribution to combine both biometrics and cryptography. Exact and automatic recognition and authentication of users are a essential difficulty in all systems. What is required is a system that could authenticate that the person is actually the person. Among all biometrics fingerprints have been used widely. But fingerprint uncertainty caused due to distortion during image capturing makes it difficult to achieve high recognition rate. In this paper this problem is avoided by using the local voronoi neighbour structure, we propose bio-cryptosystem based on fixed length bit-string which is extracted from 3D array using modified VNS. Using the fuzzy commitment scheme and binary feature vector as input, we construct bio-cryptosystem using error correcting code i.e., Reed Solomon Code. The proposed method is able to provide security and also good performance. Experimental results on database demonstrate that proposed method is effective.

KEYWORDS: Biometric cryptosystem, Voronoi neighbour structure, Fuzzy commitment scheme, error correcting code.
# TABLE OF CONTENTS

1. Introduction.................................................6  
   1.1 Cryptography...........................................6  
   1.2 Biometrics..............................................6  
   1.3 Biometric-Cryptosystems.........................6  
   1.4 Fingerprint ...........................................7  
   1.5 Fingerprint Recognition............................7  
   1.6 Problem................................................7  
   1.7 Organization of Paper.............................8  

2. Related Works..............................................9  

3. Proposed Method..........................................11  
   3.1 Generation of bit-string..........................11  
   3.2 Error Correcting Code............................13  
      3.2.1 Reed Solomon Encoding......................14  
      3.2.2 Reed Solomon Decoding......................15  
      3.2.3 Matching.......................................16  
   3.3 Performance Parameters..........................16  
   3.4 Calculation..........................................18  

4. Experimental Results and Analysis....................19  

5. Conclusion.................................................23  

References..................................................25
INTRODUCTION

1.1 CRYPTOGRAPHY

Cryptographic technology is widely used for ensuring secrecy [1] and information security such as authentication, data integrity and data confidentiality[2]. Traditional cryptographic techniques are based on Passwords and PIN’s. But there are many problems with these methods. For example passwords and PIN’s can be lost, guessed, forgotten or stolen[3]. Once stolen anyone can access the information.

1.2 BIOMETRICS

Use of biometrics has helped in handling these issues. Biometric recognition has replaced traditional cryptographic techniques of passwords and PIN’s. Biometric characteristics are classified into two types: physiological characteristics and behavioural characteristics. Physiological characteristics include fingerprint, face, iris, ear etc. Behavioural characteristics are related to behaviour of a person such as voice, signature etc. Biometric authentication is more reliable than password based authentication because biometric traits cannot be lost or forgotten. It is also difficult for attackers to forge or steal biometric trait. A number of biometric characteristics are being used in various applications as Universality, Uniqueness, Permanence, Measurability, Performance, Acceptability and Circumvention[4]. Though biometrics have many advantages still there are many disadvantages such as diverse and noisy nature of biometrics while capturing image[5], biometrics once lost cannot be reset or replaced.

1.3 BIOMETRIC CRYPTOSYSTEMS

For privacy and high security reasons a new emerging technology Biometric-Cryptosystem is proposed which overcomes the above problems. In biometric cryptosystems biometric traits are secured with a cryptographic key i.e., it uses both cryptography technology and
Among all biometric techniques fingerprint recognition [6-7] is the most popular biometric trait for recognizing a person.

1.4 FINGERPRINT

Fingerprints are the traces of an impression from the friction ridges of a human finger. Fingerprints generally contain impressions on last joint of fingers and thumbs. The most evident structural characteristic of a fingerprint is its pattern of valleys and ridges but they can often bifurcate. Figure 1.1 (a) shows the image of a fingerprint taken from a sensor device. Figure 1.1 (b) shows the different parts of a fingerprint.

![Figure 1.1](image)

1.5 FINGERPRINT RECOGNITION

A fingerprint is the feature pattern of one finger[8]. A fingerprint is the pattern of ridges and valleys. Each individual has unique fingerprints. Uniqueness is determined by local ridge characteristics called minutiae. A good quality fingerprint contains about 40-100 minutiae [9-10]. Fingerprint recognition is the process of comparing known and unknown fingerprints to check if the impressions are from the same fingerprint or not. It can be done by identification and verification. There are two types of approaches for fingerprint recognition: Minutiae based and Correlation based. Many researchers mostly make use of minutiae based approach for matching of fingerprints.

1.6 PROBLEM
Minutiae based method makes assumption that two fingerprints to be matched are of approximately same size. But this is not valid in all cases such as matching of partial fingerprints. Even two fingerprints captured using two different scanners may have different size. Sometimes because of cuts or scars or distortion while pressing causes same finger not to be identified. Figure 1.2 shows same fingerprint with different prints.

![Figure 1.2](a) (b) (c)

In this paper we propose fingerprint recognition method based on modified Voronoi Neighbour Structures (VNSs) using error correcting code to reduce fingerprint uncertainty. In the proposed method we first form VNS and then modified VNS. Modified VNS is mapped into a three dimensional array which produces a fixed length bit string. This binary length fixed string is combined with error correcting code to construct an effective biometric cryptosystem. Here we use the concept of fuzzy commitment scheme [25].

1.7 ORGANIZATION OF PAPER

The rest of the paper is organised as follows:

- Section 2 related works on biometric cryptosystems are reviewed.
- Section 3 explains the proposed method.
- Section 4 illustrates experimental results of the proposed method.
- Section 5 gives conclusion of the whole report.
RELATED WORKS

A number of works have been done in the field of biometric cryptosystems.

Fuzzy commitment scheme [25] is a pioneer theoretical contribution to combine cryptography and biometrics. In [17] Hao, Anderson, and Daugman (2006) applied FCS to iris pattern and derived 140-bit keys from iris images at FRR=0.47% and FAR=0%. In [26] Juels and Sudan (2002) proposed a classical framework, named fuzzy vault, to bind a key to a biometric trait. In [27] Nandakumar, Jain, and Pankanti (2007) implemented the fuzzy vault for fingerprint and got encouraging results. In [28] Dodis et al. (2004) generalized most of previous methods and gave a theoretical framework of generating robust key from biometric data and analysed the security in the information theory sense. In [29] Fu, Yang, Li, and Hu (2009) discussed the privacy and security issues of biometric systems from the viewpoint of information theory. The reason that applying FCS to fingerprint is that it is difficult to extract fixed-length feature of high distinguishability from fingerprints. So, we use the VNS to generate feature vector.

Fingerprint minutiae forms voronoi tessellations which have good local stability. Local VNS have been used in many authentication systems. They always gave satisfactory performance mainly due to two reasons. Firstly, in a fingerprint if an elastic distortion occurs every minutiae keeps same neighbours until this distortion does not cause any minutiae to move out of the region. In other words, it has a stable local structure. Secondly, in a voronoi tessellation insertion or removal of minutiae affects only local structures [11]. In [21], Yu et
... presented a radial structure based fingerprint matching algorithm. Local matching is carried out by using the radial structures and followed by a global matching when the local matching between template and query fingerprints is unsuccessful. In [24], Soleymani et al. combined Delaunay triangulation and voronoi diagram together to generate a hybrid matching algorithm. Different from the algorithms as in [21-23] which start with local structure comparison, in this algorithm [24], the comparison of global topological polygons generated from the boundaries of Delaunay triangulation is performed first and then the central voronoi cells of fingerprints are compared to compute the similarity between template and query fingerprint images. In [22], Ceguerra et al. introduced an automatic fingerprint verification system based on voronoi neighbour structures. In this scheme, the voronoi neighbour act as local features and help to find a reference axis consisting of the center minutia of a voronoi neighbour structure and one of its neighbour minutiae. Then the reference axis is used to create the global features which are finally taken to calculate the similarity between a pair of template and query fingerprint images. In [23], Khazaei et al. proposed a fingerprint matching algorithm based on the voronoi diagram. In this algorithm, a unique central cell is found and used for local matching. With the help of local central cell matching, this algorithm is able to filter un-matched fingerprint pairs instantly. Moreover, another process is activated when local central cell matching fails under nonlinear distortion.
PROPOSED METHOD

3.1 Generation of bit string using VNS

3.1.1 Generation of VNS

To reduce the problem of fingerprint recognition and increase the effectiveness during the fingerprint recognition caused by distortions we generate a bit string using modified Voronoi Neighbour Structures. This structure is distortion insensitive, rotation invariant and reliable.

Voronoi Neighbour Structures have good local and global structural stability under small distortion. Consider we are given a fingerprint. We create a set of minutiae points \( \{m_1, m_2, \ldots, m_n \} \). For these minutiae points set voronoi tessellations which divides the given fingerprint into smaller regions such that all the points in the region are closer to the respective \( m_i \) than to any other minutiae in other regions. Voronoi Neighbour Structures are formed from the voronoi tessellations by connecting all the minutiae present in all the regions.

3.1.2 Modified VNS

This structure has to be modified to relinquish the change caused by the distortion. Take a minutiae as central minutiae for all other minutiae. This minutiae must be connected to all its neighbour minutiae in the voronoi tessellation[11]. By joining all these points we draw triangles.
To reduce the distortion caused in the same fingerprint we draw Delaunay triangulation for these triangles. A Delaunay Triangulation ensures that circumcircle associated with each triangle contains no other point in its interior. In figure 1.3 (a) circumcircle associated with T1 and T2 are empty. So this is a Delaunay triangulation. Where in figure 1.3 (b) circumcircle is not associated with T1 or T2 i.e., contains a point in their interior. While capturing image there may be distortion which causes enlargement of division of minutiae. If large distortion moves minutiae out of the region VNS will be changed[12]. By Delaunay triangulation this problem can be solved. Even if some points are not included because of Delaunay the circumcircle will be extended which removes the distortion and includes previously not included minutiae. This new structure is called as Modified Voronoi Neighbour Structure. Figure 1.4(a)Voronoi tessellation (b)Delaunay Triangulation(bold)
Using the modified VNS obtained above we generate a bit string with a 3D array. Minutiae extracted from fingerprint can be represented as 

\[ m = (x, y, \Theta, t) \]

Where \((x, y)\) is the co-ordinate of minutiae, \(\Theta\) is the orientation, \(t\) is the type of minutiae. To generate bit-string we adopt a 3D array mapping [13-15] method where we map VNS into a 3D array. Let \(W_x, W_y, W_z\) be length, breadth, height of the array. \(C_x, C_y, C_z\) be length, width, height of each cell in the 3D array. Central minutiae which is at the centre of first layer of 3D array is \(m = (x_1, y_1, \Theta_1)\). Remaining VNS \(m_n = (x_n, y_n, \Theta_n)\) are rotated and transformed based on central minutiae to form new co-ordinate \(m_n' = (x_n', y_n', \Theta_n')\) using the following formula:

\[
\begin{align*}
X_n' &= \cos(\Theta_1)x_n - \sin(\Theta_1)x_1 + \frac{W_x}{2} \\
Y_n' &= \sin(\Theta_1)x_n + \cos(\Theta_1)y_n - y_1 + \frac{W_y}{2} \\
\Theta_n' &= \Theta_n - \Theta_1 \text{ if } \Theta_n \geq \Theta_1 \\
&= 2\pi + \Theta_n - \Theta_1 \text{ if } \Theta_n < \Theta_1
\end{align*}
\]

Now central minutiae is located at \((W_x, W_y, 1)\). Now bit-string can be obtained by following method: If a cell in an array contains the minutiae then it is assigned 1, else it is assigned 0. Even if more than one minutiae fall in the same cell it is assigned as 1. By this method distortion which shifts minutiae can be tackled. The length of the bit-string is \((W_x/C_x) \cdot (W_y/C_y) \cdot (W_z/C_z)\).

Figure 1.5 (a) Local VNS (b) 3D array with VNS mapped onto it (c) Bit string formed on the array where VNS is mapped.
Figure 1.5 Generation of bit string from 3D array

3.2 Error Correcting Code

Error correction is detection of errors and reconstruction of original, error free data. Among all error correction schemes we use error correcting code. It is a system of adding redundant data to a message such that corrupted message can be recovered where we can even specify the number of errors. There are two types of ECC’s: Convolutional and Block. Under block codes there are many methods [16-18]. In this method we will use Reed Solomon Codes.

Reed Solomon Codes are non-binary BCH codes or linear block codes. To construct non-binary BCH codes we use same method as binary BCH codes. Roots of $g(x)$ are $GF(q^m)$ where $n=(q^m) - 1$.

Choose 2t consecutive powers of $\alpha$, an element of order $n$ in $GF(q^m)$. For RS codes, $m=1$ and $\alpha$ is a primitive element in $GF(q)$, then

$$n=q-1$$

$$n-k \leq 2t \rightarrow n-k=2t$$

$$d \geq 2t+1 \rightarrow d \geq n-k+1$$

Reed Solomon code is denoted by $RS(n,k)$

Where $n=$ codeword length

$$(n \text{ is between 7 and 65535})$$
k=message length

For Reed Solomon codes, the code minimum distance is given by [20]
\[ d_{\text{min}} = n - k + 1 \]

The code is capable of correcting any combination of ‘t’ or fewer errors, where ‘t’ can be expressed as [21]
\[ t = \frac{n - k}{2} . \]

### 3.2.1 Reed Solomon Encoding

Reed Solomon Encoder is used at the transmit end by which redundancy bytes are added to the input data to be transmitted. RS encoder is designated as (msg,n,k)

Where msg = data to be encoded

\[(n,k) = \text{Reed Solomon Code}\]

Codeword is obtained by using RS encoder. This codeword (c) is set for thresholding (thr). Thresholding of codeword can be defined as:

\[
c = \begin{cases} 
0 & \text{if } c \leq \text{thr} \\
1 & \text{if } c > \text{thr} 
\end{cases}
\]

Where thr=2

Here the dimension of all bit-strings are reduced to the size of the codeword to eliminate the correlation between bit-strings with different users. Now XOR operation is performed for binary fixed length string of template fingerprint (b) and codeword (c) obtained from RS encoder. This value is stored in ‘e’. \( e = b + c \). Meanwhile the hash value of codeword is calculated i.e., \( h(c) \).

### 3.2.2 Reed Solomon Decoding

Reed Solomon Decoder is used at the receiver to correct the errors occurred on the way by use of redundant information. RS decoder is designated as (code,n,k)
Where code = data to be decoded

\[(n,k) = \text{Red Solomon Code}\]

Here query fingerprint \((b')\) is XOR’ed with the ‘e’ value stored during encoding to obtain \(e'=b'+e=b'+b+c\). This \(e'\) is decoded using RS decoder to form \(c'\). This decoded codeword \((c')\) is reduced in dimension and thresholding is done to this codeword \((c')\).

Thresholding can be defined as:

\[
c = \begin{cases} 
0 & \text{if } c' \leq \text{thr} \\
1 & \text{if } c' > \text{thr} 
\end{cases}
\]

Where \(\text{thr} = 12\)

ON the other-side hashvalue of \(c'\) is calculated i.e., \(h(c')\).

Finally if \(b\) and \(b'\) are from same trait then we will get \(h(c)=h(c')\).

### 3.2.3 Matching

Consider a fingerprint is captured by an input device. This is extracted into a feature vector and is stored. A matching must be done to see if any false acceptance or false rejection of fingerprint is there. Matching must be done to the input trait and stored feature vector using a threshold set for comparison. These are calculated using match scores. Depending on matching score, input is classified as genuine or imposter. Genuine score means similarity or difference between templates belonging to the same trait. Imposter score means similarity or difference between templates belonging to different trait. The higher the score the more similar the samples are. Threshold concludes that scores above this value can be considered as genuine and scores below are considered as imposter. There are some parameters used to calculate the score which will be explained in next section.

### 3.3 Performance Parameters

There are parameters used to measure the performance of a biometric system. They are
3.3.1 Verification

It is one to one matching which involves confirming or denying the claimed identity of a person by comparing with the stored template of the claimed identity and measuring the degree of similarity.

3.3.2 Identification

It is one to many matching where a person identity is compared with all stored templates of various feature vectors. Here similarity is calculated using scores.

3.3.3 False Acceptance Rate (FAR)

FAR is the probability that a user making a false claim about his/her identity will be verified as that false identity. FAR is matching between input and non-matching template. FAR is fraction of imposter score > threshold.

3.3.4 False Rejection Rate (FRR)

FRR is the probability that a user making a true claim about his/her identity will be rejected as him/herself. FRR fails to detect match between input and matching template. FRR is fraction of genuine score < threshold.
3.3.5 Equal Error Rate (ERR)

False Accept Rate and False Reject Rate intersect at certain point. At this point FAR=FRR. This is called Equal Error Rate (ERR). ERR indicates accuracy of the system. In general lower the ERR the higher is the accuracy of the biometric system.

![Equal Error Rate Diagram](image)

3.3.6 Genuine Acceptance Rate

It is the fraction of genuine scores that exceeds the threshold.

\[ \text{GAR} = 1 - \text{FRR} \]

3.3.7 ROC Curve

It is plotting False Accept Rate vs False Reject Rate.

3.4 Calculation

In this method matching is done to calculate both genuine and imposter score. Here score is calculated using pdist2 method which calculates distance between given two sets of observations. In this many metrics can be used to calculate the distance but in this method we use spearman method.

![Random ECC Hash Diagram](image)
4. Experimental Results and Analysis

4.1 Database Selection

For the proposed method we evaluate using FVC 2002 3 databases i.e., DB1, DB2, DB3 where each database consists of 800 fingerprint images which are collected from 100 fingers with 8 samples from each finger.

4.2 Extraction of minutia

Minutia are extracted from each fingerprint image by using software VeriFinger 6.0 from Neuro-technology [30].

4.3 Performance Evaluation

There are three performance metrics used for performance evaluation. They are (1) FAR which is ratio of unsuccessful genuine attempts to total genuine attempts, (2) FRR which is ratio of successful imposter attempts to total imposter attempts, (3) ERR which is defined as the value when FAR=FRR. We have to compare our results with other
works. So, we have to divide the database into two sets. In the proposed method we take only two images for each fingerprint. Two different protocols are used for recognition of the proposed method: 1vs1 protocol and FVC protocol.

For this data set 1vs1 protocol is used. First image of each finger is compared with another image from same finger. From this we can calculate FRR by using the values of ‘e’ stored. First image of each fingerprint is compared with two images of remaining fingerprints. From this we can calculate FAR. This comparison is done for all 100 fingerprints. So it results in 100 genuine matching attempts and 2450 imposter matching attempts.

In this method for matching score is calculated by calculating the distance between two sets of observations. For this we use two methods: (1) Spearman(2) Correlation.

The database is fixed with some values for Wx, Wy, Wz of array and Cx, Cy, Cz of cell. Mx=Wx/Cx, My=Wy/Cy, Mz=Wz/Cz. The product of the three i.e., Mx, My, Mz gives the length of the whole array. By varying the size of Mx, My and Mz we have obtained matching performance of the proposed method in terms of the EER which are applied on the database FVC 2002 DB1, DB2 and DB3. We have used two methods to calculate the distance between two sets of observations. For each method we have got different EER.

Table 1 describes the EER obtained for different values of Mx, My, Mz using the spearman method. The optimal values are obtained at Mx=5, My=5, Mz=10 (250) i.e., size of array is 250. The EER value is also optimal when compared with others i.e., at DB1 it is 1.55%, at DB2 it is 2.84%, at DB3 it is 1.1%. Maximum value is obtained at size of Mx=10, My=10, Mz=10 with size of array as 1000 i.e., EER at DB1=4.4%, at DB2=19.46%, at DB3=1.25%.

Table 1

Array size values and EER(%) on DB 2002 using spearman method
Table 2 describes the EER obtained for different values using the correlation method. Minimum value is obtained at $M_x=5$, $M_y=5$, $M_z=10$ (bold) i.e., at DB1 it is 1.83% at DB2 it is 2.24%, at DB3 it is 1.04%. For these two methods overall optimal values are taken at $M_x=5$, $M_y=5$ and $M_z=10$ and the best method is correlation. The EER values are 1.83% for DB1, 2.24% for DB2 and 1.04% for DB3.
Among all databases DB2 gives high EER for both methods and DB3 gives low EER for both methods.

**Table 2**

Array size values and EER(%) on DB 2002 using correlation method

<table>
<thead>
<tr>
<th>DATABASE</th>
<th>Mx</th>
<th>My</th>
<th>Mz</th>
<th>EER(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002 DB1</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>01.98</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>10</td>
<td></td>
<td><strong>01.72</strong></td>
</tr>
<tr>
<td>5</td>
<td>8</td>
<td>10</td>
<td></td>
<td>01.84</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>5</td>
<td></td>
<td>02.76</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>7</td>
<td></td>
<td>03.78</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>10</td>
<td></td>
<td>02.04</td>
</tr>
<tr>
<td>2002 DB2</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>01.73</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>10</td>
<td></td>
<td><strong>02.70</strong></td>
</tr>
<tr>
<td>5</td>
<td>8</td>
<td>10</td>
<td></td>
<td>06.84</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>5</td>
<td></td>
<td>23.10</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>7</td>
<td></td>
<td>24.00</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>10</td>
<td></td>
<td>22.24</td>
</tr>
<tr>
<td>2002 DB3</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>01.25</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>10</td>
<td></td>
<td><strong>01.59</strong></td>
</tr>
<tr>
<td>5</td>
<td>8</td>
<td>10</td>
<td></td>
<td>01.64</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>5</td>
<td></td>
<td>01.14</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>7</td>
<td></td>
<td>01.17</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>01.17</td>
</tr>
</tbody>
</table>
The error correcting code used here is reed Solomon. It gives minimal value of EER when compared with other error correcting codes such as BCH code.

**4.4 ROC Curves**

![ROC Curves](image)

**Figure 1.7** ROC curve for FVC 2002 DB1 for both methods i.e., (a) correlation (b) spearman

![ROC Curves](image)

**Figure 1.8** ROC curve for FVC 2002 DB2 for both methods i.e., (a) correlation (b) spearman
Fingerprint Biometric Cryptosystem combining Error Correcting Code and Modified Voronoi Neighbour Structure

5. Conclusion

In the modern society information security is more important and is receiving many challenges. Biometric cryptosystems which combines cryptography and biometrics provide security to the information. Fuzzy commitment scheme is best used for this and it generates binary fixed length feature vector. But extracting feature vector from fingerprint is difficult due to uncertainty during capturing. So, in this paper we proposed an alignment free bio-cryptosystem based on modified VNS. Fingerprint uncertainty which is caused due to distortion is reduced by forming VNS and modifying the VNS. Generally small distortion within the region is dealt with 3D array quantization whereas large distortion is dealt with modified VNS. Afterwards binary feature is used with FCS combining ECC i.e., Reed Solomon Code. This code corrects if any error is there. Matching is also done for this. Experimental results shown indicates that the proposed method performs well.

Figure 1.9 ROC curve for FVC 2002 DB3 for both methods i.e., (a) correlation (b) spearman.
REFERENCES


