**Hand Based Cancelable Biometric Authentication Scheme**

By

Faizanur Rahman (Roll No. 2015085)

&

Manish Kumar Vyas (Roll No. 2015144)

Supervisor:

Dr. Pritee Khanna



Computer Science and Engineering

**INDIAN INSTITUTE OF INFORMATION TECHNOLOGY DESIGN & MANUFACTURING, JABALPUR**

May 28, 2018 to June 14, 2018

# CERTIFICATE

This is to certify that the thesis entitled, “Hand Based Cancellable Biometric Authentication System using X-OR transformation” submitted by Mr. Faizanur Rahman (2015085) and Mr. Manish Kumar Vyas (2015144) in partial fulfilment of the requirements for the award of degree of Bachelor of Technology at PDPM Indian Institute of Information Technology, Design and Manufacturing, Jabalpur is a record of genuine work carried by him under my supervision. To the best of my knowledge, the material embodied in this thesis has not been submitted elsewhere to any other university/institute for the award of any degree.

#### Dr. Pritee Khanna (Associate Professor)

#### Computer Science and Engineering

PDPM Indian Institute of Information Technology, Design and Manufacturing, Jabalpur

482005, India.

Date………….

Place………

# ACKNOWLEDGEMENT

I would like to take this opportunity to thank everyone who helped, guided and motivated us through the whole project. We would like to express our special thanks of gratitude to our supervisor Dr. Pritee Khanna for giving us this great opportunity to work under her excellent guidance and valuable advice. This project would not have been possible without her support and encouragement. Her guidance and valuable advice not only helped me to improve my technical knowledge but also improved my ethical life which will help me in the future as well.

We greatly appreciate the motivation and technical support by **Ms. Harkeerat Kaur** and **Mr. L. Druva Kumar** who responded promptly to our request for frank comments. We would like to thank the institute for providing us all the valuable resources, and an opportunity to gain knowledge and exposure.

At last but not the least, we would like to thank our dear parents who encouraged us to extend our reach, with their help and support, we have been able to complete this.

Faizanur Rahman

2015085

[faizanurrahman@iiitdmj.ac.in](mailto:faizanurrahman@iiitdmj.ac.in)

+91 9155197873

Mr. Manish Kumar Vyas

2015144

### TABLE OF CONTENTS

|  |  |  |
| --- | --- | --- |
| Sr. Number | Name of the Chapter | Page Number |
| **Chapter 1** | **INTRODUCTION** |  |
| **Chapter 2** | **LITERATURE REVIEW** |  |
| **Chapter 3** |  |  |

***Chapter 1***

**INTRODUCTION 1**

* 1. [Biometric Authentication 1](#_heading=h.30j0zll)
  2. [Cancellable Biometrics 2](#_heading=h.2et92p0)
  3. [Scope of work 3](#_heading=h.3znysh7)

### Chapter 2

#### LITERATURE REVIEW 4

* 1. Biometric Cryptosystem 4
  2. Cancellable Biometric 4
     1. Biometric Salting Technique 4
     2. Non Invertible Transformation 5
  3. Motivation 7

***Chapter 3***

#### PROPOSED TEMPLATE TRANSFORMATION SCHEME 8

#### 

* 1. Data Acquisition
  2. Pre Processing 8

|  |  |  |
| --- | --- | --- |
| 3.2.1 | Introduction | 9 |
| 3.2.2 | Image Segmentation   1. Image Segmentation based on statical approach 2. Image Segmentation based on edge 3. Image segmetation based on wavelet transform | 9 |
| 3.2.3 | Edge Linking   1. Morphological Operation 2. ExtraPolation | 10 |
| 3.2.4 | Log Transform |  |
| 3.2.5 | Local Contrast Enhancement |  |
| 3.2.6 | Laplacian of gaussian |  |
| 3.2.7 | Convolution with Maxican Hat filter |  |

* 1. Feature Extraction 10
     1. Maximum Curvature Method 12
  2. Non Invertible Transformation 13
     1. XOR Function 13
     2. Median Filtering 14
  3. Matching 15
  4. Evaluation of Performance Parameters 15
     1. Confusion Matrix for Multi Class Classification System 15
  5. K-fold Cross Validation 16
     1. K-fold Cross Validation with different random keys 16

### Chapter 4

***Chapter 5***

#### EXPERIMENTAL RESULTS AND ANALYSIS 17

* 1. Evaluation Scenarios 17
  2. Visualizations 17
  3. Performance Analysis 20

#### CONCLUSIONS 21

#### REFERENCES 22

**CHAPTER 1: INTRODUCTION**

**Project Origin Details:** (**Status: On-going**).

Privacy Enhancing Revocable Biometric Identities (PERBI), 2016-19 –Awarded by **Board of Research in Nuclear Sciences (BRNS),** Department of Atomic Energy, Govt of India (Funding Rs. 28.8 lacks).

I contributed to the above live projects under the supervision of **Dr. Pritee Khanna (Principal Investigator)** at the Indian Institute of Information technology, and built a Multimodal Biometric System with Revocable Capabilities, and Implemented a dorsal hand vein authentication system from scratch.

**My Major Contribution:**

1. During Processing Dorsal Hand Image, developed a heuristic blurring method to remove hair from the image.
2. Extracted clear vein pattern from the dorsal Image by Implementing Maximum Curvature Method.
3. Implemented a Cancellable capability to address the Stolen token (user information) scenario.
4. Reduce the dimension of data up to 75% and achieve 94% multi-class classification accuracy.

In this project, I was to build a biometric authentication system and need to perform authentication based on a person's vein pattern. Since veins are present inside the body, in most cases, not visible to the naked eye so this system was more secure than others.

# CHAPTER 2: LITERATURE REVIEW

This chapter talks about the previous works that have been done and also tells about the motivation behind the contributing to this project*.*

In this chapter, also, we will introduce the system of biometrics and discuss various security concerns related to biometrics in the current scenario. Also, we will talk about cancellable biometrics and the feature of recurrence.

**Biometrics** is an excellent system for security used in various platforms such as industry, banking, mobile phones. Presently, many methods are available to verify individual identities, such as fingerprint recognition, voice recognition, retinal scans, facial recognition.

These systems also pose a risk of compromising biometric information in many ways, such as **fingerprints can be hacked from glass panels or other locations** by mimicking their fingerprints. In the past, fingerprint systems have repeatedly been hacked by the **sticky fingerprint method**.

To address this problem and to provide better preservation of information, we are attempting to develop a biometric detection system based on the idea of ​​cancelable biometric.

## Biometric Authentication System

Biometric authentication is a process in which a person's identity is verified based on specific biological characteristics. In biometric authentication, first, a person's biometric information is captured and then matched with the data stored in the database. If both data (captured and stored) match, the authentication is confirmed.

Biometric authentication is the most effective and secure authentication system because a person's biological information is unique. It is possible that a person's password and unique ID can be stolen and misused. Biometric identity is always safe, cannot be leaked, and very difficult to transfer from one person to another.

## Cancellable Biometric Authentication

Since biometric authentication is a widely used authentication system in various departments and is stored digitally in a database, there are chances that someone can steal a piece of biometric information by invading the database and misuse its confidential information.

To avoid such attacks and secure our data, we can use the cancellable biometric authentication system. To protect biometric information in this cancelable biometric system, we intentionally and repeatedly distort the user's biological data.

Templates are responsible for the distortion in the feature by which the original data transformed into some other information. When an attacker tries to steal data, he gets changed information instead of the original information. To secure the user's information and deactivate the stolen data is done by changing the template information, which changes all previous biometric information in the database.

**Motivation**

In the past, much work has already been done to secure biometric information. Many research papers have been published. In all these researches, biometric salting and non-invertible transform techniques were used. The biometric salting technique includes Random Projection, Random Convolution, Random Mapping, and Random Noise transformation. non-invertible transformation includes median filtering technique.

After doing a literature review, I found the following inspiration for this project.

1. I noticed in the literature review that the dorsal veins are novel biometric features. They are more secure than other biometric features such as thumbprints. The dorsal vein also tells us about the livelihood of the individual, as the image of the dorsal vein captured by the device depends on the thermal heat generated during blood circulation. If a person is not alive, the vein patterns will not clear.

2. I noticed in the literature review that After 2010, There are not many contributions in this area yet.

3. I observe in the literature review that there is no contribution to dorsal hand cancellable biometric.

# CHAPTER 3: Building Dorsal Hand Vein Authentication From Scratch

* 1. **Data Acquisition**

**About Data:**

I used 850 dorsal hand images of size 400\*400, taken from a special device that uses Infrared light to capture veins data. **850 Biometric Data = 85 people, 10 samples each**.

**How data capture devices work:**

Unlikely to oxygenated hemoglobin, deoxidized hemoglobin absorbs light at a wavelength of about 760nm, which is in the range of the near-infrared (NIR) band. Therefore, when the dorsal hand is illuminated with near-infrared light, deoxidized hemoglobin absorbs the light and appears as a black pattern in the dorsal image.

**Sample Image Data:**



**Statistical Property of image, this is approximated value with 20 sample using ImageJ software:**

Statistical parameters provide us information regarding spatial distribution, changes in brightness, and description regarding the structural arrangement of vein patterns.

|  |
| --- |
| Fig 1. Sample image histogram and statistical properties taken from ImageJ software. |

Channel: gray scale

Histogram- unimodal

Min pixel: 31

Max pixel: 214

Mean: 154.702

Variance: 1044.885

Skew: -1.03

Kurt: 1.505

#### Pre-processing

The aim of pre-processing is to improve the existing feature in the data. In the dorsal hand vein image, it suppresses unwillingness to distortions or enhances the visibility of the vein pattern.

**Why do we need to enhance the image?**

Because in real-time, the biometric user has hair on their dorsal arms, which reduces the accuracy of biometric authentication. If we want to make biometric reliable and robust in real-time, first of all, we have to remove hair from the image. While smoothing the image data, I found that smoothing does not work. It fails to remove hair, and also it produces the undesired result.

Because we know that, in the Fourier domain, noises have a higher frequency than features. Hence the low pass filter like Gaussian filter, median filter, and mode filter should have to remove higher frequency from noisy data but, it doesn't work because veins are present in the neighbor of hairs. That's the reason for the undesired appearance of noise in enhance data.

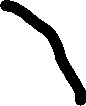
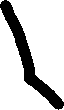
**To understand what is going, look at the plots of the image surface.**



****

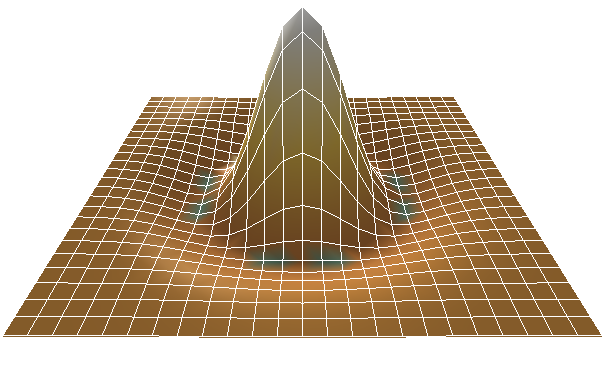
****

****





****As we can see above image, there are two types of lines are drawn -one is red and other is black. After smoothing, I observe that black line is still there in filtered data but red line is not present which is undesired, also I observe that around the veins pattern there are little nose which is due to hair. Also, if we pass our data trough High Pass filter then again undesired result found as shown on right side. After doing research and experiment on smoothing filters, I developed a heuristic method (Normalized Mexican Hat Filter) that completely removed hair without affecting vein patters.

**Normalized Mexican Hat filter.**

Mexican filters is the negative [normalized](https://en.wikipedia.org/wiki/Normalizing_constant) second order [derivative](https://en.wikipedia.org/wiki/Derivative) of gaussian filter. When a flat surface (with any pixel intensity) convolved with kernel then all resultant will be flat surface (with zero-pixel intensity). I deigned a positive normalized (mean is non-zero) of Mexican kernel.

**Pre-Processing and Hair Removal Consist of Three Step.**

**Log Transform –**

During log transformation, the dark pixels in an image are expanded as compare to the higher pixel values. i.e. Reduced skin pixel intensity by surpassing higher pixels and enhance hair structure by expanding the dark pixel.

**Local Adaptive Histogram Contrast Enhancement:**

Local contrast enhancement (LACHE) is a technique for bringing out detail and texture in an image. It is very similar to sharpening which accentuates only fine and **Stochastic component** detail of dark pixel.

**Normalized Mexican hat filter**

**// need source**

**3.3 Feature Extraction**

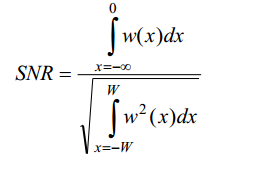
Features are relevant information in image or data, which can be used to identify present content in image. It provides information regarding spatial distribution, changes in brightness, and description regarding the structural arrangement of surfaces. Therefore, the use of textural features is an important source of information for image description.

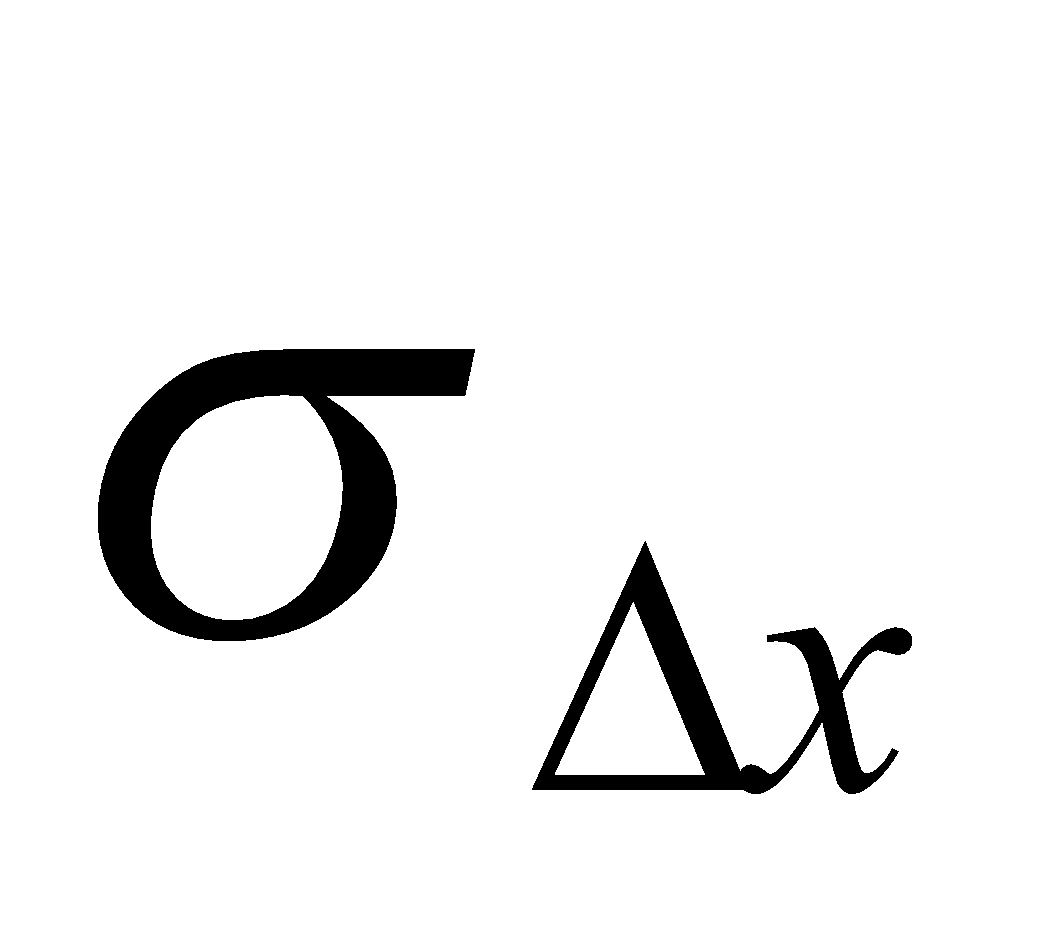
Feature extraction algorithms can be broadly classified into two class: one is a **dense descriptor** which extracts local features pixel by pixel over the input image, the other is a **sparse descriptor** which first detects the interest points in a given image and then samples a local patch and describes its invariant features.

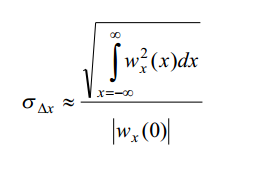
Feature descriptors are extracted from the input image and can be based on **first-order statistics, second-order statistics, parametric models, coeﬃcients obtained from an image transform, or even a combination of these measures.**

Good feature descriptors pose some quality which includes,

**Good detection:** Operation should have a low probability of missing an edge as well as should have a low probability of falsely marking non-edges**. In other words, detected feature should contain relevant information.** Good detection is expressed mathematically in terms of the signal-to-noise ratio (SNR). This ratio is defined as the quotient between the response on the step (edge) and the standard deviation of the noise. SNR is directly proportional to high rate of detection.

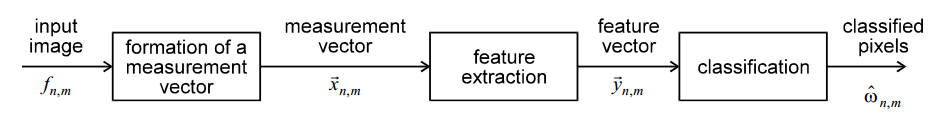


**Good localizations:** Good localization is defined with the standard deviation of the localization error IMG_259the operation should locate an edge at the correct position. **In other words, detected feature should be accurate as much as possible.**



**Immunity to interfering objects:** The detection of an edge should not be affected by the presence of edge structures coming from neighboring objects. **In other words, detected feature should be independent and non-overlapping to each other.**

Let’s define some fundamental structure for feature extraction.



For feature extraction, firstly we have to formulate a measurement vector based on information regarding spatial distribution, brightness level, and description structural arrangement of surfaces. Formulated vector can be a form of Statistical models, Parametric models, etc.

**Feature Extraction from Statistical Method:**

Methods based on the statistical approach do not explore hierarchical structures presented by the texture, but represent its properties in indirect and probabilistic manner.

**a). First-Order Statistics (Thresholding operation):**

To formulate a measurement vector, we have to choose a critical value, which divide image into two parts -object part, and non-object part.

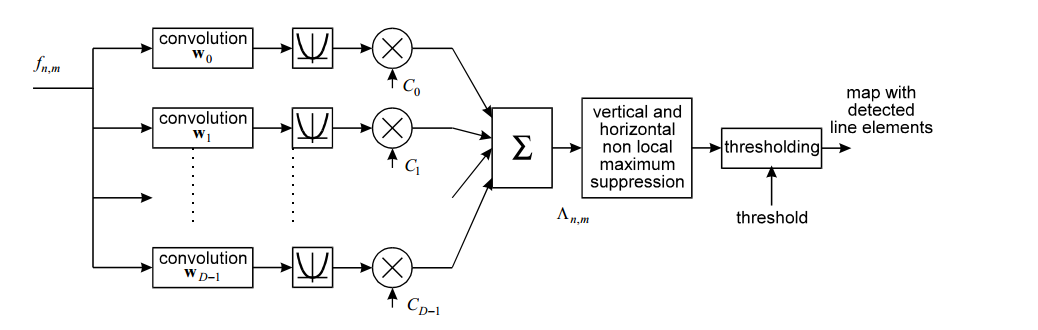
1. Gray Level Thresholding

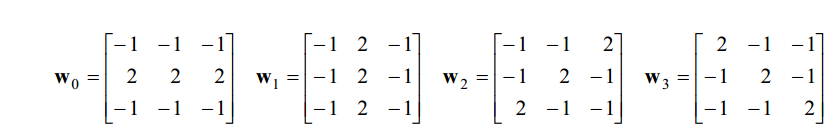
In first order critical values are decided by mean and variance of image. In our case, the image plane contained three regions -skin, vein and hair. For detecting these three segments we have to calculate the conditional probability of each region. We have to determine a decision function that maps the input image onto three regions. Decision function is equivalent to the application of a multi-threshold operation to the grey level. The performance of the method is poor. Since our image data-sets have unimodal distribution of gray level. So, PARZEN estimated conditional probability of these three segments is overlapped. Due to overlapping zones in the conditional densities the error rate is unacceptable large. This above method is also known as **gray level thresholding.** We can improve this result by taking local threshold on predefined size of kernel unlike gray level thresholding take global threshold values.

**a). Second-Order Statistics (Line, Edge detection):**

In first order statistics, since it is described by mean and variance so it only considers individuals pixels that makes feature measurement more sensitive to changes in image. Therefore, to avoid this problem, we can use **second order statistics** that depends on the transitions between two or more pixel in image.

**Line detection:**





The classical way to detect line elements is to correlate the image with a number of templates. Each template aims at the detection of a line element with a specific orientation. The templates are chosen such that - taken together - all orientations are covered. Usually the orientation is quantized to four directions: horizontal, vertical and diagonal. Known templates for these directions are:

For each image pixel location, the cross correlations between the image data and the four templates are determined. The maximum of the four correlations represents the degree of match at that image pixel location. Comparing this maximum with some well-chosen threshold is the simplest method to complete the detection process. Unfortunately, such a process yields configurations of line elements which violates the **constraint of thinness.** A more sophisticated method is to add non-local maximum suppression schemes, applied to each of the four correlated images. In order to prevent the connectedness between line elements from being broken the directional suppression method is used, i.e. matched to the orientation of the template.

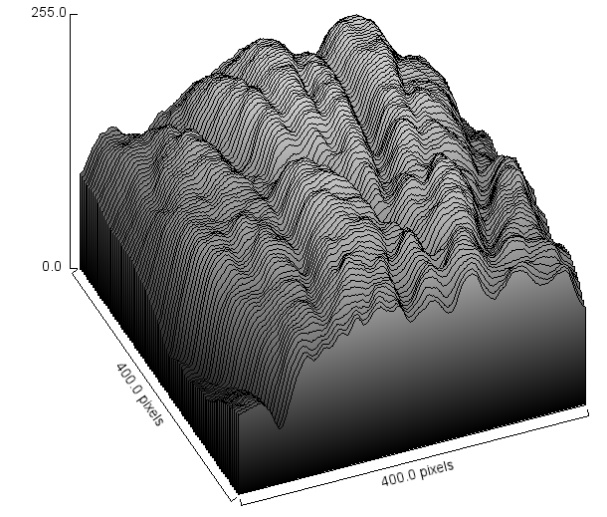
The performance of the method is poor. Due to non-local maximum suppression multiple responses which coming from different templates that produce maximums at neighboring positions.

An improvement of the performance is achieved when the four templates are replaced with one **rotationally invariant template.**

**Local Maximum Curvature Feature Detector**

To detect feature based on first order statistics or higher order, the local threshold is decided by local profile of either side of dent profile but due to presence of noise in data, vein feature detection quality decreases. So, I need a method that consider the surface and structure of veins. In literature review, I found that there is already a method is developed for finger vein extraction, called **Maximum curvature method**.

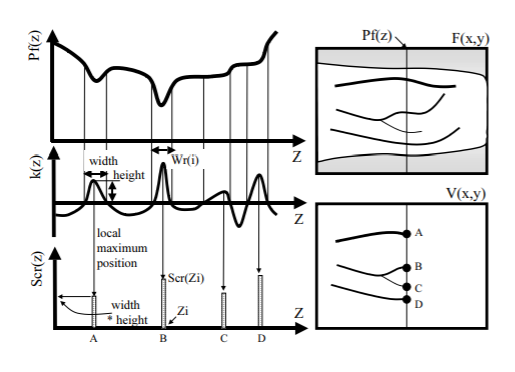






As we can clearly see in surface plot that where veins are present that looks like a dent valley (at point A and B). Since veins have less intensity then skin, so somehow, we have to detect the dent valley to extract clear vein pattern.





Earlier, the local threshold is chosen to separate vein pattern from skin but due to present of noisy data not acceptable vein patter are extracted. To address this problem N. Miura, A. Nagasaki, and T. Miya take et. Al. carefully designed a method to extract clear vein pattern. Since as we see in surface plot that when veins are present it is very dent and in other location of surface it has less dent valley. In maximum curvature method, a probabilistic score is given to each location based on width and depth of valley then select a global threshold to segment vein from skin. I implemented a modified version of maximum curvature method in which I choose a local threshold value instead of global threshold.

Maximum Curvature Method is based on cross-correlation between a kernel and a test image. It convolves the kernel with the binary image representing the test image (rotated by 180 degrees), and evaluates how they cross-correlate. If the kernel and test image are very similar, the output of the correlation corresponds to a single scalar and approaches a maximum. In case kernel and probe represent images from the same vein structure, but are misaligned, the output is not guaranteed to be accurate. To mitigate this aspect, Miura et al. proposed to add a small cropping factor to the model image, assuming not much information is available on the borders. This allows the convolution to yield searches for different areas in the probe image. The maximum value is then taken from the resulting operation. The convolution result is normalized by the pixels lit in both the cropped model image and the matching pixels on the probe that yield the maximum on the resulting convolution.

**Miura paper vein extraction steps:**

* Extraction of the center positions of veins
  + Calculation of curvatures profile
  + Detection of center position and assignment of probabilistic score
* Connection of the center positions
* Labeling of the image

**Local Maximum Curvature Method Step:**

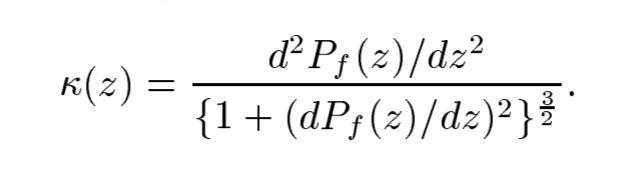
* Extraction of center position of veins
  + Calculation of curvatures profile
  + Detection of center position
  + Assignment of probabilistic score
* Weighted connection of center position
* Local Labeling of center

Let’s discus what are these step-in details.

**EXTRACTION OF THE CENTER POSITIONS OF VEINS-**

Since cross-sectional profile of vein pattern surrounded by skin look like dent because of vein pattern have less intensity then skin. To extract center positions of veins a probabilistic score is assign to each cross-sectional profile to check how much a profile is dent, large value of score show very dent profile. This step is subdivided into three steps as mention below

**CALCULATION OF THE CURVATURES OF PROFILES**

In this step a mathematical function called kappa, is calculated which check whether a profile is dent or not depending on its value.

This kappa equation is designed carefully, we can see in numerator, profile is double derivate which are responsible to detect changes and denominator value normalize overall value. If kappa value is positive then profile is concave upward otherwise it is concave downward. Kappa function preserve structure of texture but it reduces the intensity of dark pixel (vein) and increase the intensity of bright pixel (skin). In other work, Kappa function is a filter that enhances the texture visibility.

I applied Kappa function filter in four direction -horizontal, vertical, and both diagonal directions. As expected, it enhanced the present textures in image, and we get four result images.

**DETECTION OF THE CENTERS POSITION AND ASSIGNMENT OF PROBABILISTIC SCORE**



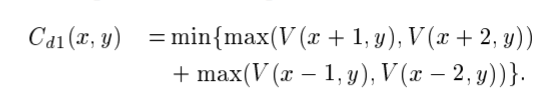
To identify correct location and width of veins in dorsal image, for each direction, I find all peaks and through of profile and then find width by difference of two peaks. Also find height of peaks. For each center position I assigned a probabilistic score by multiplying width and height.

**CONNECTION OF VEIN CENTER:**

Now, I have dorsal image with a score in four direction. Since there is chance of getting noisy vein structure so for connecting the centers of veins and eliminating noise, the following filtering operation is proposed by Miura paper authors.

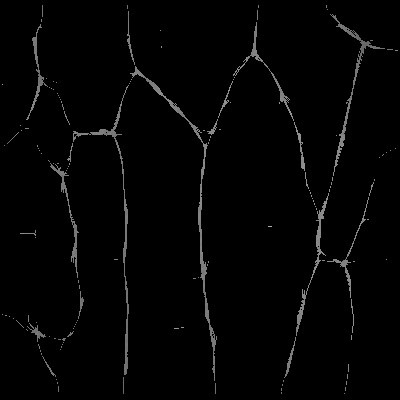
for each center position:

* For horizontal
  + Four neighbor’s pixels are selected, two from left side and two from right side of center.
  + If both sides have larger intensity in compare of center position, then we connect the center position with its neighboring pixels.
  + Else eliminate the center position i.e. intensity value is set to zero.
* Similarly, we can select neighbor’s pixel in other direction too and follow same algorithms as for horizontal direction.



**LABELING THE IMAGE:**

I have four images in all direction with vein pattern as a result of connecting veins center. Now, for each center position I have four pixels value then replace center position with median value of these four pixels value. Finally, binarized the labeled image based on threshold.

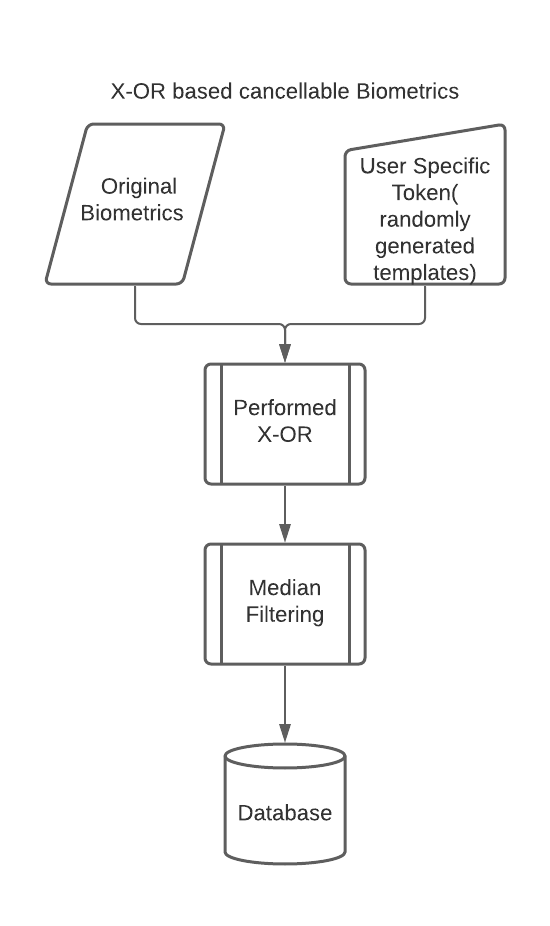


**CANCELLABILITY:**

Biometric systems have been repeatedly hacked using technique like database attack. Therefore, we are trying to develop a biometric identification system based on the idea of “cancelable Biometrics” using a template protection approach generating binary features which are revocable.

To protect our digital biometric information, we convert it to non-invertible transformed information and attacker unable to get original information because transformed data is non-invertible. As we saw in literature review that there are many available methods to provide protection on data like bio hashing, random slop, and X-OR methods.

Implemented Cancellability functionality in our biometric system is shown below:



**CLASSIFICATION OF VEIN PATTERN**

After storing secure biometric data into databases, the most important aspect to complete the system is classification of different biometric data to a genuine person. For this particular instance, I used machine learning. Machine learning takes data and try to find underlying relation between data. There are lot of algorithms out there.

After doing literature review on different types of algorithms in machine learning. I found that,

* Machine learning takes input and map to its output by figuring out internal linkage of input and output. This is called trained model on specific data.
* If algorithms take garbage then it learns the garbage pattern and output is also garbage.
* If input data have high dimension then trained model is underfitting the model that means learned underlying pattern is still unknown (“curse of dimensionality”), either we need more data or we need to reduce the dimensionality of data by famous data reduction technique.
* There are a lot to learn in machine learning, and it’s the basic of all future changing technology.

…need to update…

How I implement classification is shown below:

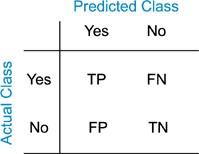
## Evaluation of Performance Parameters

Performance parameters have been calculated using various methods like -

#### Confusion Matrix for Multi-Class Classification System

A confusion matrix is a table that is often used to describe the performance of a classification model (or "classifier") on a set of test data for which the true values are known. For multi-class model one of the class is assumed as positive and other as negative and then confusion matrix is calculated. Same exercise is repeated for all the classes. Confusion Matrix consists of following values -

* + - * *True Positives (TP):* These are cases in which we predicted positive, and actual class is positive as well.
      * *True Negatives (TN):* We predicted negative, and actual class is negative as well.
      * *False Positives (FP):* We predicted positive, but actually it is negative (Also known as a "Type I error").
      * *False Negatives (FN):* We predicted negative, but actually it is negative (Also known as a "Type II error") .



#### Fig. 10. Confusion Matrix

**False Acceptance Rate**

The false acceptance rate, or FAR measures the probability of incorrectly accepting an unauthorized user. FAR can be calculated as follows

FAR = FP / (FP+TN)

#### False Recognition Rate

The false recognition rate, or FRR, measures the probability of incorrectly rejecting an authorized user. FRR can be calculated as follows

FRR = FN / (FN+TP)

#### 3.8 K-fold Cross Validation

In *k*-fold cross-validation, all the samples of a person are randomly partitioned into *k* equal sized subgroups. Of the *k* subgroups, a single subgroup is taken as the validation data group for testing the model and the remaining subgroups are used as training data. This process is then repeated *k* times (the *folds*), with each of the *k* subgroup used exactly once as the validation data. Results obtained over k-iterations are averaged produce a single estimation. One of the advantage of this method is that all observations are used for both training and validation. In our project, we have used k-fold cross validation for k=1.

#### 3.8.1 K-fold Cross Validation with different random keys

K-fold cross validation is performed by changing the randomly generated key (as defined in the section “Non-invertible transformations”) for transformation purpose. Results have been generated for 5 different keys.

DET (Detection Error Tradeoff) curves have also been plotted to visualize the performance of fingerprint after using non-invertible transformations. These curves are plotted between False Positive Rate (FPR) and False Negative Rate (FNR) with FPR on x-axis and FNR on Y-axis.

# CHAPTER 4: EXPERIMENTAL RESULTS AND ANALYSIS

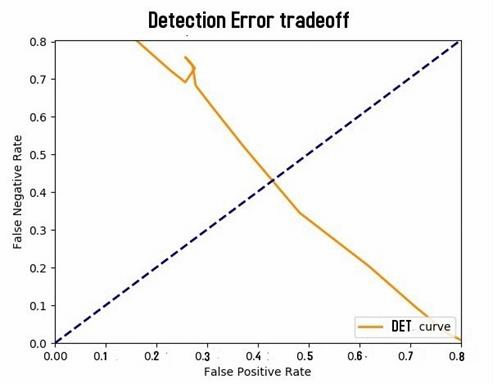
Analysis is performed to study the features of template security such as (i) performance, (ii) non-invertibility, and (iii)changeability of the proposed approach under *stolen token scenario*. It is illustrated that the templates so generated are non-invertible, can be revoked easily and are delivering good performance.

## Evaluation Scenario

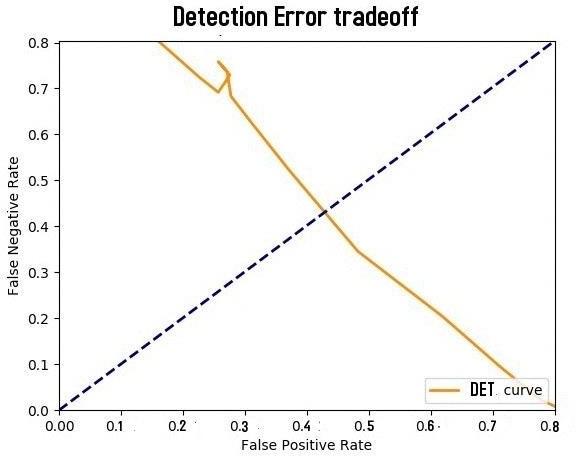
Evaluation of performance parameters has been done on (i) original feature vectors stored in the form of chain codes and then on (ii) transformed chain codes using XOR and median filter methid for transformations. FVC2004 DB1A [10] database of 1680 images (140 subjects with 12 samples each) is divided as 7 images for training and 5 images for testing.

## Visualizations

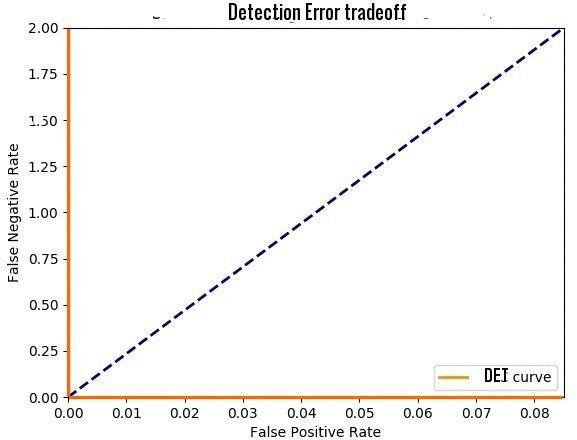
Some of the visualizations are –



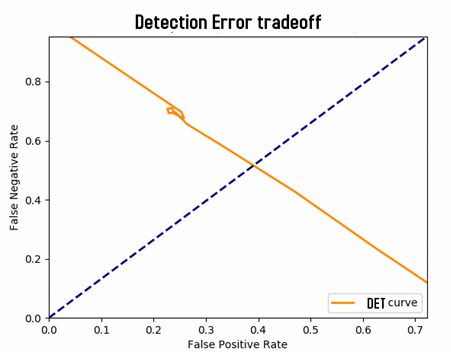
#### Fig. 11(a). Original case implementation with K-fold cross validation.



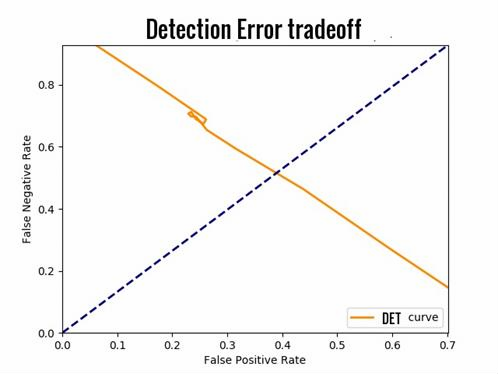
**Fig. 11(b). Worst case implementation with K-fold cross validation.**



**Fig. 11(c). Best case implementation with K-fold cross validation.**



**Fig. 12(a). Worst case implementation with K-fold and 5 different Keys (5 Way K-fold).**



**Fig. 12(b). Worst case implementation with K-fold and 10 different Keys (10 Way K-fold).**

It is observed that matching is being done with a very high accuracy on the databases as described above (in the section of “Acquisition”). Accuracy and other parameters like *False Positive Rate (FPR)*, *False Negative rate (FNR)* and *True Positive Rate (TPR)* have been recorded and visualized on various threshold values.

The efficiency for original feature vector obtained directly from the image in the form of chain codes obtained was 100% .

The efficiency after applying non-invertible transformations to the original feature vector obtained was 100% for both worst and best cases.

|  |  |  |  |
| --- | --- | --- | --- |
| **Method/Case** | **Original Case** | **Worst Case** | **Best Case** |
| **K-fold** | 0.42 | 0.44 | 0.00 |
| **5-way K-fold** | - | 0.45 | 0.00 |
| **10-way K-fold** | - | 0.46 | 0.00 |

#### Table 1. Equal Error Rate using different methods for different cases

* 1. **Performance Analysis**

Worst case performance is comparable to original case which proves that the distortions provided by the transformations to the original templates does not reduces the uniqueness of the fingerprint.

A median filtered chain code was taken and XORed by the same set of keys at three levels to obtain a new chain code. The new chain code so generated did not match the original code that was initially. Therefore, median filter transformation provides the feature of non-invertibility.

Original chain codes were converted to rotation invariant chain code thereby providing the feature of alignment free which ensures that in whatever angle input template is given the output chain code will be same.

# CHAPTER 5: CONCLUSIONS

Performing training and testing on different database along with non-invertible transformation techniques and various visualizations of performance evaluation parameters reveals that the templates so generated are non-invertible, can be revoked easily and are delivering good performance. The proposed approach based on cancellable biometrics has been tested and is successfully working and hence ready to implement.

# REFERENCES

1. S. Chikkerur, N. Ratha, J. Connell, R. Bolle, Generating registration-free cancelable fingerprint templates, in: Proceedings of the 2nd IEEE International Conference on Biometrics: Theory, Applications and Systems, 2016, pp. 1–6.
2. C. Lee, J.-Y. Choi, K.-A. Toh, S. Lee, Alignment-free cancelable fingerprint templates based on local minutiae information, IEEE Trans. Syst., Man, Cybern., Part B 37 (4) (2016) [980–99](http://refhub.elsevier.com/S0031-3203(17)30021-3/sbref3)2
3. S. Tulyakov, F. Farooq, P. Mansukhani, V. Govindaraju, Symmetric hash functions for secure [fi](http://refhub.elsevier.com/S0031-3203(17)30021-3/sbref4)ngerprint biometric systems, Pattern Recognit. Lett. 28 (2007)

2427[–](http://refhub.elsevier.com/S0031-3203(17)30021-3/sbref4)2436[.](http://refhub.elsevier.com/S0031-3203(17)30021-3/sbref4)

1. G. Kumar, S. Tulyakov, V. Gavindaraju, Combination of symmetric hash functions for secure fingerprint matching, in: Proceedings of the 20th International Conference on Pattern Recognition, 2010, pp. 890–893.
2. B. Yang, D. Hartung, K. Simoens, C. Busch, Dynamic Random Projection for Biometric Template Protection, in: Proceedings of the 4th IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), 2010, pp. 1– 7.
3. [T. Ahmad, J. Hu, S. Wang, Pair-polar coordinate-based cancelable fi](http://refhub.elsevier.com/S0031-3203(17)30021-3/sbref5)ngerprint templates, Pattern Recognit. 44 (10[–](http://refhub.elsevier.com/S0031-3203(17)30021-3/sbref5)11) (2011) 2555[–](http://refhub.elsevier.com/S0031-3203(17)30021-3/sbref5)2564.
4. P. Das, K. Karthik, B.C. Garai, A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs, Pattern Recognit. 45 (9) (2012) 3373–3388.
5. W. Yang, J. Hu, S. Wang, J. Yang, Cancelable Fingerprint Templates with Delaunay Triangle- based Local Structures, Cyberspace Safety and Security, Lecture Notes in Computer Science, 8300, 2013 pp. 81–91.
6. Quan, Feng, et al. "Cracking cancelable fingerprint template of Ratha." Computer Science and Computational Technology, 2008. ISCSCT'08. International Symposium on. Vol. 2. IEEE, 2008.
7. FVC2004, 2004. Available from[: http://bias.csr.unibo.it/fvc2004/databases.asp](http://bias.csr.unibo.it/fvc2004/databases.asp)
8. S. Chikkerur, N. Ratha, J. Connell, R. Bolle, "Generating registration-free cancelable fingerprint templates", *Proc. IEEE Int. Conf. Biometrics: Theory Applications and Systems*, pp. 1-6.
9. N. Ratha, S. Chikkerur, J. Connell, R. Bolle, "Generating cancelable fingerprint templates", *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561-572, Apr. 2007.
10. N. Ratha, S. Chikkerur, J. Connell, R. Bolle, "Generating cancelable fingerprint templates", *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561-572, Apr. 2015.