International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

SCRUTINY THE SUSCEPTIBILITY IN BIOMETRICS

JayanthiVagini K[1], Manimekalai M[2]

[1]*Department of Computer Application, AJK College of Arts & Science, Coimbatore*
[2]*Department of Information Technology, AJK College of Arts & Science, Coimbatore*

ABSTRACT

The objective of this scrutiny is to find the susceptibility in biometrics system and their performance against known problems. Identity management plays a critical role in a number of applications. Examples of such applications include regulating international border crossings, restricting physical enroll to important facilities like nuclear plants or airports, controlling logical access to shared resources and information, performing remote financial transactions, or distributing social welfare benefits. The proliferation of web-based services (e.g., online banking) and the deployment of decentralized customer service. The main aim of this paper is to discuss with main emphasis on partial biometric with the help of proposing algorithm TMSE(Template Matching with Southerland Equation) and maintain the partial variation in the databases of biometrics system.

KEYWORDS:BIOMETRIC, SECURITY, SUSCEPTIBILITY, ENROLL, PARTIAL VARIATION, TMSE

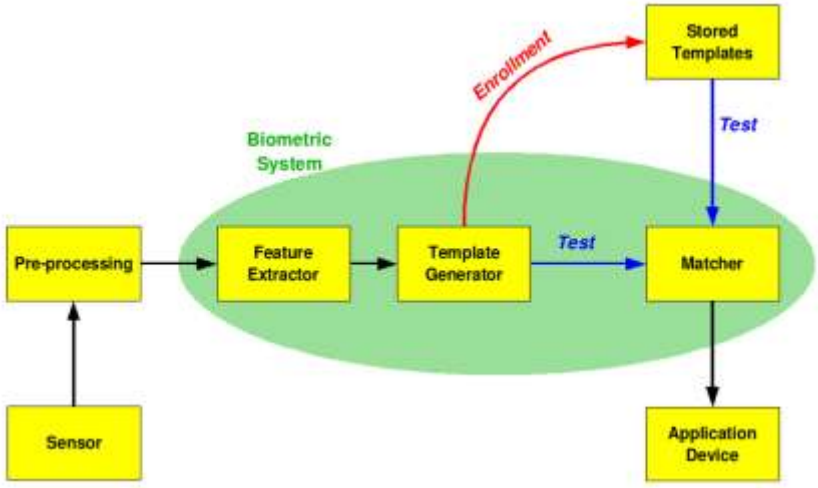
I.INTRODUCTION

Biometric use is very application dependent. Certain biometrics will be better than others based on the required levels of convenience and security. No single biometric will meet all the requirements of every possible application. First, in verification (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps are involved in the verification of a person. In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison. 'Positive recognition' is a common use of the verification mode, "where the aim is to prevent multiple people from using the same identity".

Second, in identification mode the system performs a one-to-many comparison against a biometric database in an attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be". The latter function can

only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective.

The first time an individual uses a biometric system is called *enrollment*. During enroll, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way. A vector of numbers or an image with particular properties is used to create a *template*. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the file size and to protect the identity of enroll.



During the enrollment phase, the template is simply stored somewhere (on a card or within a database or both). During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyse the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area). Selection of biometrics in any practical application depending upon the characteristic measurements and user requirements. In selecting a particular biometric, factors to consider include, performance, social acceptability, ease of circumvention and/or spoofing, robustness, population coverage, size of equipment needed and identity theft deterrence. Selection of a biometric based on user requirements considers sensor and device availability, computational time and reliability, cost, sensor size and power consumption.

II. RELATED WORK

2.1 Biometric performance

The following are used as performance metrics for biometric systems:

False match rate (FMR, also called FAR = False Accept Rate): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs that are incorrectly accepted. In case of similarity scale, if the person is an imposter in reality, but the matching score is higher than the threshold, then he is treated as genuine. This increases the FMR, which thus also depends upon the threshold value.

False non-match rate (FNMR, also called FRR = False Reject Rate): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs that are incorrectly rejected.

Receiver operating characteristic or relative operating characteristic (ROC): The ROC plot is a visual characterization of the trade-off between the FMR and the FNMR. In general, the matching algorithm performs a decision based on a threshold that determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be fewer false non-matches but more false accepts. Conversely, a higher threshold will reduce the FMR but increase the FNMR. A common variation is the *Detection error trade-off (DET)*, which is obtained using normal deviation scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).

Equal error rate or crossover error rate (EER or CER): the rate at which both acceptance and rejection errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is the most accurate.

Failure to enroll rate (FTE or FER): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.

Failure to capture rate (FTC): Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.

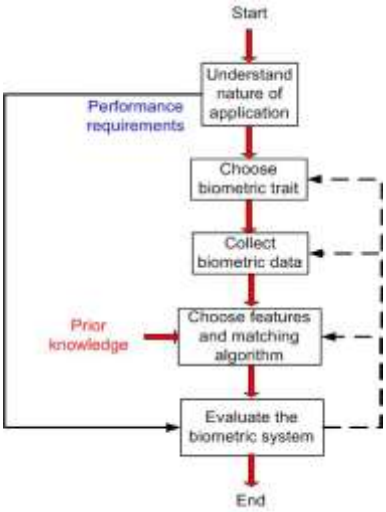
Template capacity: the maximum number of sets of data that can be stored in the system.

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

Fig Three different fingerprint impressions of the same finger. (a) Rolled fingerprint, (b) plain fingerprint and (c) latent fingerprint

2.2 The Design Cycle of Biometric Systems

The design of a template matching (template matching algorithm) biometric system typically entails the following major activities, some of which are carried out iteratively. The foremost step in designing a biometric system is understanding the nature of the application and the performance requirements. This is followed by choosing the right biometric trait(s) for the application in hand. Given a specific biometric trait, one needs to collect biometric data from a subset of target population and design or train the core biometric modules, including the feature extractor and the matcher. Finally, the developed biometric system must undergo a thorough evaluation procedure to ensure that it meets the requirements of the application.



III.PROPOSED TECHNOLOGY

No two people are believed to have identical fingerprints, but it have found that partial similarities between prints are common enough that the fingerprint-based security systems used in mobile phones and other electronic devices can be more vulnerable than previously thought.

The vulnerability lies in the fact that fingerprint-based authentication systems feature small sensors that do not capture a user's full fingerprint. Instead, they scan and store partial fingerprints, and many phones allow users to enroll several different fingers in their authentication system. Identity is confirmed when a user's fingerprint matches any one of the saved partial prints.

3.1Creating the MasterPrint

There could be enough similarities among different people's partial prints that one could create a "MasterPrint." A MasterPrint that could reveal a similar level of vulnerability. Indeed, they found that certain attributes in human fingerprint patterns were common enough to raise security concerns. The attributes of MasterPrints culled from real fingerprint images, and then built an algorithm for creating synthetic partial MasterPrints. Experiments showed that synthetic partial prints have an even wider matching potential. The high matching capability of MasterPrints points to the challenges of designing trustworthy fingerprint-based authentication systems and reinforces the need for multi-factor authentication schemes.

3.2 Guidelines for Capturing Fingerprints

✓ The images of all the ten fingers are to be captured. The fingerprints must be captured in the sequence of slaps of four fingers of left hand, right hand followed by the two thumbs.

✓ The fingers have to be positioned correctly on the platen to enable capture. There should be no direct light shining on the platen. Use the Indicators on fingerprint devices for positioning of fingers. The fingers should be placed in right direction on the device. Please consult the manufacturer manual incase of any doubt or else consult the supervisor.

✓ Use a lint free cloth periodically to clean the platen of the finger print device for good finger print capture

✓ Check devices periodically for scratches, out of focus images, only partial images getting captured. In case any such problem is noticed, then report to your Supervisor/HQ and request for change of equipment.

✓ Fingerprints cut off, wet/smudged fingerprint; very light prints due to insufficient pressure will result in poor quality. The resident's hands should be clean (no mud, oil etc.). Ask resident to wash hands with water and soap, if necessary.

✓ The fingers should not be excessively dry or wet. Moisten with a wet cloth or dry finger with a dry cloth.

✓ The Enrollee should be requested to place all four fingers of the left hand/right hand/two thumbs to platen of the fingerprint scanner for the four-finger capture to ensure good contact and maximize the area of the captured fingerprints. Ensure that the fingers are placed flat and till the top joint of the finger is placed well on the scanner. The top of the fingers should be within the platen area and not outside the defined area.

✓ If automatic capture does not happen, the operator should force the capture when force capture tab is enabled in the enrolment software.

✓ The operator should check the actionable feedback when capture fails. Some actionable feedbacks provided by software are:

- Number of fingers present does not match with expected number of fingers
- Finger not positioned correctly
- Too much Pressure (duty cycle)
- Too little pressure
- Central region missing
- Excessive moisture (wetness)
- Excessive dryness

✓ The operator should visually check the image for quality and for typical problems. In case there are problems go back to steps above to retry the capture.

✓ When image quality is pass or if maximum number of captures are exhausted , move on to the next step.

✓ Fingerprints are best captured in standing position.

✓ In case of additional fingers, ignore the additional finger and capture the main five fingers.

✓ Make sure your own fingerprints do not get mixed with the resident's fingerprints. Operators can carefully put small pressure on the resident's fingers to capture the fingerprints but always make sure not to mix your own fingerprints.

3.3Image Matching Algorithm

In this paper, we have considered two image matching algorithm for image comparison.

✓ Template matching with Pixel values

✓ Shorthand equation

Template Matching with pixel values is a high-level machine vision method that distinguishes the parts on an image that match a predefined layout in the database. The algorithm is:

✓ An input image is converted into grey scale image.

✓ It is passed through spatial frequency filter in order to smoothen the broken edges and remove the noise.

✓ All the separate white regions are marked as different objects and counted, cropped to its minimum size. A junk object is created around each pixel.

✓ After that, the pixel region is resized to the size of templates and then each pixel is compared to all the templates pre-saved in a matrix database.

Sorthand Equationconsider shifting the window Wby (u,v). The pixels in W change done as two methods 1.Compare each pixel before and after using the sum of squared differences (SSD) 2. Defines an SSD "error"E(u,v).

$$E(u,v) = \sum_{x,y} w(x,y)[I(x+u,y+v) - I(x,y)]^2$$

E is the difference between the original and the moved window. U is the window's displacement in the x direction. V is the window's displacement in the y direction. W(x, y) is the window at position (x, y). This acts like a mask. Ensuring that only the desired window is used.I is the intensity of the image at a position (x, y). I(x+u, y+v) is the intensity of the moved window. I(x, y) is the intensity of the original. Maximize this by,

$$\sum_{x,y} [I(x+u,y+v) - I(x,y)]^2$$

expand the object using the Taylor series,

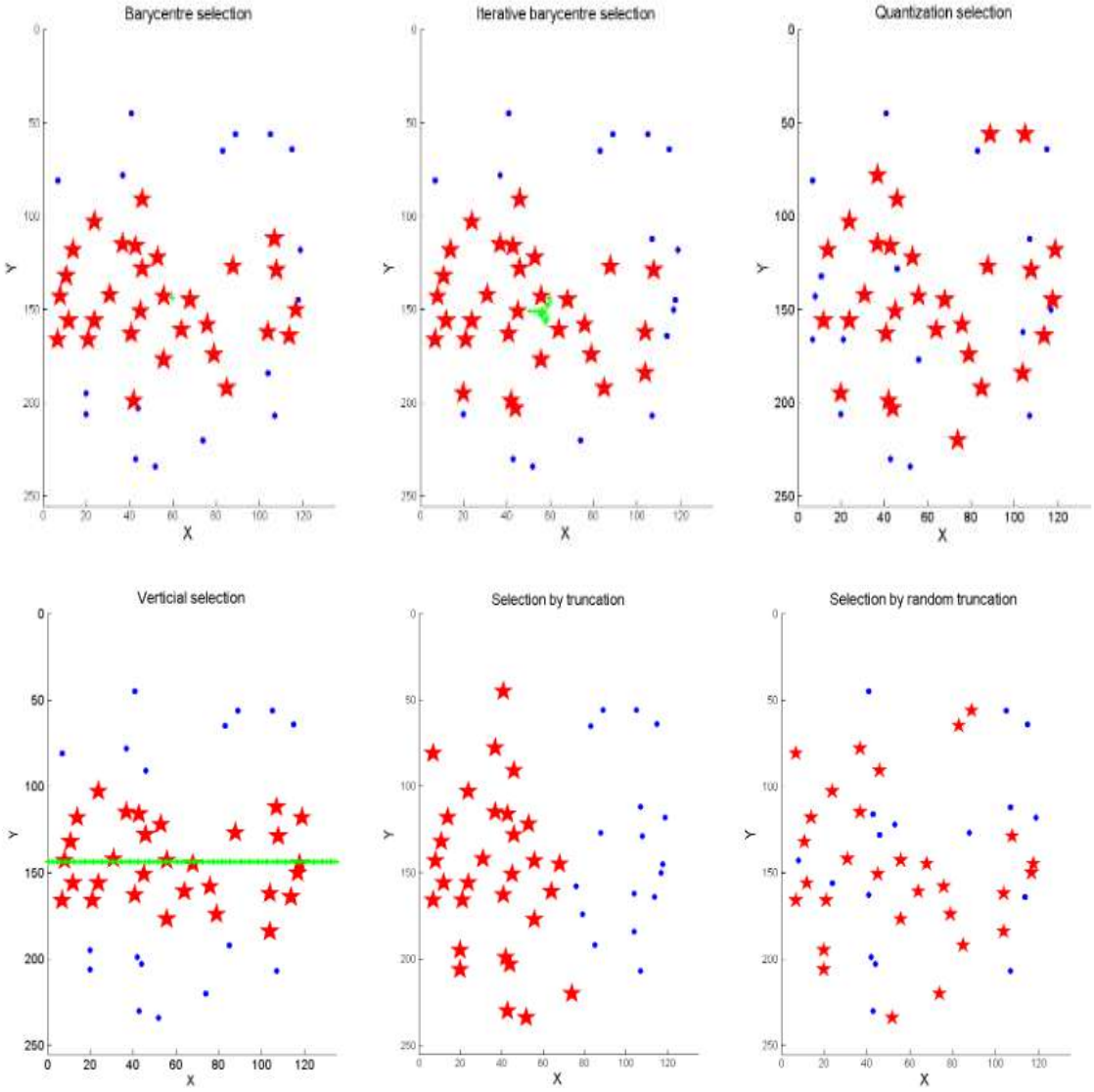
$$E(u,v) \approx \sum_{x,y} [I(x,y) + uI_x + vI_y - I(x,y)]^2$$

IV.EXPERIMENTAL RESULTS

4.1 Localization of partial variations in the template matching

Selected partial variations are represented by a red star and others with a blue circle. We can see that the structure of the fingerprint template uses an Y ascending sorting of the pixels. The CORE point is the focus of the innermost recurring ridge in a fingerprint. With the barycentre and iterative barycentre approach, we select minutiae near the estimated CORE. With the K-mapping method, Sutherland equation, we have partial variations in different part of the template, we have nearly the same reduced template matching than the barycentre and iterative barycentre ones. With the vertical selection method, we reduce biometric in top and bottom of the template matching. With the truncation method, we reduce the right part of the template matching. With the random truncation method, we obtain a similar shape of the fingerprint than the K-mapping and Sutherland equation.

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354



V.CONCLUSION

Fingerprint recognition is one of the most mature biometric technologies and it has been in use for over 100 years. Despite the maturity of fingerprint technology, its widespread adoption in a diverse set of applications has raised several new challenges that the scientific community is currently addressing. While different types of fingerprint sensing technologies have been developed, capturinghighqualityfingerprintimagesfromfingersundernon-idealconditions and unhabituated users is still problematic. One technology that shows promise is the acquisition of 3D fingerprints in a touchless mode. A major advantage of this modality is that it can capture rolled-equivalent fingerprint images much faster than the conventionalrolling process. It may also avoid the skin distortion introduced by rolling and other partial variations.The proposed algorithm is faster and reduces process overheads when compared with traditional minutiae based algorithms as it avoids tasks like partial variations, alignment and orientation.

REFERENCES

[1.] Zhao, Q., Zhang, D., Zhang, L.,andLuo, N. (2010) High resolution partial fingerprint alignment using pore–valley descriptors, Pattern Recognition, Vol. 43, Pp. 1050-1061.

[2.] P. J. Phillips, W. T. Scruggs, A. J. OToole, P. J. Flynn, K. W. Bowyer, C. L. Schott, and M. Sharpe. FRVT 2006 and ICE 2006 Large-Scale Results. Technical Report NISTIR 7408, NIST, March 2007.

[3.] 3.M. Theofanos, B. Stanton, and C. A. Wolfson. Usability & Biometrics: Ensuring Successful Biometric Systems. Available at http://zing.ncsl.nist.gov/biousa/docs/ Usability_and_Biometrics_final2.pdf, June 2008.

[4.] ISO/IEC 19795-1:2006. Biometric Performance Testing and Reporting – Part 1: Principles and Framework. Available at http://www.iso.org/iso/iso_catalogue/ catalogue_tc/catalogue_detail.htm?csnumber=41447, 2006.

[5.] American National Standards Institute. Data Format for the Interchange of Extended Friction Ridge Features.Technical report, ANSI/NIST-ITL, 2010.

[6.] M. Indovina et al. ELFT Phase II - an evaluation of automated latent fingerprint identification technologies.Technical report, NISTIR 7577, April 2009.

[7.] D.Maltoni,D.Maio,A.K.Jain, andS.Prabhakar. Handbook ofFingerprint Recognition (2nd Edition). Springer Verlag, 2009.

[8.] Gonzalez RC, Woods RE. *Digital Image Processing*.3rd edition.Prentice Hall; 2002.

[9.] Venkatesan S, Madane SSR. Face recognition system with genetic algorithm and ANT colony optimization. *International Journal of Innovation, Management and Technology*.2010;1(5)