Major Project Report
on

ALTERNATIVE "IS ALIVE" BASED APPROACH FOR ALTERED FINGERPRINT IDENTIFICATION

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS
FOR THE AWARD OF DEGREE

of

MASTER OF ENGINEERING
(Computer Technology and Applications)
Delhi University, Delhi

Submitted By:
SAVITA SHARMA
University Roll No 8834
University Enrol No DP-790/07

Under the Guidance of:

Dr. S. K. Saxena
Senior Faculty
Department Of Computer Engineering
Delhi College of Engineering, Delhi

DEPARTMENT OF COMPUTER ENGINEERING
DELHI COLLEGE OF ENGINEERING
DELHI UNIVERSITY

2010

CERTIFICATE

This is certified that the major project report titled **"*Alternative "Is-Alive" based approach for altered fingerprint identification*"**, is the work of Savita Sharma (University Roll No. 8834), a student of Delhi College of Engineering. This work was completed under my direct supervision and guidance and forms a part of the Master of Engineering (Computer Technology and Applications) course and curriculum.

(Dr. S. K. Saxena)
Project Guide
Department of Computer Engineering
Delhi College of Engineering, Delhi – 110042

ACKNOWLEDGEMENT

No volume of words is enough to express my gratitude towards my guide **Dr. S. K. Saxena**, Senior Faculty, Computer Science and Engineering, Delhi College of Engineering, Delhi, who has been very concerned and has aided for all the materials essential for the preparation of this thesis report. He has helped me to explore this vast topic in an organized manner and provided me with all the ideas on how to work towards a research-oriented venture.

I am also thankful to **Dr. (Mrs) Daya Gupta**, Head of the Department, Computer Science and Engineering, Delhi College of Engineering, Delhi for the motivation and inspiration that triggered me for the thesis work.

I would also like to thank the staff members and my colleagues who were always there at the need of the hour and provided with all the help and facilities, which I required for the completion of my thesis work.

This is certified that the work submitted in this major project has not been submitted anywhere else in part or full.

I am very much grateful to my family for their valuable support and inspiration that helped in conceptualizing the thesis.

(Savita Sharma)
M.E. (Computer Technology and Application)
Department of Computer Engineering
Delhi College of Engineering, Delhi – 110042

ABSTRACT

Fingerprint recognition for unique identification suffers from a disadvantage of being easy to imitate when compared to other forms of biometric authentications where surgical procedure is necessary. Different material can be used to mould and reproduce exact copy of a fingerprint with its detailed shape and extended characteristics (e.g. minutiae point locations). Recent research in this field shows the lack of aliveness detection mechanism in fingerprint sensors technology. Security issues with authentication device are a major concern in many applications. This work proposes the use of heartbeat as means of “is-alive” detection along with minutiae based fingerprint recognition to overcome the above stated challenges.

Keywords – Multi-modal biometrics, fingerprint identification, heartbeat detection, fake fingerprint identification, altered fingerprint identification, is-alive detection, liveness detection, minutiae based recognition, ridge based recognition, correlation based recognition

TABLE OF CONTENTS

TABLE OF FIGURES

CHAPTER 1 - INTRODUCTION

Today fingerprint recognition[1], as a means of unique identification, finds a widespread usage for individual as well as enterprise needs than any other form of biometric identification. Though, being the most effective means of identification, fingerprint recognition suffers from a disadvantage of being comparatively easy and fast to imitate as compared to other forms of biometric authentications where surgical procedure is necessary. Also, the performance of such recognition is dependent upon the fingertip surface condition that again is affected by the environmental context or personal cause of usage (e.g. wet, dry, scarred, and oriented). This can result in fake fingerprints[2] and altered fingerprints[3] being sometimes considered the same. Though, a considerable research there has been a done in the topic of fingerprints identification, the altered fingerprints have not been studied to that level of detail.

Considering the criticality and widespread use of fingerprint identification, it is required that automatic detection of fake and altered fingerprints is extremely fast with limited human intervention. This research proposes a new multi-modal biometric technique to identify altered fingerprints which employs detection of life mechanism i.e. by detecting a heartbeat in the finger being used. The scope of the research is limited to online authentication only (where user is involved in the authentication process) as opposed to offline authentication (for e.g. at a crime scene where the event has already happened). The research also showcases a simulation scenario for fingerprint identification using the heart beat detection mechanism modeled using MATLAB software.

[1] Fingerprint recognition refers to the automated method of verifying a match between two human fingerprints.

[2] Fake finger is another person’s identity. Fake fingers are made of latex or silicone and known to everyone

[3] Altered fingerprints are real fingers that are used to hide one’s identity. Altered fingers are used to mask one’s own identity. Alteration of fingerprints can be done by many techniques like cutting, burning, plastic surgery and abrading

CHAPTER 2 - LITERATURE REVIEW

Biometric Recognition

Biometric recognition (or simply biometrics) refers to the use of distinctive anatomical (e.g. fingerprints, face, iris) and behavioral (e.g. speech) characteristics called biometric identifiers or traits for automatically recognizing individuals.

Biometrics is becoming an essential component of effective person identification solutions because biometric identifiers cannot be shared or misplaced and they intrinsically represent the individual’s bodily identity. All biometric identifiers are a combination of anatomical and behavioral characteristics. For e.g. finger prints are anatomical in nature but the usage of the input device (i.e. how a user presents a finger to the fingerprint scanner) depends on persons behavior.

Criteria classify a characteristic as a biometric identifier

Any human anatomical or behavioral characteristic can be used a biometric identifier to recognize a person as long as it satisfies the following requirements.

- Characteristic should be **universal** i.e. each person should possess the biometric characteristic
- Characteristic should be **distinct** i.e. any two persons should be sufficiently different in terms of their respective biometric characteristics
- Characteristic should be **permanent** i.e. biometric characteristic should not vary over time (with respect to matching criteria)
- Characteristic should be **collectable** i.e. it should be possible to quantitatively measure the biometric characteristic

Commonly used Biometric Identifiers

- **Retina -** Retinal recognition creates an "eye signature" from the vascular configuration of the retina which is supposed to be a characteristic of each individual and each eye, respectively
- **Iris** – Refers to the use of irides of an individual's eyes as a biometric identifier. The iris begins to form in the third month of gestation and the structures creating its pattern are largely complete by the eight month. Its complex pattern can contain many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles and a zigzag collarette. Iris scanning is less intrusive than retinal because the iris is easily visible from several meters away
- **Face** – Face is one of the most acceptable and non-intrusive biometric characteristic. However, face recognition suffers for challenges of tolerating the effects of aging, facial expressions, variations in imaging environment and facial pose with respect to the camera
- **DNA** - Deoxyribonucleic acid (DNA), one-dimensional code unique for each person, is considered to be the most reliable biometrics. This method, however, suffers from some drawbacks like 1) contamination and sensitivity, since it is easy to steal DNA from an individual, 2) no real-time application is possible because DNA matching requires complex chemical methods, 3) privacy issues
- **Hand and finger geometry** – Hand features (e.g. length of fingers) relatively do not vary over time and are atypical to an individual. However, due to limited distinctiveness, hand geometry based systems are only used for verification and not for identification
- **Infrared thermogram** (facial, hand or hand vein) - The pattern of heat radiated by the human body is also considered to be unique for each person. An infrared camera can be used to capture the heat radiations; however, the image acquisition is rather difficult where there are other heat emanating surfaces near the body
- **Voice** – Voice capture is one of simple and unobtrusive means of recognition but is affected by factors such as person’s heath, stress and emotional state

- **Ear** - The shape of the ear and the structure of the cartilaginous tissue of the pinna are considered to be distinctive. Matching the distance of salient points on the pinna from a landmark location of the ear is the suggested method of recognition in this case. Though, this method is not believed to be very distinctive
- **Signature** – Person’s signature (or the way of writing) is also considered to be a characteristic of that individual and has been employed a method of verification since a long time. Signatures, however, changes over time and is influenced by physical and emotional conditions

Though a biometric characteristic may provide an effective authentication mechanism, there could however be the limitations in using any single biometric characteristic:

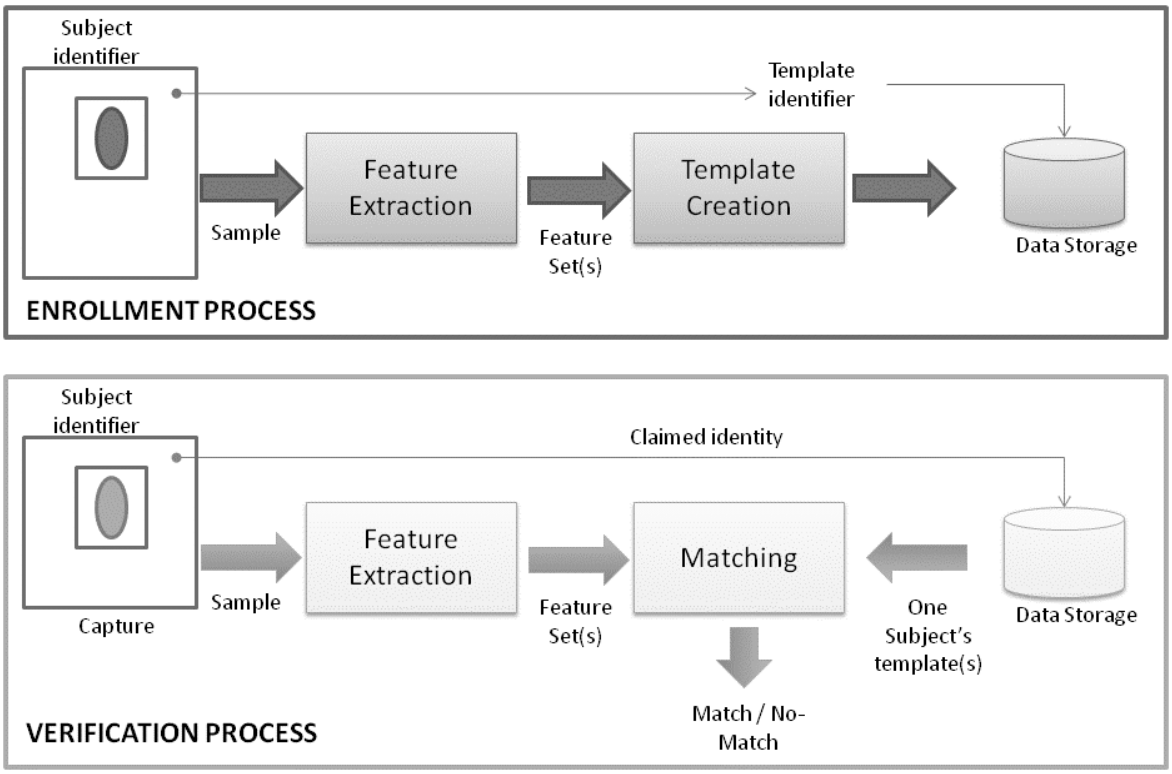
- **Noise in sensed data**. For e.g. fingerprint / face with scars
- **Intra-class variation** i.e. the data acquired from an individual during authentication may be different from the data that was used to generate the template during enrollment
- **Distinctiveness** - While a biometric characteristic is expected to vary significantly across individuals, there may be large inter-class similarities in the feature sets used to represent these characteristic
- **Non-universality** - in reality a group of users may not posses that particular biometric characteristic
- **Spoof attacks** - An individual may attempt to forge the biometric characteristic

A multi-modal biometric system can be a prospective solution to overcome these limitations. Multi-modal biometric systems integrate two or more type of biometric recognition and verification systems. This research proposes the integration of heart beat recognition for “is-alive” check with fingerprint recognition to increase its reliability.

Implementing a Biometric Recognition System

A critical consideration in the design of a practical biometric system is to determine how an individual would be recognized. Depending upon the context, a biometric system may either be used for verification (also known as authentication) or identification of an individual.

- A **verification system / authentication system** authenticates an individual’s identity by comparing the captured biometric characteristic with his/her previously captured reference template in the system. The systems performs a one-on-one comparison for confirming the claim of identity
- An **identification system** recognizes an individual by searching the entire enrollment template database for a match. It conducts one-to-many comparisons to establish individual’s presence in the database and if present, returns the identifier of the matched reference. Essentially, an identification system establishes individual’s identity without the subject having to claim his/her identity



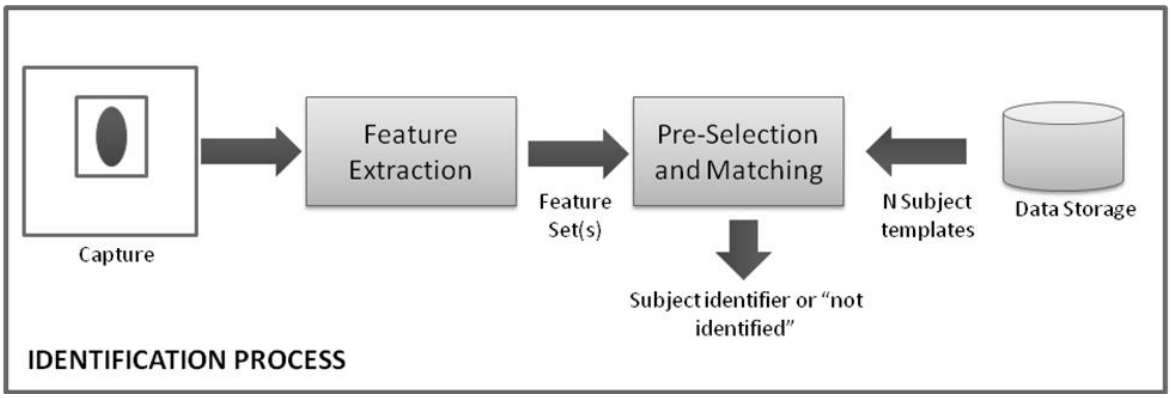


Figure 1, Enrollment, verification and identification process

The enrollment, verification and identification process involved in user recognition use the following system modules.

- **Capture** – Senses and captures the digital representation of the biometric characteristic
- **Feature extraction** – Processes the raw digital representation of the biometric characteristic to generate a compact but expressive representation, called a feature set
- **Template creation** – Organizes one or more feature sets into a template that can be saved in a persistent storage. The template is sometimes also referred to as a reference.
- **Pre-selection and matching** – is used when a biometric characteristic needs to be compared with a large number of enrolled templates. Pre-selection and matching optimizes the identification procedure by reducing the effective size of the template database so that the input can be matched to a relatively small number of templates
- **Data storage** – stores templates and other demographic information about the user

Using these five modules, three main processes can be performed namely enrollment, verification and identification. A verification system uses the enrollment and verification process while an identification system uses the enrollment and identification process.
In a practical biometric system, key issues that need to be considered are:

- **Performance** – Recognition accuracy, speed, resource requirements and robustness to operational and environmental factors
- **Acceptability** – Extent to which users are willing to accept biometric identifier in their daily lives
- **Circumvention** – Ease with which the biometric system can be evaded by fraudulent methods

Comparison of commonly used biometric characteristics

Biometric Identification	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Retina	H	H	M	L	H	L	L
Iris	H	H	H	M	H	L	L
Face	H	L	M	H	L	H	H
DNA	H	H	H	L	H	L	L
Fingerprint	M	H	H	M	H	M	M
Hand Geometry	M	M	M	H	M	M	M
Facial Thermogram	H	H	L	H	M	H	L
Hand vein	M	M	M	M	M	M	L
Voice	M	L	L	M	L	H	H
Ear	M	M	H	M	M	H	M
Signature	L	L	L	H	L	H	H

Table 1, Comparison of commonly used biometric characteristics H – High, M – Medium, L – Low

The above table shows that fingerprint as a biometric characteristic represents a balance amongst all other approaches.

Human fingerprint for Biometric identification

A human fingerprint is an impression pattern left on any hard smooth surface by the ridged dermis (skin) (called friction ridges) of the fingertip. The fundamentals of fingerprint identification are permanence and individuality.

A human fingerprint consists of ridges and valley on your skin. On a fingerprint, the ridges appear as dark lines, the valleys as space between the ridges. Each fingerprint contains a number of unique physical characteristics called minutiae, which includes certain visible aspects of a fingerprint such as ridges, ridge endings and bifurcations (forks in ridges). Minutiae are generally found in the core points of fingerprints, located near the center of the fingertips. These characteristics are used to distinguish two fingerprints, or to state that they are the same. For e.g. even identical twins have different fingerprints.

The fingerprints are used for identification purposes because:

1. Ridge patterns and the details in small areas of friction ridges are unique and never repeated. Typical fingerprint has 35-50 identification points (minutiae) and the odds of two being alike are 1 in 64 billion
2. Friction ridges develop on the fetus in their definitive form before birth
3. Ridges are persistent throughout life except for permanent scarring
4. Friction ridge patterns vary within limits which allow for classification

Classification of Fingerprints

A closer examination of fingerprints reveals some very common, somewhat common, or somewhat rare patterns.

Loops are very common patterns in fingerprints – about 65% of all fingerprints are loops. Somewhat common patterns are Whorls – about 29% of all fingerprints are whorls. Somewhat rare patterns are Arches – only about 6% of all fingerprints are arches.

Figure 2, Right Loop

Figure 3, Left Loop

Figure 4, Double loop

Figure 5, Whorls

Figure 6, Arch

Figure 7, Tented Arch

Fingerprint Recognition

Fingerprint recognition refers to the automated means of verifying a match between two human fingerprints. There are two generally recognized classes or categories for finger print recognition:

- **Minutiae-based approach** - This approach is based on identifying characteristics of the prints that are less obvious than the more pronounced traits. Minutiae are extracted from the two fingerprints and stored as sets of points in the two-dimensional plane. Minutiae-based matching essentially consists of finding the

alignment between the template and the input minutiae sets that results in the maximum number of minutiae pairings

- **Non-minutiae feature-based approach** – Minutiae extraction is extremely difficult in a low-quality fingerprint images, whereas other features of fingerprint ridge pattern may be extracted more reliably than minutiae, even though their distinctiveness is generally lower. The approaches belonging to this family compare fingerprints in term of features extracted from the ridge pattern
- **Correlation-based Approach** - This approach relies on not only the identifying characteristics of the print patterns, but also the positioning of those traits within the pattern. This involves the establishment of what are known as registration points along the body of the print, effectively providing a point of reference for the comparison process. Two fingerprint images are superimposed and the correlation between corresponding pixels is computed for different alignments (e.g., various displacements and rotations)

Minutiae-based Approach for Fingerprint recognition

A fingerprint contains a number of unique physical characteristics called minutiae, which includes certain visible aspects of fingerprints such as ridges, ridge endings and bifurcations (forks in ridges). Minutiae are generally found in the core points of fingerprints, located near the center of the fingertips.

Typically, minutiae-based representations rely on locations of the minutiae and the directions of ridges at the minutiae location. Fingerprint classification identifies the typical global representations of fingerprints. Some global representations include information about locations of critical points (e.g., core and delta) in a fingerprint.

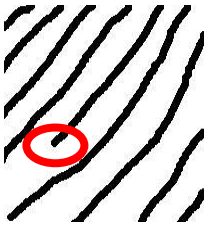


Figure 8, Ridge ending

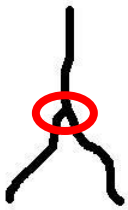


Figure 9, Ridge bifurcation

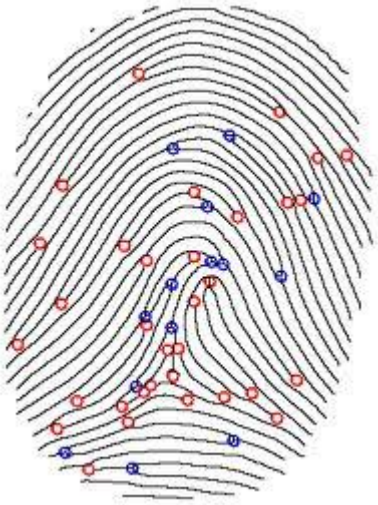


Figure 10, Fingerprint image with different minutiae points marked

Reasons to use minutiae based representations are:

I. Minutiae capture much of the individual information
II. Minutiae-based representations are storage efficient, and
III. Minutiae detection is relatively robust to various sources of fingerprint degradation
IV. Minutiae templates are a fraction of the size of fingerprint images and require less storage memory and can be transmitted electronically faster than images

While minutiae based methods of fingerprint matching are effective, it has a drawback that the quality of the prints must be quite high in order to verify a match. The extracted minutiae templates contain a number of false minutiae, while some minutiae’s can be missed as well, especially in the case of bad quality fingerprints.

Minutiae-based fingerprint systems use a large number of successive processing steps. In general, the following steps can be identified:

- Directional field estimation
- Adaptive filtering for noise reduction
- Threshold-ing to obtain a binary fingerprint image
- Morphological operations like thinning to obtain ridges that are only one pixel wide
- Minutiae extraction from the thinned image
- Application of heuristics to reduce the number of false minutiae
- Registration of minutiae templates by Hough transform
- Matching score computation

Let T and I be the representation of the template and input fingerprint, respectively. Each minutia may be described by number of attributes like:

1. Location in the fingerprint image
2. Orientation
3. Type (e.g. ridge termination or ridge bifurcation)
4. Weight based on the quality of the fingerprint image in the neighborhood of the minutiae

However, most common minutiae matching algorithms consider each minutia as a triplet m = {x, y, Θ} that indicates the x, y minutia location coordinates and the minutia angle Θ:

$\mathbf{T} = \{\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_m\}$, $\mathbf{m}_i = \{x_i, y_i, \Theta_i\}$, i = 1…m

$\mathbf{I} = \{\mathbf{m}'_1, \mathbf{m}'_2, \ldots, \mathbf{m}'_n\}$, $\mathbf{m}'_j = \{x'_j, y'_j, \Theta'_j\}$, j = 1…n

Where, m and n denote the number of minutiae in T and I, respectively.

A minutia $\mathbf{m}'_j$ in **I** and a minutia $\mathbf{m}_i$ in **T** are considered "matching," if the spatial distance (sd) between them is smaller than a given tolerance r_0 and the direction difference (dd) between them is smaller than an angular tolerance Θ_0.

$sd(\mathbf{m}'_j, \mathbf{m}_i) = \text{sqrt}\,(x'_j - x_i)^2 + (y'_j - y_i)^2 \le r_0$ and (1)

$dd(\mathbf{m}'_j, \mathbf{m}_i) = \min(|\Theta'_j - \Theta_i|, 360^0 - |\Theta'_j - \Theta_i|) \le \Theta_0$ (2)

R_0 and Θ_0 are necessary to compensate for errors in feature extraction algorithms and to account for small plastic deformations that can cause minutiae position to change.

Aligning the two fingerprints is a mandatory step in order to maximize the number of matching minutiae. Correctly aligning two fingerprints certainly requires displacement (in x and y) and rotation (Θ) to be recovered and likely involves other geometrical transformations like scale resolution and other kinds of distortion.

Let map(.) be the function that maps a minutia $\mathbf{m}'_j$ (from I) into $\mathbf{m}''_j$ according to a given geometrical transformation; for example, by considering a displacement of [Δx, Δy] and a counterclockwise rotation Θ around the origin[4].

$\text{map}_{\Delta x,\Delta y,\Theta}(\mathbf{m}'_j = \{x'_j, y'_j, \Theta'_j\}) = \mathbf{m}''_j = \{x''_j, y''_j, \Theta''_j + \Theta\}$, where

$$\begin{pmatrix} x''_j \\ y''_j \end{pmatrix} = \begin{pmatrix} \cos\Theta & -\sin\Theta \\ \sin\Theta & \cos\Theta \end{pmatrix} \begin{pmatrix} x'_j \\ y'_j \end{pmatrix} + \begin{pmatrix} \Delta x \\ \Delta y \end{pmatrix}$$

Let mm(.) be an indicator function that returns 1 in the case where the minutiae $\mathbf{m}''_j$ and $\mathbf{m}_i$, match according to (1) and (2).

$$mm(\mathbf{m}''_j, \mathbf{m}_i) = \begin{cases} 1 & sd(\mathbf{m}''_j, \mathbf{m}_i) \le r_0 \text{ and } dd(\mathbf{m}''_j, \mathbf{m}_i) \le \Theta_0 \\ 0 & \text{otherwise} \end{cases}$$

Then, the matching problem can be formulated as

[4] The origin is usually selected as the minutiae centroid (i.e. average point); before the matching step, minutiae coordinates are adjusted by subtracting the centroid coordinates.

$$\underset{\Delta x,\ \Delta y,\ \Theta,P}{\text{maximize}} \quad \sum_{i=1}^{m} mm(map_{\Delta x,\Delta y,\Theta}(\mathbf{m'}_{P(i)}),\mathbf{m}_i), \qquad (3)$$

where P(i) is an unknown function that determines the pairing between I and T minutiae; in particular, each minutia has either exactly one mate in the other fingerprint or has no mate at all:

1. P(i) = j indicates that the mate of the $\mathbf{m}_i$ in T is the minutia $\mathbf{m}'_j$ in I;
2. P(i) = null indicates that minutia $\mathbf{m}_i$ in T has no mate in I;
3. a minutia $\mathbf{m}'_j$ in I, such that for all i = 1..m, P(i) ≠ j has no mate in T;
4. for all i = 1..m, k = 1..m, i ≠ k => P(i) ≠ P(k) or P(i) = P(k) = null (this requires that each minutia in I is associated with a maximum of one minutia in T).

Equation (3) requires that the number of minutiae mates be maximized, independently of how strict these mates are; in other words, if two minutiae comply with Equations (1) and (2), then their contribution to equation (3) is made independently of their spatial distance and of their direction difference.

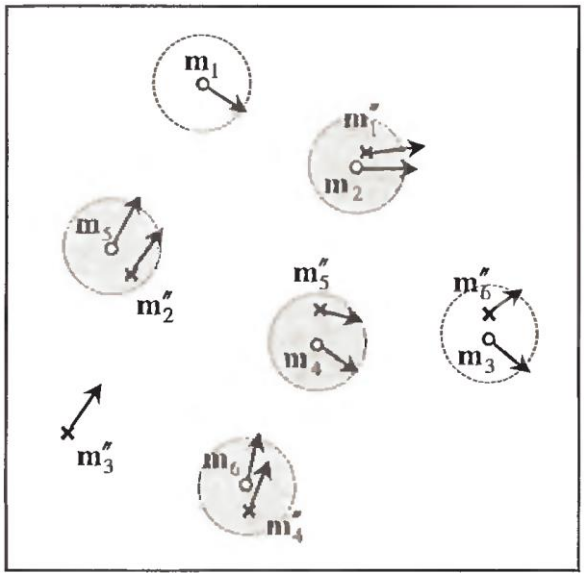


Figure 11, Minutiae of I mapped into T coordinates for a given alignment

Also, to comply with constraint 4 above, each minutia **m**"$_j$ already mated has to be marked, to avoid mating it twice or more.

To achieve the optimum pairing (according to Equation 3), a slightly more complicated scheme should be adopted i.e. in the case when a minutia of I falls within the tolerance hyper-sphere of more than one minutia of T, the optimum assignment is that which maximizes the number of mates.

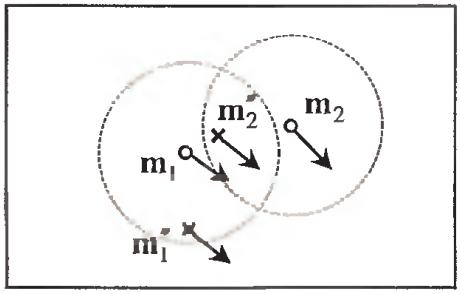


Figure 12, If m_1 were mated with m”$_2$ (closest minutiae), m_2 would remain unmated, however, pairing m_1 with m”$_1$, allows m_2 to be mated with m”$_2$, thus maximizing equation (3)

Solving the minutiae matching problem (equation 3) is trivial when the correct alignment (Δx,Δy,Θ) is known; in fact, the pairing (i.e., the function P) can be determined by setting for each i = 1..m:

- P(i) = j if **m**”j = map (**m**’j) is closest to mi among the minutiae {**m**”$_k$ = map$_{\Delta x,\Delta y,\Theta}$(**m**’$_k$) | k = 1..n, mm(**m**”$_k$,**m**$_i$) = 1};
- P(i) = null if k = 1..n, mm(map$_{\Delta x,\Delta y,\Theta}$(**m**’$_k$), **m**$_i$) = 0

Also, the maximization in equation (3) can be easily solved if the function P (minutiae correspondence) is known; in this case, the unknown alignment (Δx, Δy, Θ) can be determined in the least square sense (Umeyana(1991) and Chang et al. (1997)).

However in practice both the function P and correct alignment (Δx, Δy, Θ) is not known which makes the matching problem hard because of its exponential nature. Hence the minutiae matching problem has been generally addressed as a point pattern matching problem which can be solved using numerous approaches like relaxation methods, algebraic and operational research solutions, tree-pruning approaches, energy-minimization methods, Hough transform, and so on.

An approach to point pattern matching, as proposed by Chang et al. (1997) consists of the main steps:

1. Detect the minutiae pair (called the principal pair) that receives the maximum Matching Pair Support (MPS) and the alignment parameters (Θ, s) that can match most minutiae between T and I. The principal pair that has maximum MPS is determined through a Hough transform-based voting process
2. The remaining minutiae mates (i.e., the function P) are then determined once the two fingerprints have been registered to superimpose the minutiae constituting the principal pair
3. The exact alignment is computed in the least square sense once the correspondence function is known

To accomplish Step 1, which is at the core of this approach, the algorithm considers segments defined by pairs of minutiae $\mathbf{m}_{i2}\mathbf{m}_{i1}$ in T and $\mathbf{m}'_{j2}\mathbf{m}'_{j1}$ in I and derives, from each pair of segments, the parameters ‘Θ’ and ‘s’ simply as

$$\Theta = angle(\overline{\mathbf{m}_{i2}\mathbf{m}_{i1}}) - angle(\overline{\mathbf{m}'_{j2}\mathbf{m}'_{j1}}), \quad (4)$$

$$s = \frac{length(\overline{\mathbf{m}_{i2}\mathbf{m}_{i1}})}{length(\overline{\mathbf{m}'_{j2}\mathbf{m}'_{j1}})} \quad (5)$$

A transformation (Δx, Δy, Θ, s), which aligns the two segments, must necessarily involve a scale change by an amount given by the ratio of the two segment lengths, and a rotation by an angle equal to the difference between the two segment angles

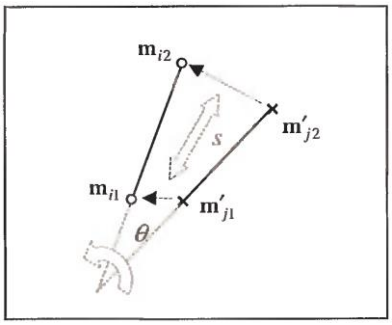


Figure 13, Transformation that aligns the two segments involves a rotation and a scale changes as defined by equations (4) and (5)

The principal pair and the parameters (Θ*, s*) are determined as

maxMPS = 0 //maximum matching pair support

for each $\mathbf{m}_{i1}$, i1 = 1..m

for each $\mathbf{m}'_{j1}$, j1 = 1..n //m_{i1}, m'_{j1} is the current pair for which MPS has to be estimated

{ Reset **A** //the accumulator array

for each $\mathbf{m}_{i2}$, i2 = 1..m, i2 ≠ i1

for each $\mathbf{m}'_{j2}$, j2 = 1..n, j2 ≠ j1

{Θ,s are computed from $\overline{\mathbf{m}_{i2}\mathbf{m}_{i1}}$, $\overline{\mathbf{m}'_{j2}\mathbf{m}'_{j1}}$ according to equations (4) and (5)

Θ^+,s^+ = quantization of Θ,s to the nearest bins

$A[\Theta^+,s^+]$ - $A[\Theta^+,s^+]$ + 1

}

$MPS = \max_{\Theta+,s+} A[\Theta^+,s^+]$

if MPS ≥ maxMPS

{ maxMPS = MPS

$(\Theta^*,s^*) = \arg\max_{\Theta+,s+} A[\Theta^+,s^+]$

Principal pair = ($\mathbf{m}_{i1}$, $\mathbf{m}'_{ji}$)

}

}

Using the above algorithm we get the principal pair and the corresponding parameters (Ɵ*, s*). Thereafter we perform step 2 and 3 to find the rest matching pairs and their alignments. Thus at the end of step 3 we get the max number of matching pairs of minutiae which helps in matching the 2 fingerprints.

Figure 14, Minutiae matching by the Chang et al. (1997) approach.

Figures a) and b) show the minutiae extracted from the template and the input fingerprint respectively; c) the minutiae are coarsely superimposed and the principal pair is marked with an ellipse; d) each circle denotes a pair of minutiae as mated by the algorithm

This is the essence of a fingerprint matching algorithm. Various other techniques are additionally used to efficiently solve and improve results of the matching problem like minutiae matching with pre-alignment, Global and local minutiae matching, distortion corrections etc.

Non-minutiae Feature-based Approach

Also called as Ridge-feature based approach, the approaches belonging to this category compare fingerprints for features extracted from the ridge pattern. Approaches followed under this category resulted from the disadvantages of minutiae-based methods as listed below:

- Extracting minutiae reliably from poor quality fingerprints is very difficult
- Minutiae extraction is computationally expensive and time consuming
- Need to increased system accuracy and robustness – by use of additional features to be in conjunction with minutiae (and not as an alternative)

The more commonly used alternatives features are:

- **Spatial relationship and geometrical attributes of the ridge lines** - Moayer and Fu introduced tree grammars to classify ridge line patterns after they are binarized and thinned. Isenor and Zaky introduced graph structures to perform incremental graph matching which was carried out to compare a set of ridges
- **Global and local texture information** - Textures are defined by spatial repetition of basic elements, and are characterized by properties such as scale, orientation, frequency, symmetry, isotropy, and so on. Fingerprint ridge lines are mainly described by smooth ridge orientation and frequency, except at singular regions. These singular regions are discontinuities in a basically regular pattern and include the loop(s) and the delta(s) at a coarse resolution and the minutiae points at a high resolution. Various techniques using filters are applied to extract both global and local textures

- **Shape features** - Ceguerra and Koprinska in 2002 proposed shape-based features where a compact one-dimensional shape signature that encodes the general shape of the fingerprint is generated from the two-dimensional fingerprint image using a reference axis. Shape based matching is then used together with minutiae based matching to make a final matching decision

Correlation-based Approach for Fingerprint recognition

Correlation-based fingerprint matching spatially correlates the fingerprint images (input and template) to estimate the degree of similarity between them. It uses the gray-level information from the fingerprint image since the gray level values of the pixels around a minutia point retain most of the information, spatial correlation provides an accurate measure of the similarity between minutia regions. These locations only characterize a small part of the local ridge-valley structures.

However, if the rotation and displacement of the input image with respect to the template are not known, then the correlation must be computed over all possible rotations and displacements, which is computationally very expensive. Further, the presence of non-linear distortion and noise significantly reduces the global correlation value between two impressions of the same finger. To overcome these problems, correlation is usually done locally only in certain “interesting” regions (regions of high curvature, minutia information regions, etc.) of the fingerprint image.

The effectiveness of the correlation-based approach depends on the ability to establish a common registration point on the two sets of prints under comparison, and compensate for any differences in the rotation or image quality of the prints.

Let T and I be the two fingerprint images corresponding to the template and the input fingerprint, respectively. An intuitive measure of their diversity is the sum of squared differences (SSD) between the intensities of the corresponding pixels:

$$SSD(T,I) = ||T - I||^2 = (T - I)^T(T - I) = ||T||^2 + |||I||^2 - 2T^TI, \quad (1)$$

Where, the superscript "T" denotes the transpose of a vector. If the terms $||T||^2$ and $||I||^2$ are constant, the diversity between the two images is minimized when the cross-correlation (CC) between T and I is maximized:

$$CC(T,I) = T^T I \quad (2)$$

Note that CC(T,I) appears as the third term in Equation 1. The cross-correlation is then a measure of image similarity. Due to the displacement and rotation that unavoidably characterize two impressions of a given finger, their similarity cannot be simply computed by superimposing T and I and applying Equation 2.

Let $I^{(\Delta x, \Delta y, \Theta)}$ represent a rotation of the input image I by an angle Θ around the origin (usually the image center) and shifted by Δx, Δy pixels in directions x and y, respectively; then the similarity between the two fingerprint images T and I can be measured as:

$$S(T,I) = \max_{\Delta x, \Delta y, \Theta} CC(T, I^{(\Delta x, \Delta y, \Theta)}) \quad (3)$$

However equation 3 rarely leads to acceptable results because of the following problems.

1. Non-linear distortion makes impressions of the same finger significantly different in terms of global structure; in particular, the elastic distortion does not significantly alter the fingerprint pattern locally, but since the effects of distortion get integrated in image space, two global fingerprint patterns cannot be reliably correlated. The fingerprint distortion problem can be addressed by computing the correlation locally instead of globally
2. Skin condition and finger pressure cause image brightness, contrast, and ridge thickness to vary significantly across different impressions

3. A direct application of Equation 3 is computationally very expensive. For example, consider two 400 x 400 pixel images; then the computation of the cross-correlation (Equation 2) for a single value of the (Δx, Δy, Θ) triplet would require 16,000 multiplications and 16,000 summations. Though the computational complexity can be simplified using smart approaches to achieve efficient implementations. For e.g. maximum correlation need not be done in a sequential exhaustive manner

“is-Alive” Detection in Biometric systems

Securing of the automated and unsupervised fingerprint recognition systems used for authentication is one of the most critical and most challenging tasks in real word scenarios as it is prone to security threats such as repudiation, coercion, contamination and circumvention

A variety of methods can be used to get unauthorized access to a system based on automated fingerprint recognition. To discourage misuse by presenting a fake finger or, even worse, to force a legitimate user of the system to present his finger, or even to hurt a person to gain access, the system must be augmented by a liveness detection system. Hence, to prevent false acceptance we have to recognize whether the finger on the fingerprint sensor is alive or not. For the purposes of the liveness detection, one or more characteristic properties of the living human body can be used.

Human body offers a vast amount of various characteristic properties, but not all of them comply with foregoing requirements and not all of them can be used with the fingerprint technology. The properties usable for “is-alive” detection can be classified into three categories as listed below:

- **Intrinsic properties** - The intrinsic properties are based on characteristics of the living human tissue. For e.g. fingerprint technology can use properties of various skin layers or body fluids

- **Involuntarily generated signals** - Involuntarily generated signals are spontaneously and uncontrollably generated by a living human body. The best known involuntarily generated signal is a pulse
- **Responses to a stimulus** – Involves monitoring the response to a tactile stimulus given within the sensing area. For e.g. an increased temperature causes enlargement of peripheral blood vessels, which can be measured as increasing amplitude of the blood flow

In this research, we explore heart beat detection augmenting fingerprint matching for human identification. To ensure a comprehensive “is-alive” detection mechanism, two key requirements should be met:

1. “is-alive” detection and the fingerprint scan have to be performed at the same time
2. ”is-alive” detection itself must not influence the fingerprint scan and vice versa

Using human heartbeat for “is-alive” detection

Human heart has an electrical conduction system that stimulates it to contract or beat. Each beat begins as an electrical impulse that arises from a specialized area of the right atrium called the sinoatrial (SA) node. The SA node is the heart's natural pacemaker. It receives messages from the brain and other centers directing it to adjust the heart rate to meet the body's needs. The electrical events occurring in the human heart are powerful enough to be detected by electrodes on the body surface. A recording of these events is an ECG of the human heart.

Benefits of using the heart beat for “is-alive” detection are:

- The way the heart beats is unique & private feature of an individual. Even identical twins might have different and distinct electrical activities in their hearts
- The heart is hidden i.e. it is not possible to easily capture the characteristics of an individual’s heart without his/her consent
- The way the heart beat is not easily observed

- Heartbeat is an inherent “is-alive” biometric. The nature of the way the heart beats as a biometric proves the liveness of the user in a natural way
- Everybody has a heart. Unlike a fingerprint, some individuals might be disabled and have no hands and thus no fingerprints

Though heart beat can serve as an effective biometric identification tool, there are still certain areas that need to be considered:

- The way the heart beats can change if an individual suffers from a heart attack or an artificial pacemaker is installed
- To obtain a sufficient “noise free” electrical heart activity measurement the user must stay fairly still for 10 – 15 seconds
- An individual’s heart beats changes through time, thus the biometric system must provide a means way of adjusting / adding changes to the template in the database on a continuous basis

Electrocardiogram (ECG)

ECG is a method to measure and record different electrical potentials of the heart. The ECG may roughly be divided into the phases of depolarization and repolarization of the muscle fibers making up the heart. There are three waves to the ECG, each of which corresponds to a stage of the heart's contraction. These waves are called P, QRS, T and U waves respectively. In an ECG graph, electrical signals from the heart are presented as a graph of voltage against time. The baseline voltage of the electrocardiogram is known as the isoelectric line. Typically the isoelectric line is measured as the portion of the tracing following the T wave and preceding the next P wave

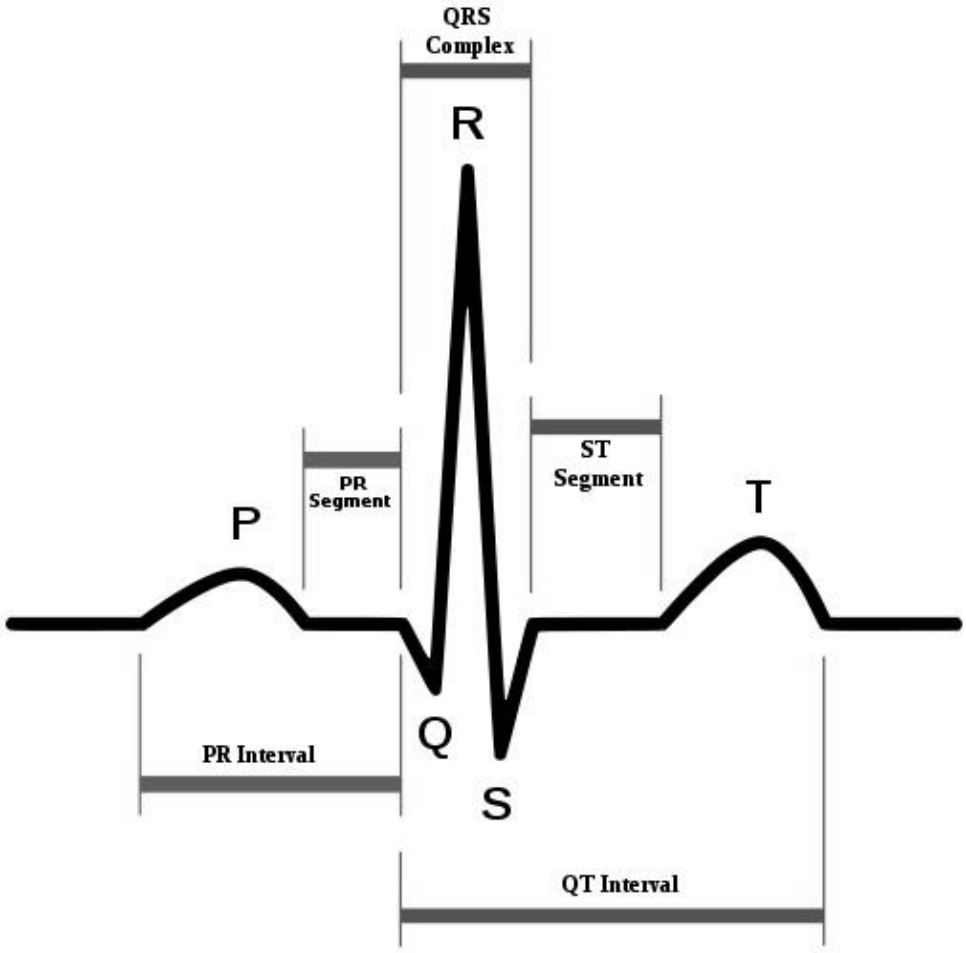


Figure 15, Elements of the ECG-complex

Feature	Description	Duration
RR interval	The interval between an R wave and the next R wave is the inverse of the heart rate. Normal resting heart rate is between 50 and 100 bpm	0.6 to 1.2s
P wave	During normal atrial depolarization, the main electrical vector is directed from the SA node towards the AV node, and spreads from the right atrium to the left atrium. This turns into the P wave on the ECG.	80ms
PR interval	The PR interval is measured from the beginning of the P wave to the beginning of the QRS complex. The PR interval reflects the time the electrical impulse takes to travel from the sinus	120 to 200ms

	node through the AV node and entering the ventricles. The PR interval is therefore a good estimate of AV node function.	
PR segment	The PR segment connects the P wave and the QRS complex. This coincides with the electrical conduction from the AV node to the bundle of His to the bundle branches and then to the Purkinje Fibers. This electrical activity does not produce a contraction directly and is merely traveling down towards the ventricles and this shows up flat on the ECG. The PR interval is more clinically relevant.	50 to 120ms
QRS complex	The QRS complex reflects the rapid depolarization of the right and left ventricles. They have a large muscle mass compared to the atria and so the QRS complex usually has much larger amplitude than the P-wave.	80 to 120ms
ST segment	The ST segment connects the QRS complex and the T wave. The ST segment represents the period when the ventricles are depolarized. It is isoelectric.	80 to 120ms
T wave	The T wave represents the repolarization (or recovery) of the ventricles. The interval from the beginning of the QRS complex to the apex of the T wave is referred to as the absolute refractory period. The last half of the T wave is referred to as the relative refractory period (or vulnerable period).	160ms
ST interval	The ST interval is measured from the J point to the end of the T wave.	320ms
QT interval	The QT interval is measured from the beginning of the QRS complex to the end of the T wave. A prolonged QT interval is a risk factor for ventricular tachyarrhythmias and sudden death. It varies with heart rate and for clinical relevance requires a correction for this, giving the QTc.	300 to 430ms
U wave	The U wave is not always seen. It is typically low amplitude, and, by definition, follows the T wave.	

Table 2, ECG Waves and Intervals

CHAPTER 3 - DESIGN AND ARCHITECTURE

The research proposes a minutia-based approach in conjunction with heartbeat detection mechanism for fingerprint matching and “is-alive” detection. The research simulates the fingerprint matching and “is-alive” detection using MATLAB software the design and architecture for which is presented later in this section. However, sensing the fingerprint image and heart beat signal requires a specialized hardware as well. The hardware design is currently not in scope for this research. Hence, acquisition stage is has been modeled via pre-existing templates. Similarly, for authentication purposes, a pre-existing database of templates has been defined for matching with the input image.

The architecture of a fingerprint identification system primarily is consisting of three components:

I. Graphical User interface
II. Authentication module
III. Template Database

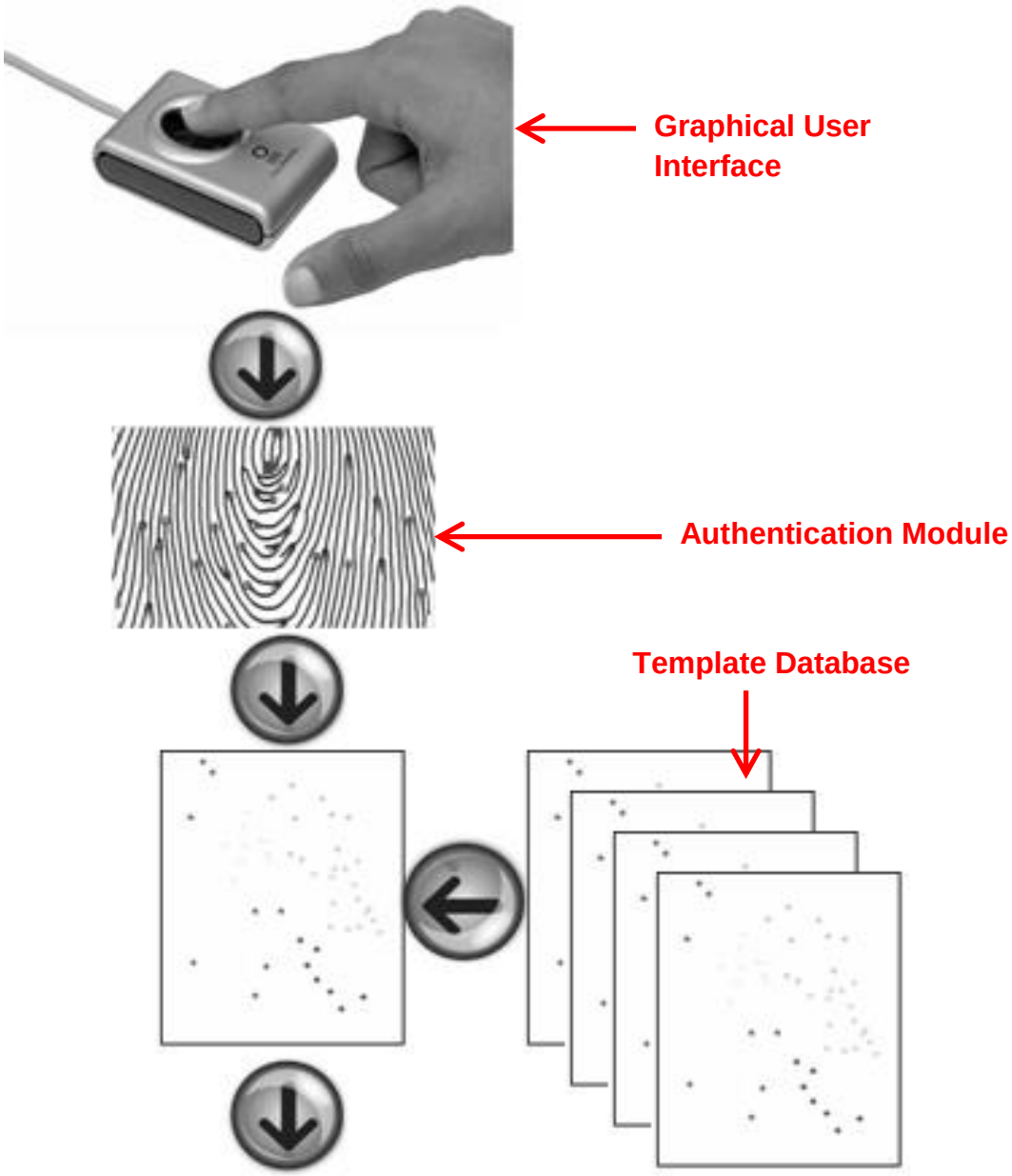


Figure 16, Architecture of the fingerprint recognition system and its working

Graphical User Interface

The user interface provides mechanisms for a user to input his fingerprints into the system. When the fingerprint images and the user ID of a person to be enrolled are fed to the user interface, a minutiae extraction algorithm is first applied to the fingerprint images and the minutiae patterns are extracted. A significant number (default value is

25) of genuine minutiae must be detected. If a fingerprint image is of poor quality, it can be enhanced to improve the clarity of ridge and mask out all the regions that cannot be reliably recovered. The enhanced fingerprint image is fed to the minutiae extractor again. For the research & simulation, high quality fingerprints have been used.

Refer to **Home GUI interface** section for details on the GUI.

Authentication module

The task of authentication module is to identify the person who intends to access the system. The person to be authenticated places his finger on the fingerprint scanner, a image of his fingerprint is taken, minutiae are extracted from the captured image and given to a matching algorithm which matches it with the person’s minutiae templates stored in the template database to authenticate the person. The problem when using biometric identification on the basis of fingerprints is that none of the fingerprint scanners can distinguish between a finger and a dummy. Here to overcome this, we check for the aliveness of fingerprint by adding one more biometric token with fingerprint e.g. heartbeat to identify person aliveness.

Template Database

The template database consists of a collection of records, each of which corresponds to an authorized person that has access to the system.

Each record contains the following fields which are used for authentication purpose:

I. User identifier
II. Minutiae templates of the person’s fingerprint
III. Other information can also be associated with the user templates (e.g., specific user privileges, various heart beat pattern records etc)

Flow Chart of Transformation operations

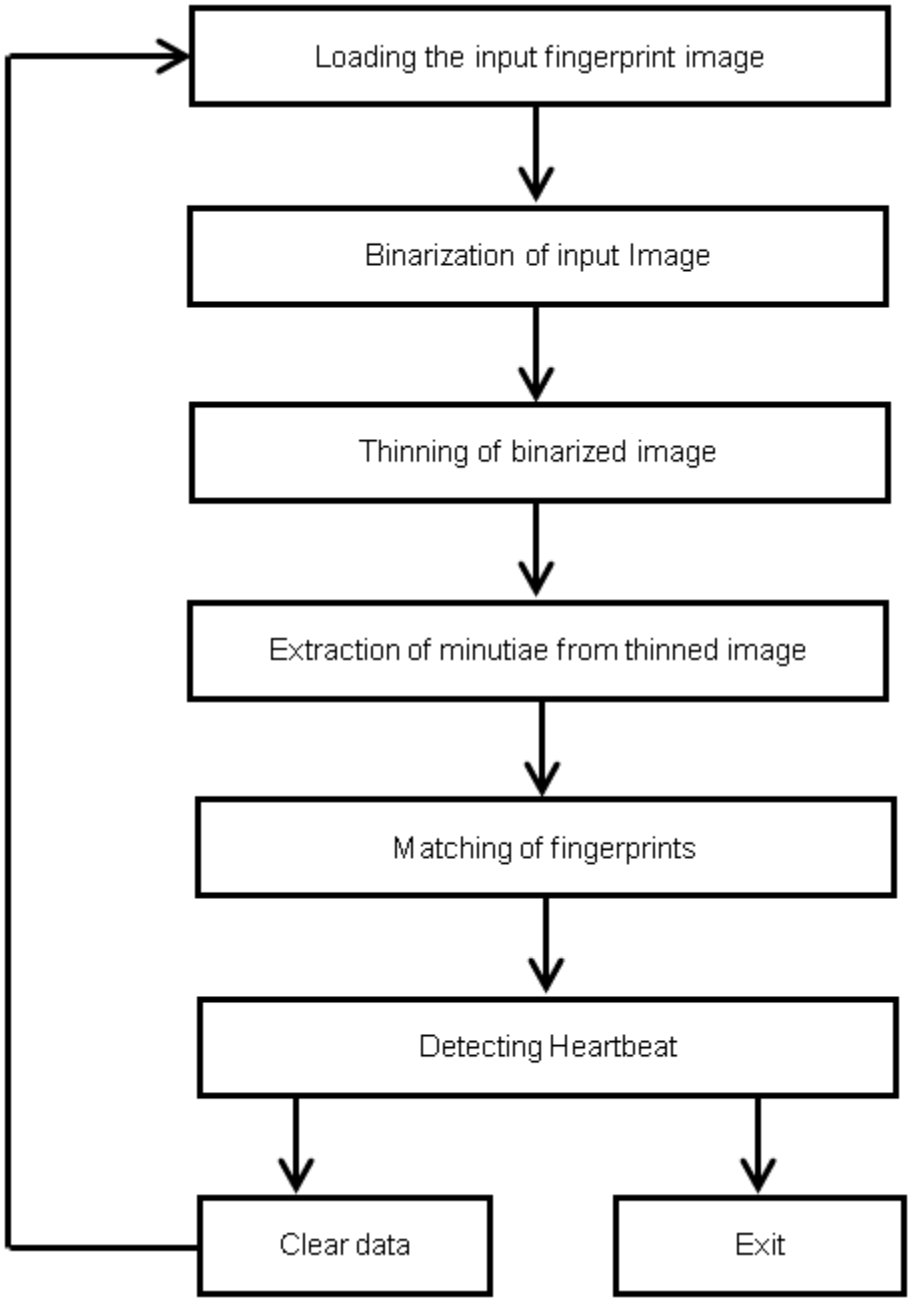


Figure 17, Flow chart of transformation operations

Binarization of Input image

Fingerprint binarization transforms the 8-bit gray image to a 1-bit image with 0-value for ridges and 1-value for furrows. Once the operation is done, ridges in the fingerprint are highlighted with black color while furrows are white.

Figure 18, Input fingerprint image

Figure 19, Fingerprint image after binarization

Fingerprint Ridge Thinning

Thinning eliminates the redundant pixels of ridges till the ridges are just one pixel wide. In each scan of the fingerprint image, redundant pixels in each small image window are marked down. And finally removes all those marked pixels after several scans.

Figure 20, Fingerprint image after thinning

Thinning operation uses the following algorithm:

1. Divide the image into two distinct subfields in a checkerboard pattern
2. In the first sub iteration, delete pixel p from the first subfield if and only if the conditions G_1, G_2, and G_3 are all satisfied
3. In the second sub iteration, delete pixel p from the second subfield if and only if the conditions G_1, G_2, and G_3' are all satisfied

Condition G1

$X_H(p) = 1$

Where,

$$X_H(p) = \sum_{i=1}^{4} b_i$$

$$b_i = \begin{cases} 1 & \text{if } x_{2i-1} = 0 \text{ and } (x_{2i} = 1 \text{ or } x_{2i+1} = 1) \\ 0 & \text{otherwise} \end{cases}$$

$x_1, x_2,\ldots,x_8$ are the values of the eight neighbors of p, starting with the east neighbor and numbered in counter-clockwise order.

Condition G2:

$2 \leq \min \{n_1(p), n_2(p)\} \leq 3$

Where,

$$n_1(p) = \sum_{k=1}^{4} x_{2k-1} \vee x_{2k}$$

$$n_2(p) = \sum_{k=1}^{4} x_{2k} \vee x_{2k+1}$$

Condition G3:

$(x_2 \vee x_3 \vee \bar{x}_8) \wedge x_1 = 0$

Condition G3’:

$(x_6 \vee x_7 \vee \bar{x}_4) \wedge x_5 = 0$

These two subiterations make-up one iteration of a thinning algorithm. The iterations are repeated until the image stops changing.

Minutiae Extraction and Matching

After fingerprint thinning, marking minutia points is relatively easy. But it is still not a trivial task as most literatures declare because at least one special case evokes my caution during the minutia marking stage.

The sliding matrix algorithm has been implementation to identify ridge ending and bifurcations.

For each 3x3 window, if the central pixel is 1 and has exactly 3 one-value neighbors, then the central pixel is a ridge branch / bifurcation [Figure 22]. If the central pixel is 1 and has only 1 one-value neighbor, then the central pixel is a ridge ending / termination [Figure 21].

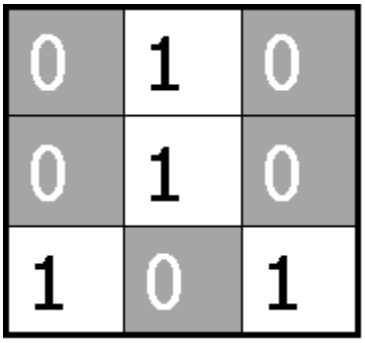


Figure 21, Bifurcation

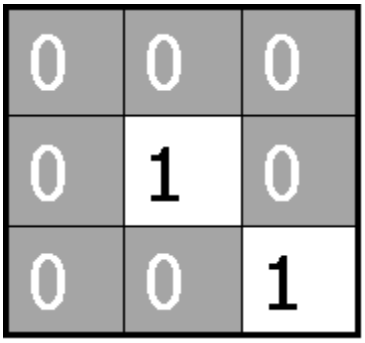


Figure 22, Termination

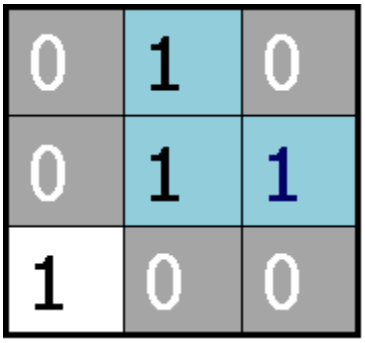


Figure 23, Triple counting branch

Figure 23 illustrates a special case wherein a genuine branch is triple counted. Suppose both the uppermost pixel with value 1 and the rightmost pixel with value 1 have another neighbor outside the 3x3 window, so the two pixels will be marked as branches too.

However, only one branch is located in the small region. So a check routine requiring that none of the neighbors of a branch are branches is added.

Also the average inter-ridge width D is estimated at this stage. The average inter-ridge width refers to the average distance between two neighboring ridges. D value can be approximated by scanning a row of the thinned ridge image and summing up all pixels in the row whose value is one, then dividing the row length with the above summation to get an inter-ridge width. For more accuracy, such kind of row scan can be performed upon several other rows and column scans can also be conducted. Finally all the inter-ridge widths are averaged to get the D.

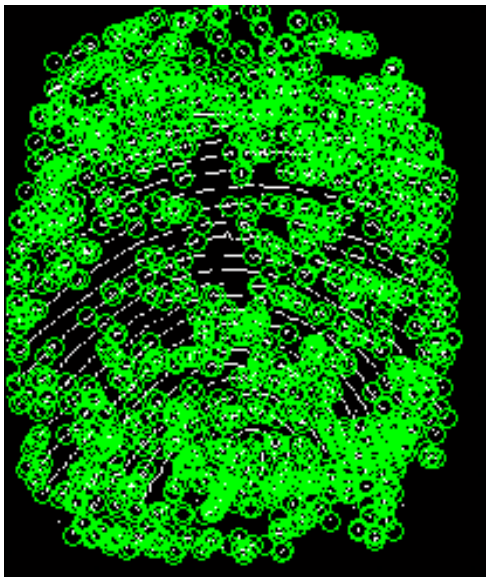


Figure 24, Minutiae extraction

For minutiae matching, the labels of input image are matched with the labels of template image, if match found, person is identified or we can ask for other database, otherwise there is no match for fingerprint

Heartbeat detection for “is-alive” check

Human heartbeat pattern is roughly regular. Hence, we can assume the regularly repeating pattern to be a periodic signal**.**

Fourier series can be used to represent such periodic signals. Fourier series decomposes any periodic function or periodic signal into the sum of a (possibly infinite) set of simple oscillating functions, namely sines and cosines

For the simulation of heartbeat signal, P, QRS and T waves have been modeled as a Fourier series to represent and regularly repeating signal. The period has been assumed to be 72 beats per minute (i.e. average heartbeat rate of a healthy human being).

Fourier's formula for periodic functions (-T to +T) using sines and cosines

For a periodic function $f(x)$ that is integrable on $[-T, T]$, a_n and b_n are called the Fourier coefficients of f.

$$c_0 = (1/2T) \int_{-T}^{+T} f(x)\, dx \qquad (1)$$

$$a_n = (1/T) \int_{-T}^{+T} f(x)\cos(nx)\, dx \qquad (2)$$

And,

$$b_n = (1/T) \int_{-T}^{+T} f(x)\sin(nx)\, dx \qquad (3)$$

One introduces the partial sums of the Fourier series for f, often denoted by

$$f(x) = c_0 + \sum_{n=1}^{\infty} [a_n\cos(nx) + b_n\sin(nx)],\ N \geq 0 \qquad (4)$$

Modeling the heartbeat using Fourier series

PR Interval = 120-200 ms (160 ms)

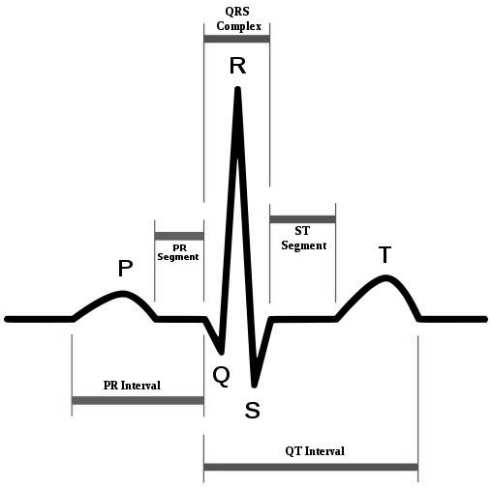
PR segment = 50-120 ms (85 ms)

QRS Complex = 80-120 ms (100 ms)

ST segment = 80-120 ms (100 ms)

QT Interval = 300-430 ms (365 ms) (QRS Complex + ST segment + T duration)

T wave = 160 ms



P Wave amplitude = 0.25 mV

Q Wave amplitude = 0.025 mV

R Wave amplitude = 2.5 mV

S Wave amplitude = 0.25 mV

T Wave amplitude = 0.35 mV

$$p(x) = \begin{cases} 0.025 \sin(\pi x/0.075) & 0 \le x \le 0.075 \\ 0 & 0.075 < x \le 0.16 \end{cases}$$

$$qrs(x) = \begin{cases} 0.7x - 0.112 & 0.16 < x \le 0.21 \\ -0.7x + 0.182 & 0.21 < x \le 0.26 \end{cases}$$

$$t(x) = \begin{cases} 0 & 0.26 < x \le 0.36 \\ 0.025 \sin(\pi(x-0.36)/0.16) & 0.36 < x \le 0.52 \end{cases}$$

CHAPTER 4 - IMPLEMENTATION

Technology Used

To implement this system MATLAB R2007a (7.4.0) has been used. The name MATLAB stands for matrix laboratory. MATLAB is a high performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation. MATLAB is an interactive system whose basic data element is an array that does not require dimensioning. This allows you to solve many technical computing problems, especially those with matrix and vector formulations, in a fraction of the time it would take to write a program in a scalar non interactive language such as C or Fortran.

This provides tools and other utilities that help to develop, execute, debug and document programs.

Here we have assumed some predefined datasets but we can use the scanner to get the fingerprint images due to financial constraints we are using datasets for fingerprints.

Analysis and Result

Home GUI interface

A graphical user interface (GUI) interface has been developed which provides a façade for fingerprint matching and “is-alive” detection. GUI accepts an input image and matched the image with the pre-existing image database for any prospective match.

The GUI primarily has been created to showcase 3 axes and support 9 different operations.

- **Axes 1** – Input fingerprint image
- **Axes 2** – Respective images in the database. At any instant axes 2 displays the current image against which the match is being performed

- **Axes 3** – Detect a live heart beat signal for “is-alive” detection

Operations supported:

1. Load fingerprint image
2. Binarize image
3. Thin image
4. Extract minutiae
5. Match in existing fingerprint database
6. Detect heat beat
7. Reset data
8. Clear data
9. Exit

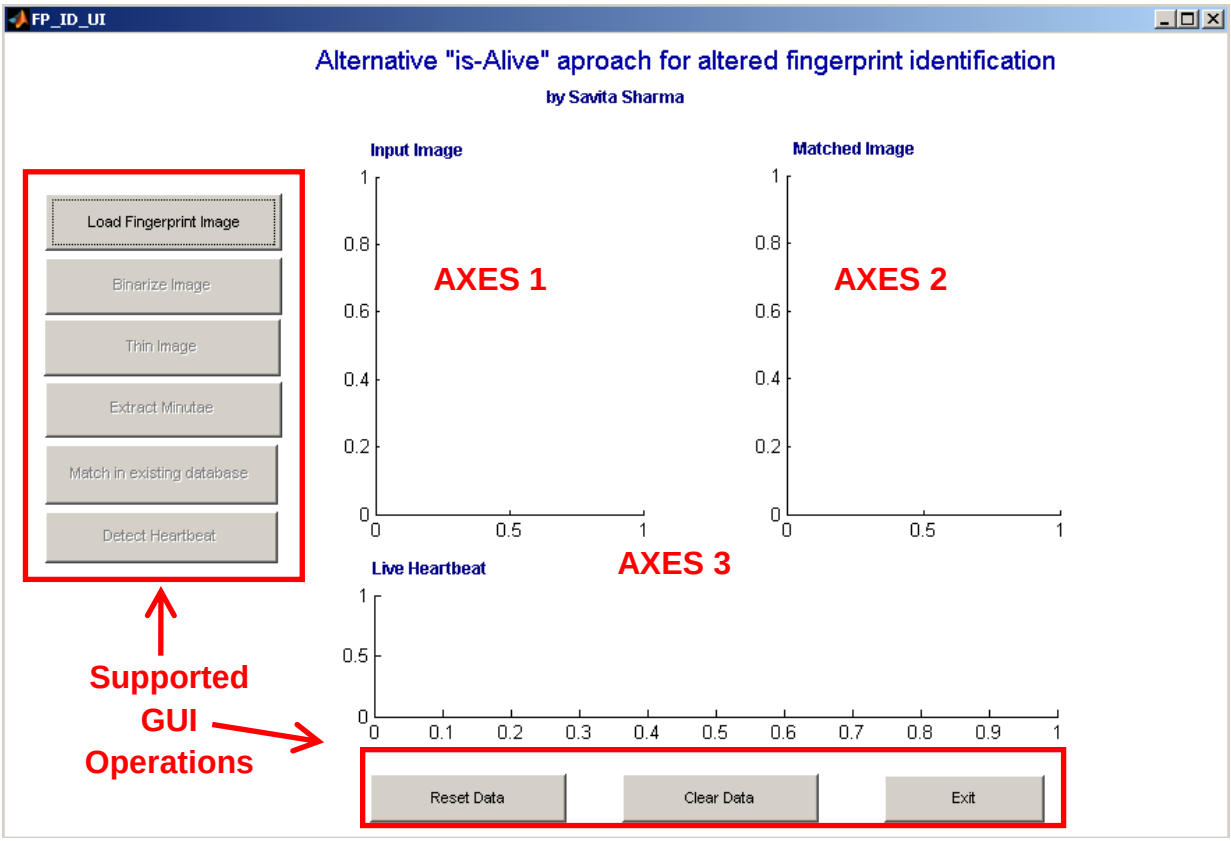


Figure 25, Home GUI Interface

The following screen shots detail various operations for the implementation of minutiae matching algorithm and “is-alive” detection mechanism for altered fingerprint identification. For simplicity all aspects of minutiae matching algorithm have not been implemented.

Load fingerprint image

When user clicks on the “Load fingerprint image”, it opens a file explorer dialog from where the user can select to load the input fingerprint image for verification and identification. Before displaying the image, the image is converted into a grayscale and scaled to the size of 250 X 250 pixels. For simplicity it has been assumed that alignment of all the fingerprint images in the database is same and no external alignment is performed as a part of the implementation.

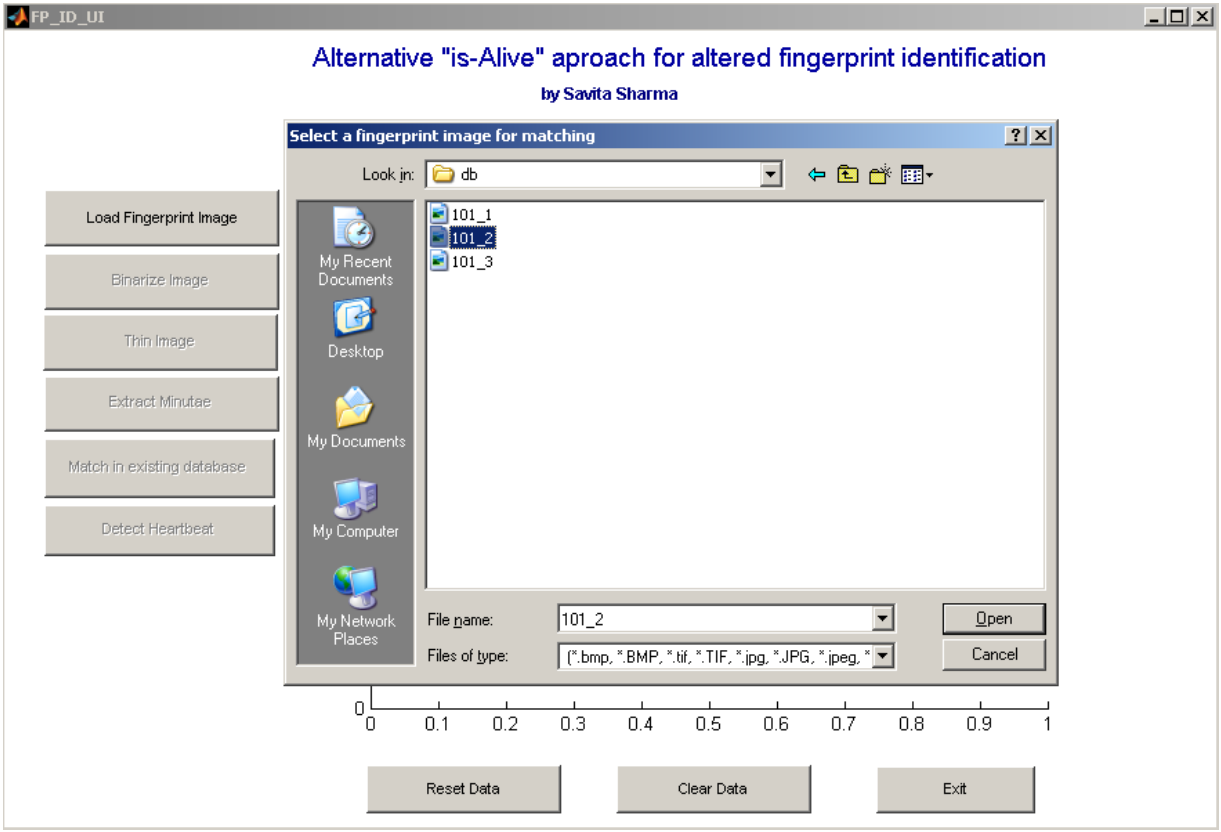


Figure 26, Load fingerprint image

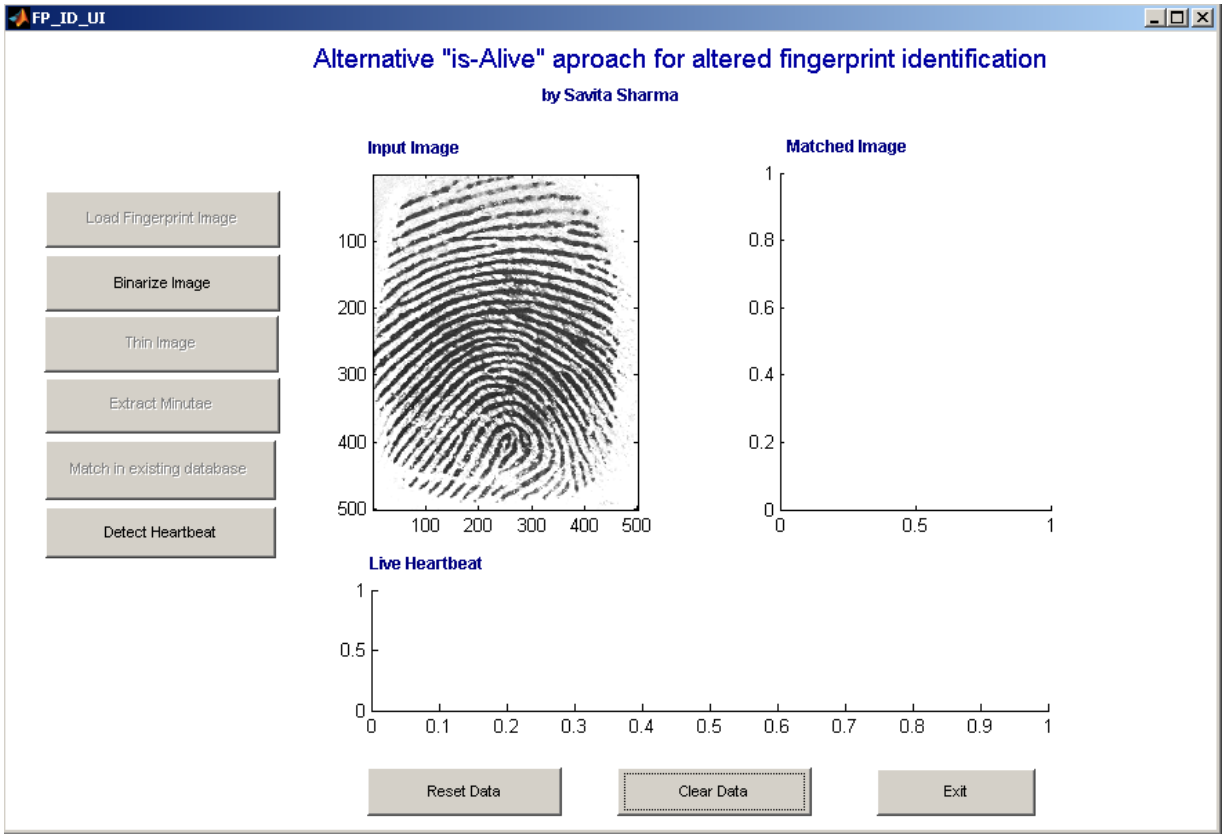


Figure 27, Display input fingerprint image after size and grayscale transformation

Binarize image

Binarize image transforms the image from grayscale image to black and white image. This simplification of the image ensures that further transformation of the image can be performed easily. On the scale of 0 to 1, any grayscale color information below and equal to 0.5 is considered as 0 (white) and above 0.5 is considered as black.

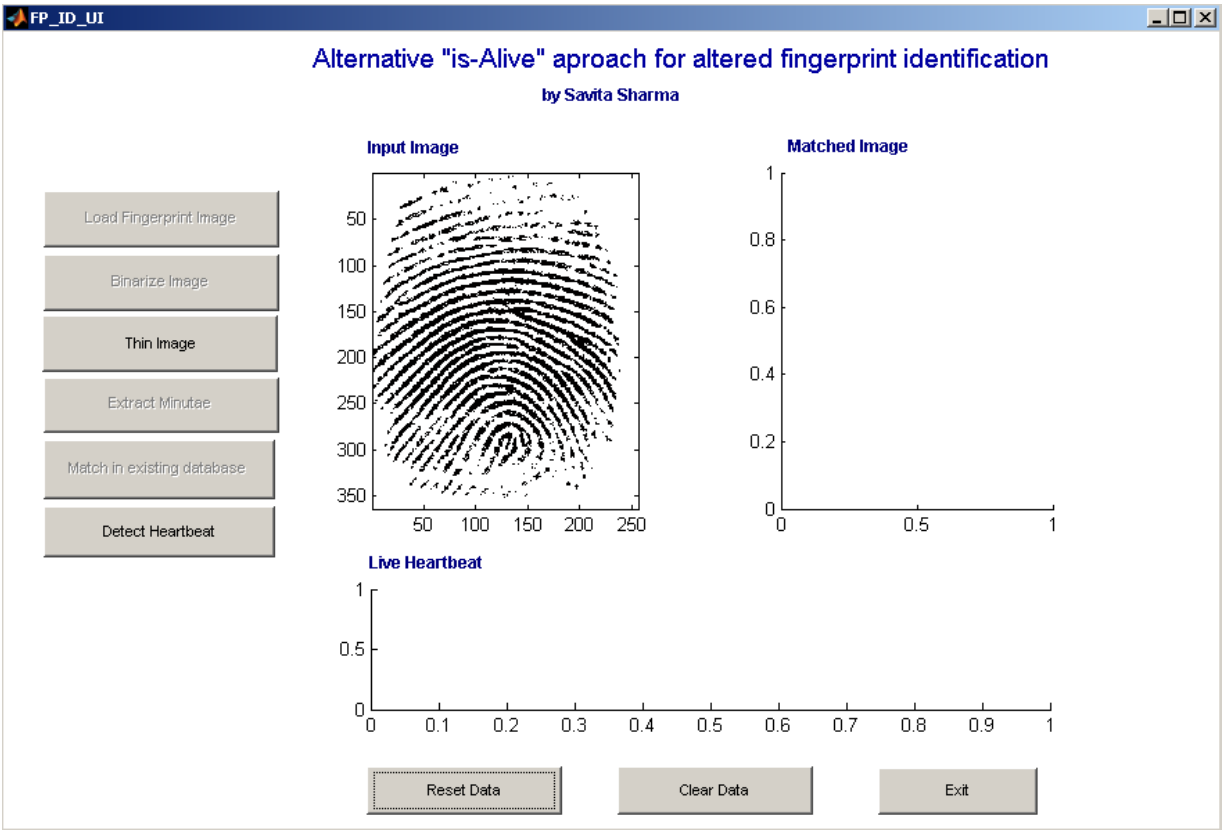


Figure 28, Binarized Image

Image Thinning

Image thinning simplifies the image data further by reducing the ridges to only 1 pixel wide.

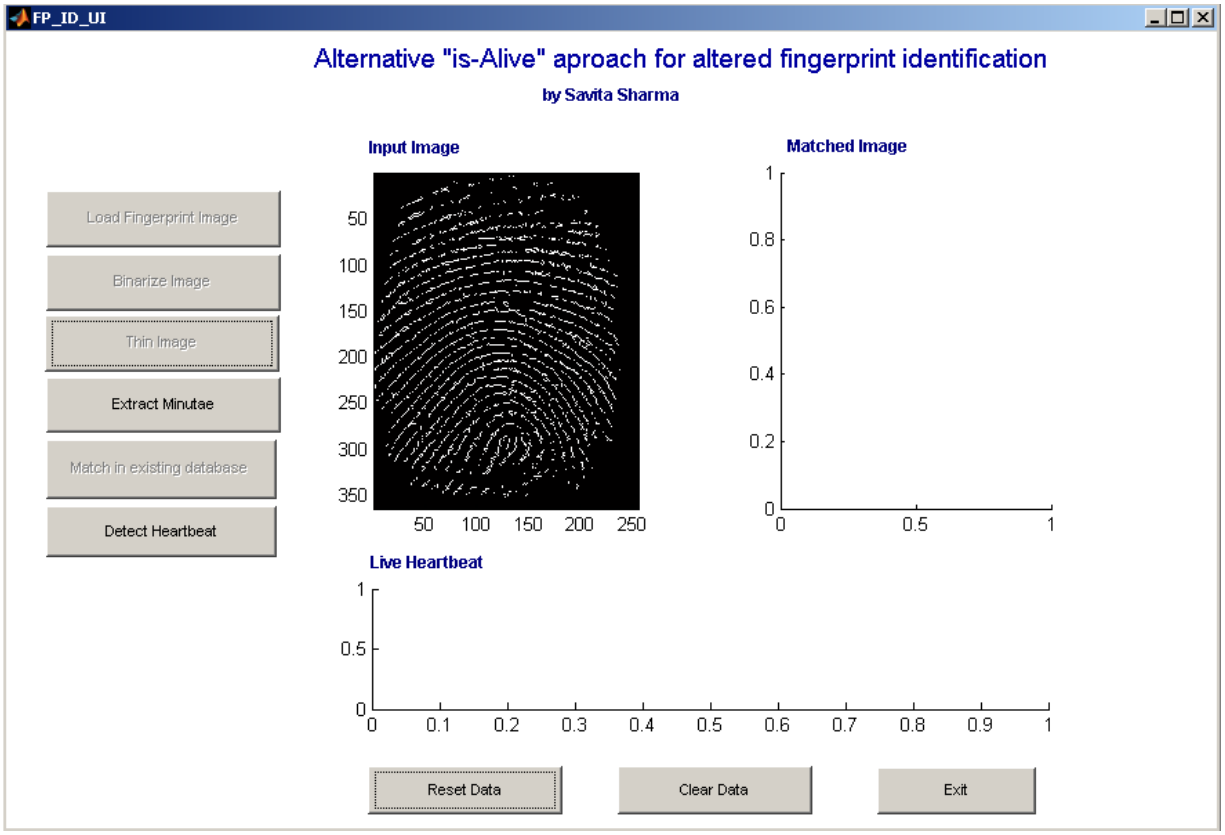


Figure 29, Thinned image

Minutiae Extraction

Minutiae extraction extracts minutiae from the thinned image (input image). This includes all minutiae points including true and false. False minutiae can be further filtered by using any of the existing techniques. The minutiae identified are the minutiae centroid(s) which are labeled as green circles in the figure below. The algorithm applies the neighborhood operations to identify the minutiae ending and minutiae bifurcations.

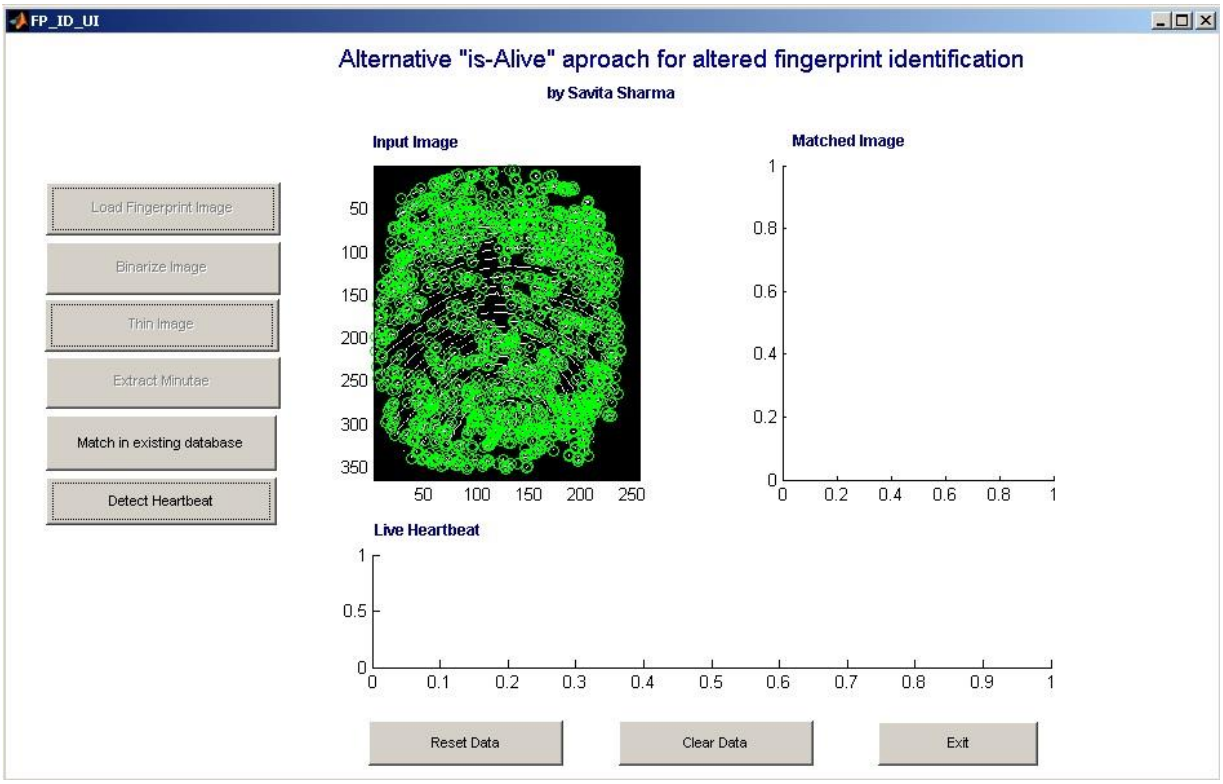


Figure 30, Minutiae extraction

Fingerprint Matching

Fingerprint matching matches the input fingerprint image with the images existing in the database for a prospective match. When user clicks on the “Match in existing database”, it opens a file explorer dialog from where the user can select to load the image database.

For each image in the database, the similar operations (binarize, thinning and minutiae extraction) are performed and minutiae and compared with input image for a match.

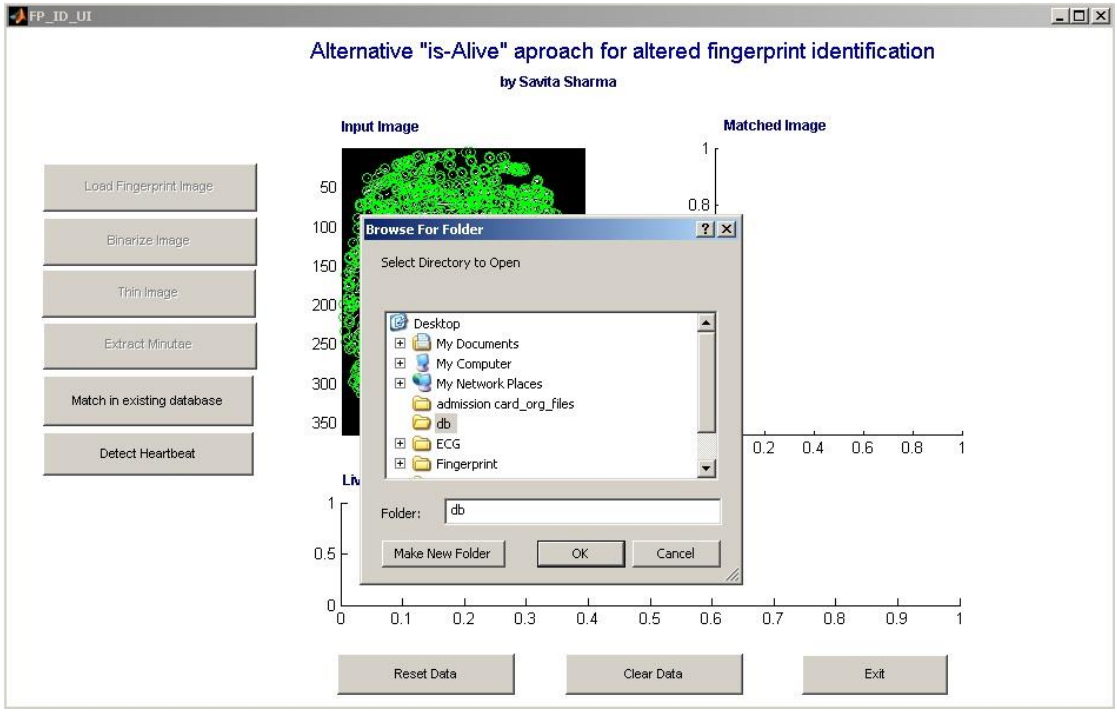


Figure 31, Select image database for matching

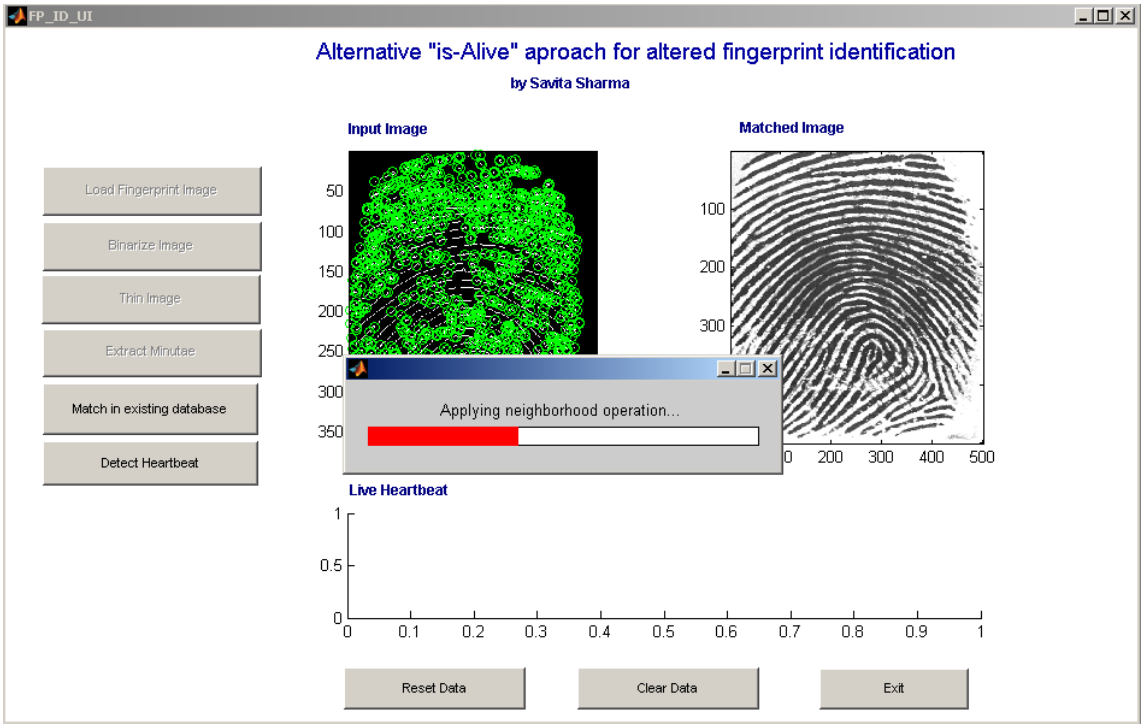


Figure 32, Minutiae comparison in progress

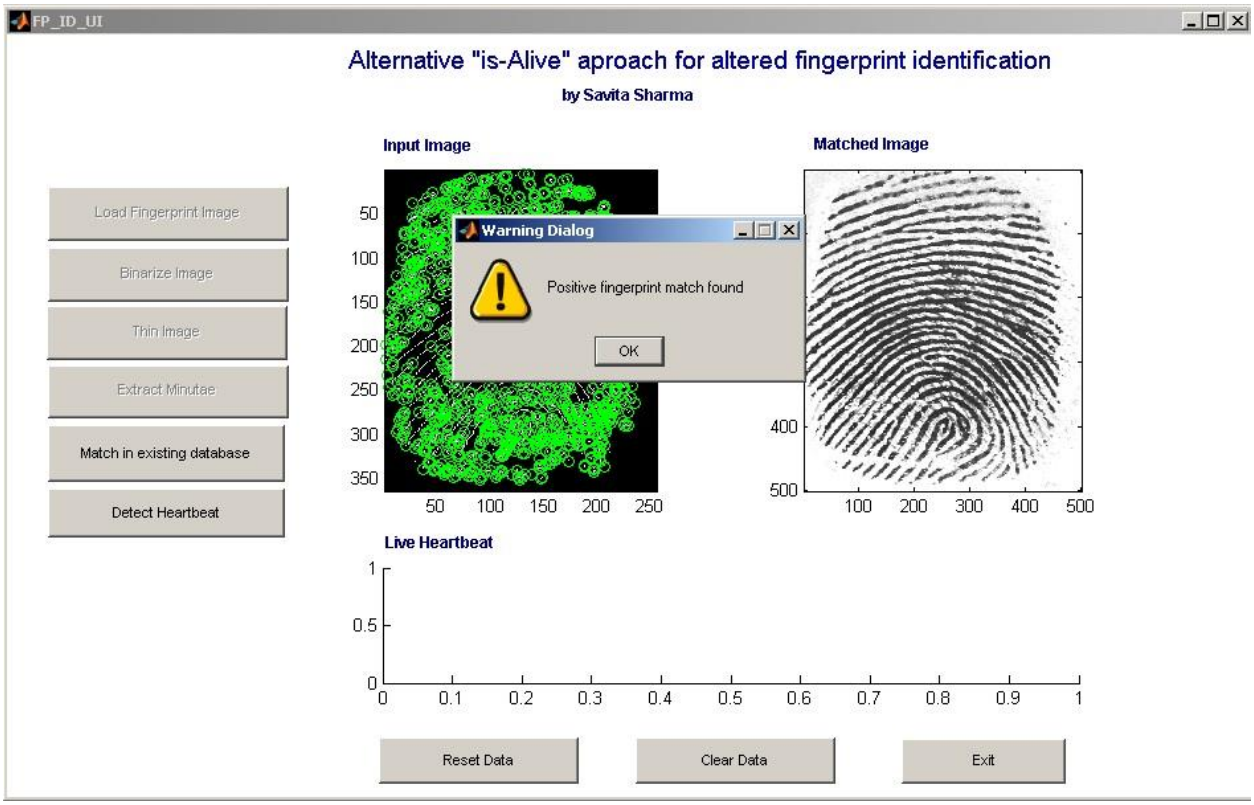


Figure 33, Fingerprint matching in progress (positive match found)

Heartbeat Detection

Heartbeat detection detects the heart beat of the user to perform “is-alive” check while authentication. The function simulates the heart beat signal using the Fourier transform for each of the P, QRS and T waves respectively. The GUI showcases the heart beat functionality which in actual needs a specialized hardware to physically detect heart beat. The design of the specialized hardware for heartbeat detection is outside the scope of this research.

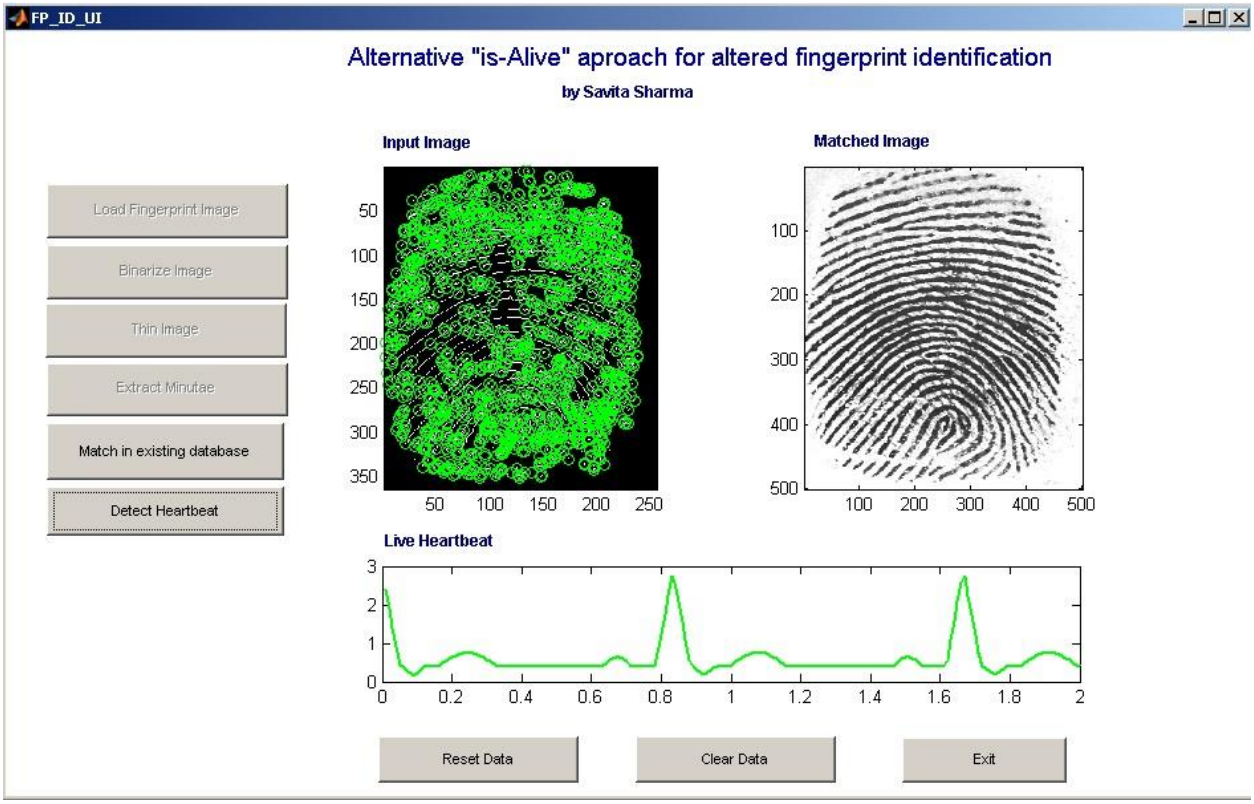


Figure 34, Heart beat detection to perform “is-alive” check

Clear All Data / Reset Data

These functions clear the existing data on the GUI window. This performs a subset operation of Reset Data. All the existing data and manipulations on the image are purged. This resets the GUI to perform a new fingerprint match and “is-alive” detection.

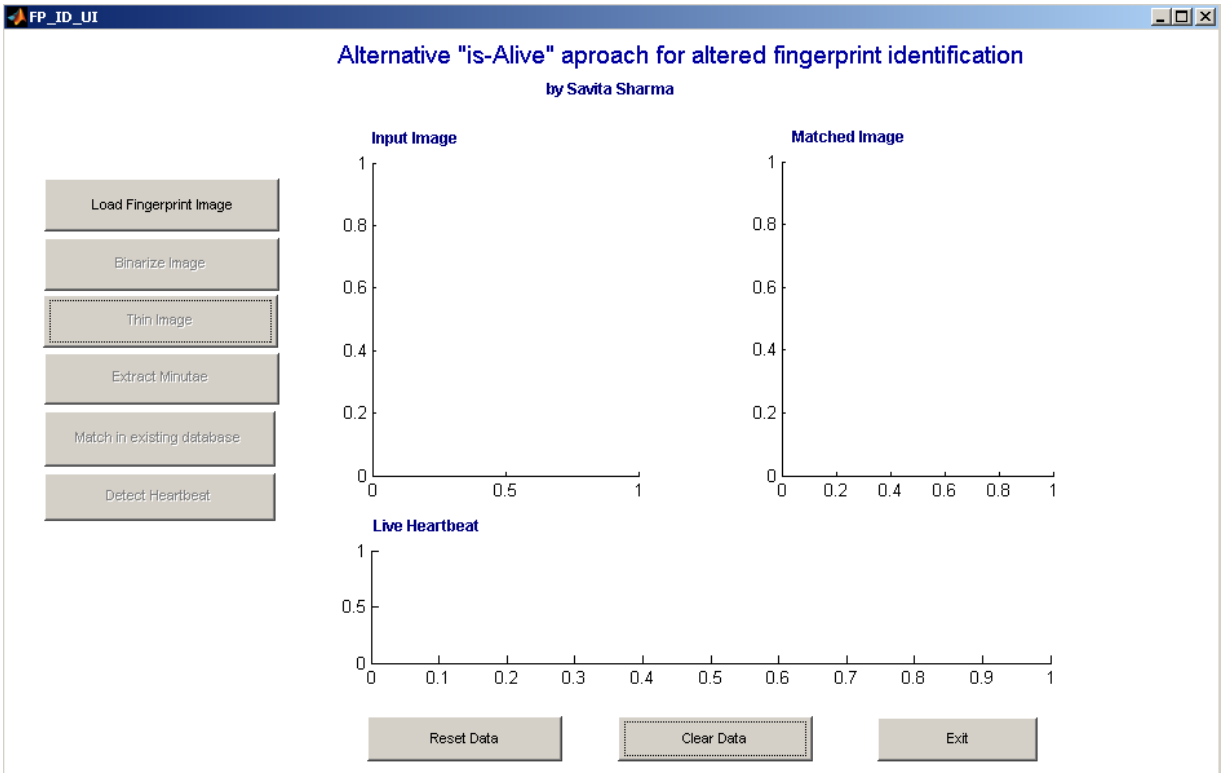


Figure 35, Reset all data

Exit GUI

Exit GUI performs an exit from all operation if pressed. It prompts the user for a “yes” or a “no”. If no is selected, the user is returned to the main screen with data-intact.

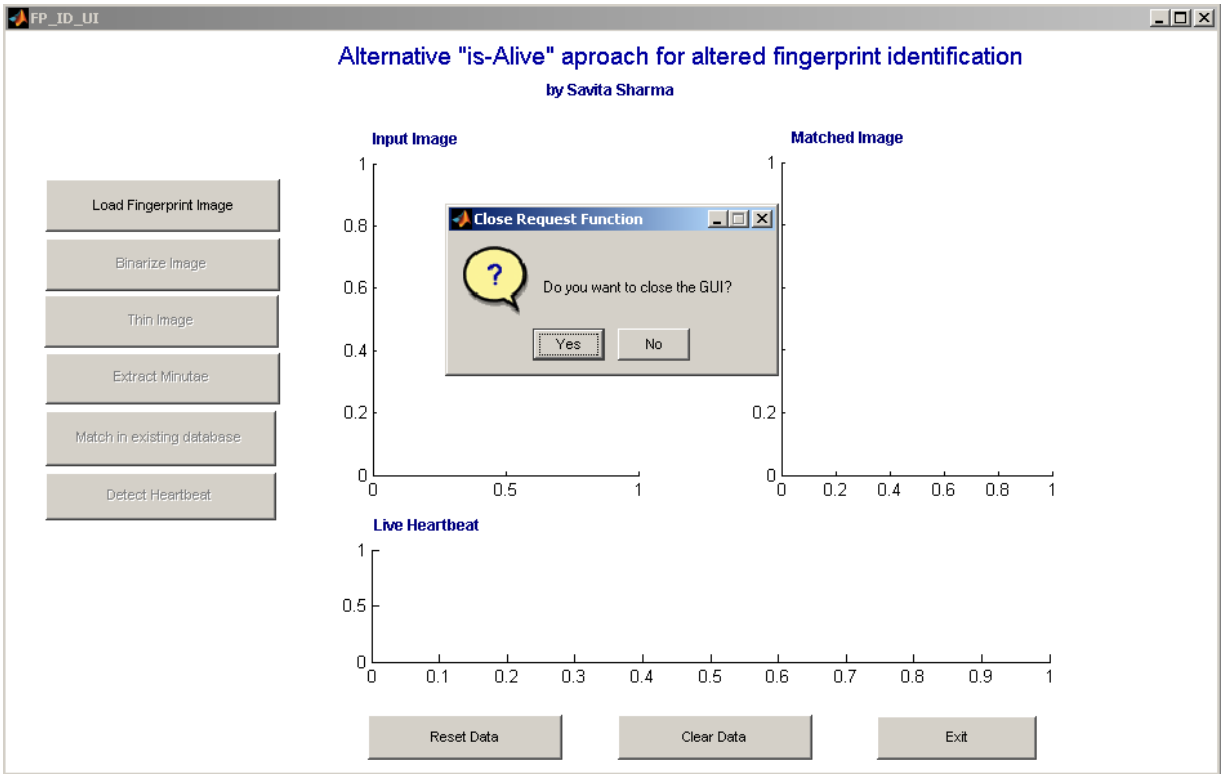


Figure 36, Exit GUI

CHAPTER 5 - CONCLUSION AND FUTURE WORK

Conclusion

Though a biometric characteristic may provide an effective authentication mechanism, there could however be the limitations in using any single biometric characteristic like noise in sensed data, intra-class variations etc. “is-alive” / liveness check can drastically enhance the reliability of a biometric system through the use of an involuntary signal generated by a living body. Leveraging on the strengths of a fingerprint recognition system, the research proposes design and development of minutiae based fingerprint identification system augmented by a heartbeat detection system for “is-alive” check. This research also presents an overview of the different steps involved in the development of a multi-modal biometric identification and verification system and simulated the authentication mechanism using MATLAB. However, the system developed can still be enhanced for decreasing the time spent during fingerprint processing and the reduction in the number of false acceptances and rejections made by the algorithm. Work is currently underway on some modifications to the matching mechanism, which would further improve the system’s accuracy.

Future Work

Multi-modal biometric authentication can drastically enhance the reliability of a biometric authentication. Heartbeat provides an effective mechanism for “is-alive” check. However, this can still be enhanced by the use of an intelligent and learning authentication model where the heart beat patterns, finger swipe patterns can be correlated to certain scenarios like coercion, fake identity etc.

REFERENCES

- *Handbook of Fingerprint Recognition* - Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar
- *Fingerprint Classification and Matching* - Anil Jain (Dept. of Computer Science & Engg, Michigan State University) & Sharath Pankanti (Exploratory Computer Vision Grp. IBM T. J. Watson Research Centre)
- A Survey Of Biometric Recognition Methods - Kresimir Delac, Mislav Grgic
- *Local Correlation-based Fingerprint Matching* - Karthik Nandakumar (Dept. of Computer Science & Engg, Michigan State University) & Anil K Jain (Dept. of Computer Science & Engg, Michigan State University)
- *A Correlation-Based Fingerprint Verification System* - Asker M. Bazen, Gerben T.B. Verwaaijen, Sabih H. Gerez, Leo P.J. Veelenturf and Berend Jan van der Zwaag (University of Twente, Department of Electrical Engineering, Laboratory of Signals and Systems)
- *Fingerprint Minutiae Matching Based on the Local And Global Structures* - Xudong Jiang and Wei-Yun Yau (Centre for Signal Processing, Nanyang Technological University)
- *Analysis of Human Electrocardiogram for Biometric Recognition* – Yongjin Wang, Foteini Agrafioti, Dimitrios Hatzinakos, and Konstantinos N. Plataniotis
- *Fingerprint minutiae extraction from skeletonized binary images* - Alessandro Farina, Zsolt M. Kovacs-Vajna*, Alberto Leone
- *Fingerprint Recognition* – Vinay Gupta & Rohit Singh (Indian Institute of Technology, Kanpur)
- *Liveness Detection for Biometric Systems Based on Papillary Lines* - Martin Drahansky, Dana Lodrova (Brno University of Technology, Faculty of Information Technology)
- *Personal Identification and Authentication by using “the way the heart beats”* - Johan F. du Preez, Prof S.H. von Solms (University of Johannesburg)

- *Continuous Authentication by Electrocardiogram Data* - Mouhcine Guennoun, Najoua Abbad, Jonas Talom, Sk. Md. Mizanur Rahman, and Khalil El-Khatib (University of Ontario Institute of Technology)
- *Fingerprint Alteration* - Jianjiang Feng, Anil K. Jain, and Arun Ross
- *Fingerprint Image Enhancement and Minutiae Extraction* – Raymond Thai