Designing of a Virtual System with Fingerprint Security by considering many Security threats

Kalpana Saini
Reasearch Scholar
IIT Roorkee
Roorkee, India

M.L.Dewal
Faculty
IIT Roorkee
Roorkee, India

ABSTRACT

In these days there is a requirement of reliable security system for process industry, in banks, homes etc. We have taken one of the Biometric modality i.e. fingerprints for this purpose which is the most reliable security tool for security of the system. Fingerprint recognition has long been favored among many biometric identification technologies due to its uniqueness and permanence. Nowadays, fingerprint recognition is considered to be the best choice for most applications from network security systems to compact devices, due to its accuracy, speed, reliability, non-intrusive interfaces, and cost-effectiveness. We have made a fingerprint matching system using MATLAB. After collecting the database we provide a security to a virtual process that has been designed in LABVIEW and make an efficient HMI.The fingerprint recognition system may suffer attacks at different points during the authentication process. Somtimes the fingerprints gives 100% matching but it may be false fingerprint.The most common attacks occur by the use of fake fingerprint during the capture of image. The transmission channel between the feature extractor and matching may also be intercepted and the fingerprint feature may be stored for the later use. The main problem relies on how to differentiate a live finger from that one made of some synthetic material. In This Paper we disscuss the all such type of attacks as well as some other interseting and other topics related to fingerprints like these may be damage or stolen by some personand effect of illlness to them. This paper gives an approch to remove such type of attacks by using a virtual system. Along with this virtual system some aspects related to secure fingerprint is also be considered in this paper.

Keywords

Authentication, Biometrics, Fingerprint recognition, HMI.

1. INTRODUCTION

1.1 Basics on fingerprint

Fingerprints are the tiny ridges, whorls and valley patterns on the tip of each finger. They form from pressure on a baby's tiny, developing fingers in the womb. No two people have been found to have the same fingerprints -- they are totally unique. There's a one in 64 billion chance that your fingerprint will match up exactly with someone else's.

Fingerprints are even more unique than DNA, the genetic material in each of our cells. Although identical twins can share the same DNA -- or at least most of it -- they can't have the same fingerprints. Fingerprinting is one form of biometrics, a science that uses people's physical characteristics to identify them. Fingerprints are ideal for this purpose because they're inexpensive to collect and analyze, and they never change, even as people age.

Fingerprints are made of an arrangement of ridges, called friction ridges. Each ridge contains pores, which are attached to sweat glands under the skin. You leave fingerprints on glasses, tables and just about anything else you touch because of this sweat.

The fingerprint surface is made up of a system of ridges and valleys that serve as friction surface when we are gripping the objects. The surface exhibits very rich structural information when examined as an image. The fingerprint images can be represented by both global as well as local features. The global features include the ridge orientation, ridge spacing and singular points such as core and delta. The singular points are very useful from the classification perspective. However, verification usually relies exclusively on minutiae features. Minutiae are local features marked by ridge discontinuities. There are about 18 distinct types of minutiae features that include ridge endings, bifurcations, crossovers and islands. Among these, ridge endings and bifurcation are the commonly used features.

There are two different types of prints:

- Visible prints are made on a type of surface that creates an impression, like blood, dirt or clay.
- Latent prints are made when sweat, oil and other substances on the skin reproduce the ridge structure of the fingerprints on a glass, murder weapon or any other surface the perpetrator has touched. These prints can't be seen with the naked eye, but they can be made visible using dark powder, lasers or other light sources. Police officers can "lift" these prints with tape or take special photographs of them.

Based on twenty years of continuing technology development and successful operational experience, fingerprint biometrics remain the only scientifically and operationally proven biometric technology, the only biometric technology with a mature infrastructure of supporting technologies, and the only technology supported by national and international standards. Technology advances made over the past few years have resulted in off-the-shelf fingerprint ID systems with the capability to complete duplicate registration searches of very large databases in seconds. Fingerprints have several advantages over other biometrics, such as the following:

1. High universality: A large majority of the human population has legible fingerprints and can therefore be easily authenticated. This exceeds the extent of the population who possess passports, ID cards or any other form of tokens.

2. High distinctiveness: Even identical twins who share the same DNA have been shown to have different fingerprints, since the ridge structure on the finger is not encoded in the genes of an individual. Thus, fingerprints represent a stronger authentication mechanism than DNA.

3. High permanence: The ridge patterns on the surface of the finger are formed in the womb and remain invariant until death except in the case of severe burns or deep physical injuries.

4. High performance: Fingerprints remain one of the most accurate biometric modalities available to date with jointly optimal FAR (false accept rate) and FRR (false reject rate).

5. Wide acceptability: While a minority of the user population is reluctant to give their fingerprints due to the association with criminal and forensic fingerprint databases, it is by far the most widely used modality for biometric authentication.

Although as we disscussed fingerprint is most reliable biomerics for authentication but because of high crimnal activities there may be attack on these fingerprints.The fingerprint recognition system may suffer attacks at different points during the authentication process. Section and sub-section headings and attributes.The most common attacks occur by the use of fake fingerprint during the capture of image. A fake fingerprint are build from latent fingerprint left at touched items such as glasses, doorknobs, glossy paper, etc. Using this fingerprint are build three-dimensional molds of rubber membrane, glue, or gelatin.
During the transmission of the image to the feature extractor may occur interception of the channel, and consequently, the fingerprint image may be stolen and later, used for fake fingerprint construction or for directly access to feature extractor by bypassing the scanner. The feature extractor may be substitute by a Trojan horse, which bypass the feature extractor and generate artificial template and submit to the matcher.
The main objective of this paper is to discuss different types of attacks. And many more interesting tasks related to fingerprints, such as how these may differ these may be destroyed or not. In the last section we also design a virtual system for get rid of those attacks. This system provides a virtual visibility of complete process.

2. DESIGNING OF FINGERPRINT MATCHING SYSTEM

2.1 Image pre-processing

It is first necessary to apply several pre-processing steps to the original fingerprint image to produce consistent results in the classic minutiae extraction procedure. Such steps generally include image Enhancement, Binarization and Segmentation**.**

2.1.1 Image Enhancement

A critical step in automatic fingerprint matching is to automatically and reliably extract minutiae from the input fingerprint images. In this paper two techniques are used for enhancement – (i) Histogram equalization and (ii) Fast Fourier Transform [2].

Histogram equalization:

If $P_s(s)$ is the PDF of Transformed intensity s and $P_r(r)$ is PDF before transformation than:

We use here transformation

$$T(r) = (L-1)\int_0^r p_r(w)\,dw$$

With the help of this we get

$$p_s(s) = \frac{1}{L-1}$$

Where $$0 \le s \le L-1$$

This is uniform independently of the form $p_r(r)$

We divide the image into small processing blocks (16 by 16 pixels i.e. M=N=16) and perform the Fourier transform according to:

$$F(x,y) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(u,v)\times \exp\left\{-j2\pi\left(\frac{xu}{M}+\frac{yv}{N}\right)\right\}$$

for x= 0, 1, 2, ..., 15 and y= 0, 1, 2, ...,15

Get the enhanced block according to

$$g(u,v) = F^{-1}\left[F(x,y)\times|F(x,y)|^K\right]$$

for u = 0, 1, 2, ..., 15 and v = 0, 1, 2, ..., 15.

Where $F^{-1}(F(x,y))$ is done by

$$f(u,v) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} F(x,y)\times\left\{j2\pi\times\left(\frac{xu}{M}+\frac{yv}{N}\right)\right\}$$

2.1.2 Binerization

Fingerprint Image Binarization is to transform the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows [3]. After the operation, ridges in the fingerprint are highlighted with black color while valleys are white.

2.1.3 Segmentation

Segmentation divides an image into its constituent regions or objects. In general, only a Region of Interest (ROI) is useful to be recognized for each fingerprint image. The image area without effective ridges and valleys is first discarded since it only holds background information [4]. Then the bound of the remaining effective area is sketched out since the minutia in the bound region is confusing with those spurious minutia's that are generated when he ridges are out of the sensor.

Estimate the block direction for each block of the fingerprint image with WxW in size (W is 16 pixels by default).

For this firstly block direction estimation has been applied

for each Least Square approximation of the block direction.

$$t_g 2\beta = 2\frac{\sum\sum g_x \times g_y}{\sum\sum g_x^2 \times g_y^2}$$

Where g_x & g_y are gradient values along x-direction and y-direction respectively.

The tangent value of the block direction, θ is the angle of ridge from axis.

$$t_g 2\theta = 2\frac{\sin\theta\cos\theta}{\cos^2\theta - \sin^2\theta}$$

Blocks without significant information on ridges and furrows are discarded based on the following formulas:

$$E = \frac{2\sum\sum g_x \times g_y + \sum\sum g_x^2 - g_y^2}{W \times W \times \sum\sum g_x^2 + g_y^2}$$

if its certainty level E is below a threshold, then the block is regarded as a background block.

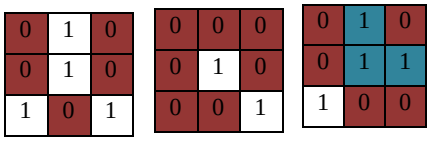
2.2 Minutia Extraction

2.2.1 Fingerprint Ridge Thinning

Ridge Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. [3] Uses an iterative, parallel thinning algorithm. In each scan of the full fingerprint image, the algorithm marks down redundant pixels in each small image window (3x3). And finally removes all those marked pixels after several scans. In my testing, such an iterative, parallel thinning algorithm has bad efficiency although it can get an ideal thinned ridge map after enough scans. [13] Uses a one-in-all method to extract thinned ridges from gray-level fingerprint images directly. Their method traces along the ridges having maximum gray intensity value. However, binarization is implicitly enforced since only pixels with maximum gray intensity value are remained. Also in my testing, the advancement of each trace step still has large computation complexity although it does not require the movement of pixel by pixel as in other thinning algorithms. Thus the third method is bid out which uses the built-in Morphological thinning function in MATLAB.
The thinned image ridge map is then filtered by other three Morphological operations to remove some H breaks, isolated points and spikes.

2.2.2 Mark Minutia Point

In general, 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 or bifurcation(a) If the central pixel is 1 and has only 1 one-value neighbor, then the central pixel is ending (b)



(a) Termination (b) Bifurcation (c) Triple counting branch

Figure 1. Minutia Marking

(c) Illustrates a special case that 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. But actually 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. The way to approximate the D value is simple. Scan a row of the thinned ridge image and sum up all pixels in the row whose value is one. Then divide the row length with the above summation to get an inter-ridge width. For more accuracy, such kind of row scan is performed upon several other rows and column scans are also conducted, finally all the inter-ridge widths are averaged to get the D.

Together with the minutia marking, all thinned ridges in the fingerprint image are labeled with a unique ID for further operation. The labeling operation is realized by using the Morphological operation: BWLABEL.

2.3 Post processing

2.2.3 False Minutia Removal

My procedures in removing false minutia are:

(a) A spike piercing into a valley

(b) A spike falsely connects two ridges.

(c) Two near bifurcations located

(d) The two ridge broken points have nearly the same orientation and a short distance the same

(e) One part of the broken ridge is so short that another termination is generated

(f) A third ridge is found in the middle of the two parts of the broken ridge

(g) Only one short ridge found in the threshold window

2.2.4 Unify Termination and Bifurication

Since various data acquisition conditions such as impression pressure can easily change one type of minutia into the other, most researchers adopt the unification representation for both termination and bifurcation. So each minutia is completely characterized by the following parameters at last: 1) x-coordinate, 2) y-coordinate, and 3) orientation.

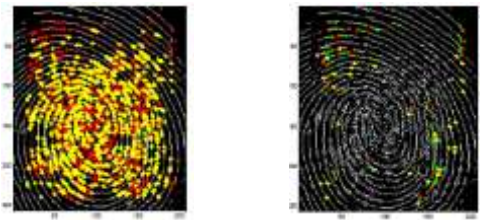


Figure 2. Minutia points (left) Minutia points after false minutia removal (right)

2.4 Minutia Matching

The matching process involves comparing one set of minutiae data to another set. In most cases, this process compares an input data set to a previously stored data set with a known identity, referred to as a template. The template is created during the enrollment process, when a user presents a finger for the system to collect the data from. This information is then stored as the defining characteristics for that particular user. Given two set of minutia of two fingerprint images, minutia match algorithm determines whether the two minutia sets are from the same finger or not.

An alignment-based match algorithm partially derived is used in my project. It includes two consecutive stages: one is alignment stage and the second is match stage.

2.2.4.1 Alignment stage

1. The ridge associated with each minutia is represented as a series of x-coordinates (x_1, $x_2 \ldots x_n$) of the points on the ridge. A point is sampled per ridge length L starting from the minutia point, where the L is the average inter-ridge length. And n is set to 10 unless the total ridge length is less than 10*L.

So the similarity of correlating the two ridges is derived from:

$$S = \frac{\sum_{i=0}^{m} x_i X_i}{\left[\sum_{i=0}^{m} x_i^{\,2} X_i^{\,2}\right]^{0.5}}$$

Where (x_i~x_n) and (X_i~X_N) are the set of minutia for each fingerprint image respectively. And m is minimal one of the n and N value. If the similarity score is larger than 0.8, then go to step 2, otherwise continue to match the next pair of ridges.

2. For each fingerprint, translate and rotate all other minutia with respect to the reference minutia according to the following formula:

$$\begin{pmatrix} xi\_new \\ yi\_new \\ \theta i\_new \end{pmatrix} = TM * \begin{bmatrix} \text{◀}i - x \\ yi - y \\ \theta i - \theta \end{bmatrix}$$

where (x,y,θ) is the parameters of the reference minutia, and TM is

$$TM = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Where (x_i~x_n) and (X_i~X_N) are the set of minutia for each fingerprint image respectively. And m is minimal one of the n and N value.

Translate and rotate all other minutia with respect to the reference minutia according to the following formula

$$\begin{pmatrix} xi\_new \\ yi\_new \\ \theta i\_new \end{pmatrix} = TM * \begin{bmatrix} \text{◀}i - x \\ yi - y \\ \theta i - \theta \end{bmatrix}$$

where (x,y,θ) is the parameters of the reference minutia.

2.2.4.2 Match Stage

The adaptive elastic string matching algorithm summarized here uses three attributes of the aligned minutiae for matching: its distance from the reference minutiae (*radius*), angle subtended to the reference minutiae (*radial angle*), and local direction of the associated ridge (*minutiae direction*). The algorithm initiates the matching by first representing the aligned input (template) minutiae as an input (template) minutiae string. The string representation is obtained by imposing a linear ordering based on radial angles and radii. The resulting input and template minutiae strings are matched using an inexact string matching algorithm to establish the correspondence.

My approach to elastically match minutia is achieved by placing a bounding box around each template minutia. If the minutia to be matched is within the rectangle box and the direction discrepancy between them is very small, then the two minutias are regarded as a matched minutia pair. Each minutia in the template image either has no matched minutia or has only one corresponding minutia.

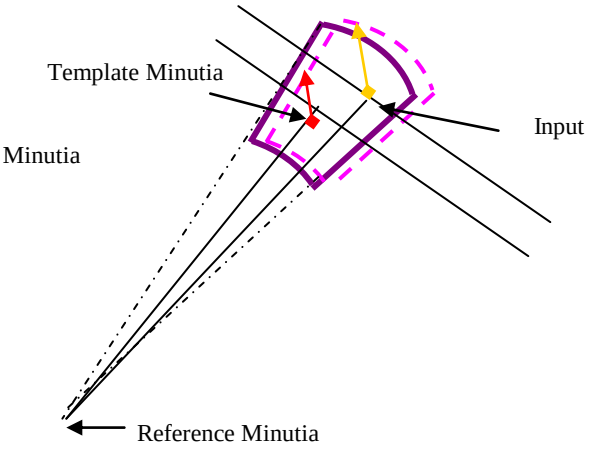


Figure 3 Bounding box and its adjustment

The algorithm tentatively considers a candidate (aligned) input and a candidate template minutiae in the input and template minutiae string to be a mismatch if their attributes are not within a tolerance window (see Fig 2) and penalizes them for deletion/insertion edit. If the attributes are within the tolerance window, the amount of penalty associated with the tentative

match is proportional to the disparity in the values of the attributes in the minutiae. The algorithm accommodates for the elastic distortion by adaptively adjusting the parameters of the tolerance window based on the most recent successful tentative match. The tentative matches (and correspondences) are accepted if the edit distance for those correspondences is smaller than any other correspondences.

The final match ratio for two fingerprints is the number of total matched pair over the number of minutia of the template fingerprint. The score is 100*ratio and ranges from 0 to 100. If the score is larger than a pre-specified threshold, the two fingerprints are from the same finger.

3. DIFFERENT EFFECTS ON FINGERPRINTS

Role of the skin on our fingertips, palm and soles of the feet is to grip other objects, and they all have characteristic "friction" ridges. Nevertheless, very little research has been carried out about how well fingers perform, how friction is achieved and why we have soft finger pads with fingerprints at all. Recent research carried out in the laboratory of the University of Manchester suggests that finger skin has frictional properties rather like rubber. The friction force rises with contact area rather than normal force. Therefore it appears strange that we have fingerprints at all since these reduce contact area.

A minor scrape, scratch or even burn won't affect the structure of the ridges in fingerprints -- new skin reforms in its original pattern as it grows over the wound. But each ridge is also connected to the inner skin by small projections called papillae. If these papillae are damaged, the ridges are wiped out and the fingerprint destroyed.

Fingerprint matching can also be effected by wet and dryness of fingers. Peoples with old age have poor quality fingerprints because of change in skin tightness. Peoples who works more manual work also have poor quality fingerprints.

4. ATTACKS ON FINGERPRINTS

A lot of serious security issues are getting uncovered in security devices that use only human fingerprints as authentication, too many myths and too many false cliams. One question which is always asked by people is can a fingerprint be changed or stolen and here's more detail about it.

Some criminals have tried to evade capture by tampering with their own fingerprints. Chicago bank robber John Dillinger reportedly burned his fingertips with acid in the 1930s. Recently, a man in Lawrence, Mass., tried to hide his identity by cutting and stitching up all ten of his fingertips (fortunately, a police officer recognized his face).

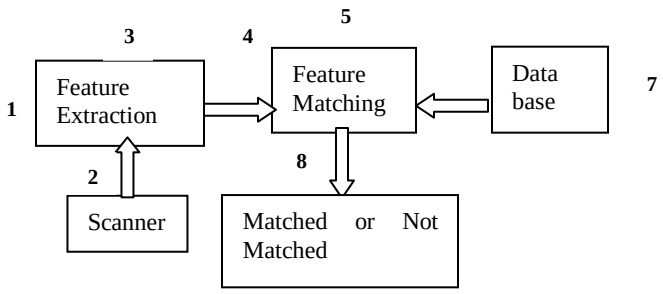


Figure 4. Areas for attack

But as fingerprint technology becomes a common form of authentication from bank vaults to luxury cars, law enforcement officials worry that would-be criminals might try to steal entire fingers for the prints. In one case, robbers in Malaysia cut off a man's fingers so they could steal his Mercedes. Companies that make biometrics security equipment realize the potential dangers of this system, and are now creating scanners that detect blood flow to make sure the finger is still alive.

Fig.4. Shows the area where attacks may occure.Fingerprint recognition is based on the fact that every human being has a unique pattern of ridges and valleys on their fingertips. A scanner makes copy of your fingerp and compares its characteristics to the ones stored beforehand. These characteristics are measured based on special points (such as branches and loops) on a print. some of these special points can be seen. The scanner uses these points as coordinates to define other branches, loops, beginning of lines, number of lines etc. The scanner used in this hack stores these characteristic points of the user's fingerprint on the smart card. The hack is to create an artificial finger using a mold that is manufactured using the legitimate user's actual finger. This type of attack is not really usable in real life as people are usually wise enough not to give their fingers as a mold material., this hack said that the scanner can be fooled using a gelatine finger instead of a live finger and can be taken further in technology "Creating a mold using a latent fingerprint".

5. PROTECTION AGAINEST ATTAKS

How the fingerprint was stolen, the fingerprint scanners should be able to reject the fake fingerprints. However detecting the aliveness of a finger it is not an easy task. The main problem relies on how to differentiate a live finger from that one made of some synthetic material. The easiest way to protect against fake finger attack is to avoid giving a mold of your fingers. To diminish the probability of a successful break-in is to use a smartcard protection for the scanner (and keep the card apart from the scanner when not used). This way the data burglar has to obtain both the smart card and a mold of the users finger. Another way to make things difficult is to use several fingers in the authentication. Then to break in to the system the breaker needs more than one mold, which is much harder than getting just one mold by fluke.

For Checking the aliveness of a finger which is touched to the scanner is to use a blood flow sensor with fingerprint Scanner. The main problem relies on how to differentiate a live finger from that one made of some synthetic material. There has been proposed some ideas to deal with this problem, which consist in using the thermal, electric and optical properties of the material presented to the fingerprint scanner. By using the temperature information, for example, it is expected that the fake finger made of silicone rubber is about 2 degree cooler than a live finger, however, due the temperature variation of the environment and the possibility of artificial heating the fake finger, the thermal measurements are not very reliable. The conductivity is another measure that could be explored, however, the conductivity of a live finger varies a lot depending of weather condition such as humidity and temperature. The optical properties such absorption, reflection, scattering and refraction,

in the human skin are different than many other synthetic material. However, it is not difficult to find materials.
As we can see, there no exists a reliable characteristic that could reject all fake fingerprints. Therefore, it is important to take special attention during the design and development of a secure fingerprint system.
Here we Design a virtual system for security of a process. This virtual system degn has dual advange taht is provide a reliable authentication security means with fingerprint as well as is aslo monitores and controls the hacking during authentication. Fig. 5 shows the window of virtual security system.

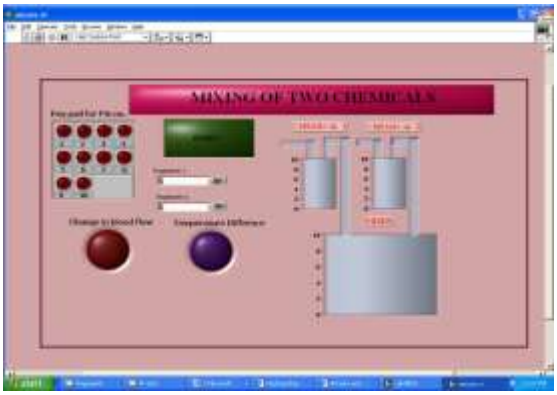


Figure 5. Window for security of a process

Here we provide a keypad for entering the Pin No. if pin no. is wrong than process is not start is indicates error and shows is to the administrator. Next security level is fingerprint sensor firstly there is a checking of aliveness of finger using a blood flow sensor if there is potential difference than only the stage is passed out otherwise it again shows an error. Next is to identify that fingerprint is natural finger or it is a fake finger made with mould, for this we use a temperature sensor. The next and last stage is matching of the finger with previous stored database. If these matched than only the process is started.

6. DESIGINING OF VIRTUAL PROCESS

We design a virtual process in LABVIEW environment. Which shows a virtual process in two steps first is preparing stage when a tank is send to the next process it's just for transferring the tank. Second stage has this tank.

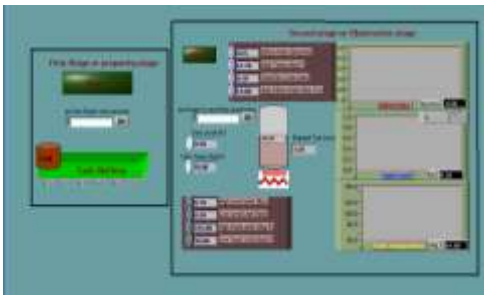


Figure 6.Virtual process of shifting and simulation of Tank

There is one more indicator for showing the time of the process. Charts show the inflow rate, tank level and tank temperature respectively.
In the figure below if start button is pressed and fingerprints are matched than the tank shifts from its initial stage to final stage.

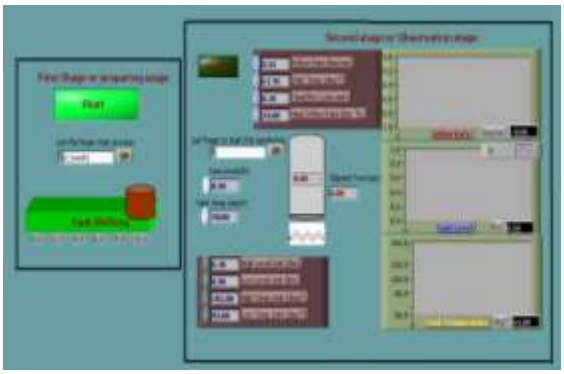


Figure 7. Preparing stage in running condition

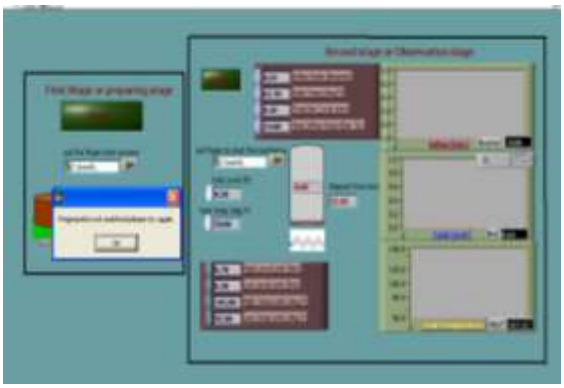


Figure 8. When fingerprints are not matched

Fig. 8 shows if fingerprint are not matched process is not started and a massege is shown that fingeprints are not matched please try again.

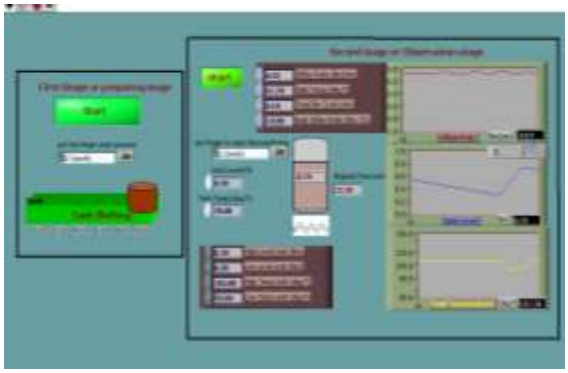


Figure 9. Shifting and Simulation in running condition

Fig 9 is the condition when both stages accept the fingerprints which are different for both processes. Means require access by different users and one user is not able to enter on the other process.

Here is a condition also in second stage that if fingerprint are not matched means the finger is not of an authenticated user than a window appears that shows that fingerprints are not matches please try again. This condition is shown in fig. 8. In this situation process is not able to start.

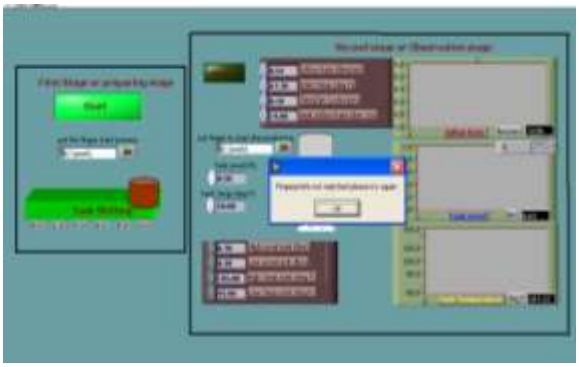


Fig.10 Fingerprints are not matched during simulation

7. CONCLUSIONS

This paper gives a approach to provide a reliable authentication using a most powerful tool fingerprints. It provides an HMI which fulfills all acceptations his paper gives the security to a virtual process means the HMI is here as an security tool. if a password or token method is used for this security then there may be risk of stolen. But in case of fingerprint security we can overcome from these problems. This paper provides a new idea of designing HMI as a virtual System. This paper discusses the points regarding fingerprints which are rarely be thinking by someone. This paper is useful for securing a system. The design of virtual system provides security from undesired access of process as well as for finding out the frauds by informing directly to administrator. There is four level securities. Fingerprint matching with pin no. and checking of fake identity shows a reliable authentication.

8. REFERENCES

[1] Maltoni, D., Maio, D., Jain, A.K., & Prabhakar, S. (2003). "Handbook of fingerprint recognition". New York: Springer..

[2] Thomas Yeo, Wee Peng Tay, Ying Yu Tai., "Image Systems Engineering Program", Stanford University. Student project.

[3] L.C. Jain, U.Halici, I. Hayashi, S.B. Lee and S.Tsutsui. Intelligent biometric techniques in fingerprint and face recognition. 1999, the CRC Press.

[4] N. Ratha, S. Chen and A.K. Jain, "Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images", Pattern Recognition, Vol. 28, pp. 1657-1672, November 1995.

[5] Ko, T. (2005). "Multimodal biometric identification for large user population using fingerprint, face and iris recognition". Proceedings of the 34th Applied Imagery and Pattern Recognition Workshop, 218-223.

[6] Luo, X., Tian, J., & Wu, Y. (2000). "A minutia matching algorithm in fingerprint verification". 15th International Conference on Pattern Recognition, 4, 833-836.

[7] Patil, P.M., Suralkar, S.R., & Sheikh, F.B. (2005). "Rotation invariant thinning algorithm to detect ridge bifurcations for fingerprint identification." Proceedings of the 17th IEEE International Conference on Tools with Artificial Intelligence, 634-641.

[8] Ross, A., Jain, A. K., Reisman, J.: "A Hybrid Fingerprint Matcher, Pattern Recognition", Vol. 36, No. 7, (2003) 1661-1673.

[9] A. Jain, L. Hong, S. Pankanti, and R. Bolle "On-line identity-authentication system using fingerprints", Proceedings of IEEE \ (Special Issue on Automated Biometrics), vol. 85, pp. 1365–1388, September 1997.

[10] Ito, K., Morita, A., Aoki, T., Higuchi, T., Nakajima, H., & Kobayashi, K. (2005), "A fingerprint recognition algorithm using phase-based image matching for low quality fingerprints" Proceedings of IEEE International Conference on Image Processing, 2, 33- 36.

[11] Jain, A.K., Ross, A., & Prabhakar, S. (2004). "An introduction to biometric recognition" IEEE Transactions on Circuits and Systems for Video Technology, 14, 4-20.

[12] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino. "Impact of artificial 'gummy' fingers on fingerprint systems". In proceedings of SPIE, vol. 4677, Jan 2002.

[13] D.Maio and D. Maltoni. "Direct gray-scale minutiae detection in fingerprints". IEEE Trans. Pattern Anal. And Machine Intell., 19(1):27-40, 1997.